Securing a ServerLink server

Overview

Securing any server is a never-ending story where every expert could add another chapter.

ServerLink benefits from and is compatible with existing security infrastructure in a company (Active Directory, GPOs, HTTPS servers, SSL or SSL telecommunication systems, VPN, access control with or without ID cards, etc).

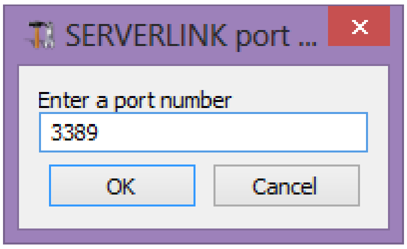
For customers who want to easily secure their servers, ServerLink offers a set of simple and effective ways to enforce good levels of security.

Changing the RDP port number and setting up the firewall

With the AdminTool, you can select a different TCP/IP port number for the RDP service to accept connections on. The default one is 3389. You can choose any arbitrary port, assuming that it is not already used on your network and that you set the same port number on your firewalls and on each ServerLink user access programs.

ServerLink includes a unique port forwarding and tunneling capability: regardless the RDP port that has been set, the RDP will also be available on the HTTP and on the HTTPS port number!

If users want to access your ServerLink server outside from your network, you must ensure all incoming connections on the port chosen are forwarded to the ServerLink s server. On the Server tab, click on the "Change RDP port" tab :



Enter a port number: 3389

Server side security options

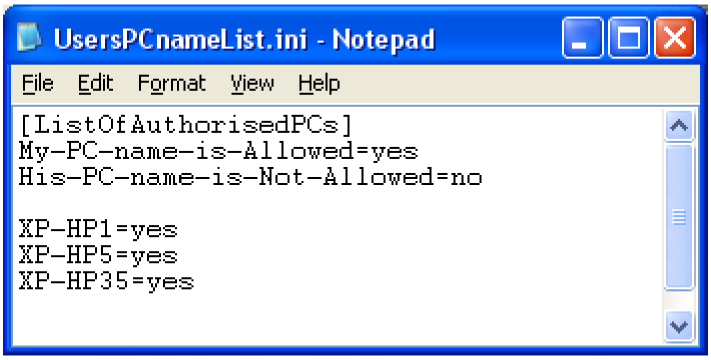
The AdminTool allows you to deny access to any user that is not using a ServerLink connection program generated by the administrator. In this case, any user that would attempt to open a session with any Remote Desktop client other than the ServerLink one (assuming he has the correct server address, the port number, a valid logon and a valid password) will be disconnected automatically.

The administrator can decide that only members of the Remote Desktop User group will be allowed to open a session.

The administrator can decide that a password is mandatory to open a session.

Through setting the applicable local Group Policy, the administrator can specify whether to enforce an encryption level for all data sent between the client and the remote computer during a Terminal Services session. If the status is set to Enabled, encryption for all connections to the server is set to the level decided by the administrator. By default, encryption is set to High.

The administrator can decide to set a firewall on the user PC names. Only the PCs that are listed in a .ini file are able to open a session. Any other PC, even with a valid logon/password, will be rejected.



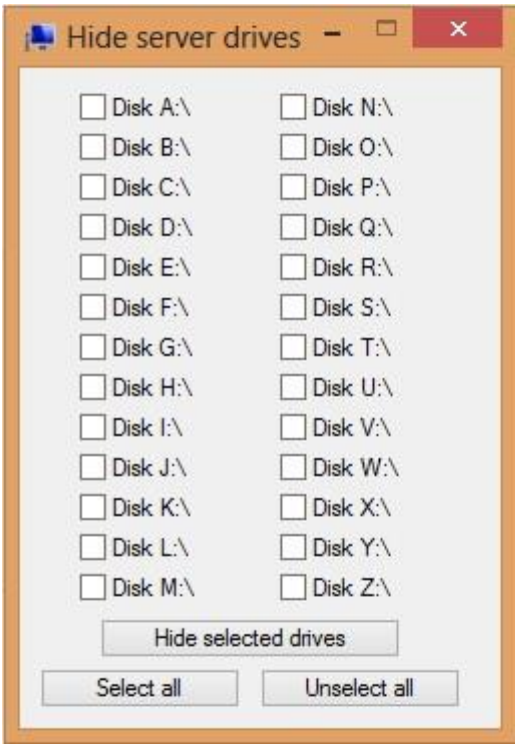
```
[ListOfAuthorisedPCs]
My-PC-name-is-Allowed=yes
His-PC-name-is-Not-Allowed=no

XP-HP1=yes
XP-HP5=yes
XP-HP35=yes
```

The administrator can also set as a rule that only users with a ServerLink connection client will be able to open a session. Any incoming access with a standard RDP or WEBTS access will be automatically rejected.

Hiding the server disk drives:

The AdminTool includes a tool that enables hiding the server disk drives to prevent users from accessing folders through My Computer or standard Windows dialog boxes. On the Security tab, click on "Hide Disk drives" :



The tool works globally. This means that even the administrator will not have a normal access to drives after the settings have been applied.

Comment: This functionality is powerful and does not disable the access to the disk drives. It just prevents the user to display it.

Notes: The tool flags the disks drives as hidden, but it also adds the HIDDEN property to the entire root folders and users list in Document and Settings. If the administrator wants to see these files he must:

1. Type the disk drive letter. For example: **D:\** which will take you to the D: drive.
2. Turn on **SHOW HIDDEN FILES AND FOLDERS** in the folder view properties.

ServerLink access program security options:

The ServerLink client generator gives the capability to lock the ServerLink client to:

- A specific PC name. It means this program will not be able to start from any other PC.
- A physical drive serial number (PC HDD or USB stick). This is a very easy and powerful way to set a high level of security. The only way to connect is with a specific client, and this specific client can only start on a specific USB stick or PC HDD. Some of our customers are delivering fingerprint-reading USB sticks to each of their users and each generated program is locked to the device serial number. In this manner, they can restrict access to the client's program itself, as well as ensuring it cannot be copied off the USB stick and used elsewhere.