

Gatekeeper FAQ (SecureLink 5+)

The SecureLink Gatekeeper is a software component designed to be installed on a Windows or Unix/Linux Server. Its purpose is to serve as a secure access point for one or more servers from your network which then communicates directly to your vendor's SecureLink instance through an encrypted tunnel via the internet.

What are the technical requirements for a Gatekeeper?

- 512MB RAM
- 200MB Disk Space
- Outbound Internet Connection (either via port 22 (ssh), port 80 (http) or via a proxy server)

Will I have to make any changes to the Firewall?

The Gatekeeper requires internet access to communicate with your vendor's SecureLink server, but there are no firewall changes necessary to enable your vendor to connect using SecureLink. If the Gatekeeper is installed on a system that does not have internet access, rules should be set on the firewall to allow outbound SSH or HTTP access directly to your vendor's SecureLink server.

Does the Gatekeeper require a dedicated workstation/server?

The Gatekeeper does not need a dedicated workstation/server. It can be installed directly on the target machine.

Is a reboot required during installation?

The Gatekeeper installation does not require a server reboot.

How long does it take to install a Gatekeeper?

A Gatekeeper installation typically takes less than 5 minutes. Ensure you have the unique Gatekeeper registration code from your vendor to complete the process.

How do I access and manage my Gatekeeper?

To access your Gatekeeper management interface you will navigate to your vendor's SecureLink server and log-in with your provided credentials. These credentials will automatically be emailed to you when your vendor creates your Gatekeeper User account. If you have not received an email from your vendor's SecureLink server, you will need to request an account from your vendor. If another person in your organization already has an administrator Gatekeeper User account, they can generate a new account for you as well.

Local access to the Gatekeeper is also available and provides limited local connectivity settings administration. The Gatekeeper can be accessed locally in two different ways. From your Windows start menu, select -> All Programs/SecureLink/SecureLink Gatekeeper. You can also access the Gatekeeper from your browser by typing <http://127.0.0.1:4680> in the address bar.

How do I enable access for my vendor?

Access will automatically be enabled for your vendor after successfully registering the Gatekeeper for the first time. If you wish to disable it or set up on an access schedule, click on the **Connection Status** link. From here, you can disable access temporarily or create a scheduled access window, outside of which the Gatekeeper will return to a disabled state.

My Gatekeepers » TestVirtual » Connection Status

Access is ENABLED

Gatekeeper access is enabled until apr 6, 2015 08:54:07 am cdt .

With access disabled, your Vendor will not be able to connect to the Gatekeeper.

To check current and past connection activity, view the [Activity Report](#).

To see who will receive an email when a connection occurs, view the [Notification List](#).

- ☒ Enable access now
☐ Enable access for hours
☐ Use an Access Schedule

Can I change Notification e-mails?

Access notification emails are controlled by each individual Gatekeeper user. Each Gatekeeper you have access to will be listed under **My Account** with the ability to toggle notifications on or off for that Gatekeeper. To send notification emails to additional users navigate to My Gatekeepers > Users and Edit the user (or add a new user) you wish to add or remove notifications for.

How do I store credentials?

The Gatekeeper provides you with the ability to store, mask and pass login credentials for your vendors. Credentials can be stored for RDP, SSH and Telnet services.

To add credentials, click on "Settings" and then select **RDP/SSH/Telnet Credentials**. Enter the required information on the credentials screen.

My Gatekeepers » TestVirtual » Settings » Credentials

Usage Instructions

Adding credentials enables you to store and pass valid username and password credentials to RDP, SSH, and Telnet services for an Application.

When your vendor accesses your Application and selects the service, the username and password you provide will be passed through to the RDP, SSH, or Telnet login window. If the credentials are accepted, your vendor will be forwarded directly to the desktop to perform their work.

Important!

RDP credential storage works with the following operating systems:
Windows Vista, XP Pro, 2003 Server & 2008 Server.

RDP Credential storage DOES NOT WORK with Windows 2000 Server, Windows 2000 Professional or any earlier versions of Windows.

[Cancel](#)

Credential Information

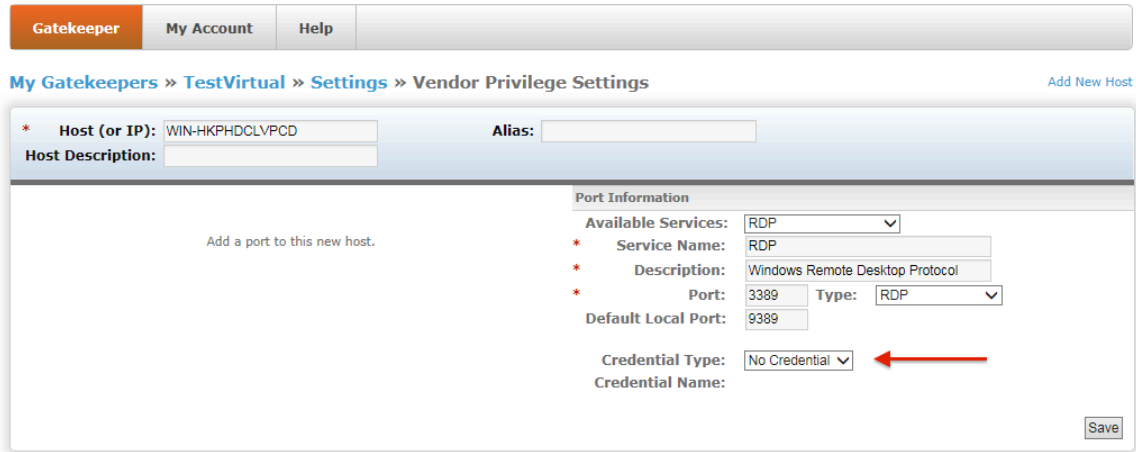
*	Credential Name:	
	Description:	
*	User ID:	
	Password:	
	Confirm Password:	
	Domain:	

Notes

You must provide valid username and password credentials which are associated with an active Windows user account.

If your vendor is unable to authenticate and says they are being prompted for a password, you will need to edit the terminal services settings on the Windows Server machine; Please go to: Start >> Administrative Tools >> Terminal Services Configuration. Click on "Connections" in the left pane. Then double-click "RDP-Tcp" to open the settings menu. Choose the "Logon Settings" tab and uncheck the "Always prompt for password" selection.

Once the credentials have been added, they will need to be associated with the appropriate host and service. To do this, select **Vendor Privilege Settings** from the **Settings** menu. You can either add the credentials to an existing host/service or click **Add New Host** and enter the hostname/ip of the device you would like to add. Hover your mouse over the service in question, click "Edit" and add the appropriate credential and then save it.



Gatekeeper My Account Help

My Gatekeepers >> TestVirtual >> Settings >> Vendor Privilege Settings [Add New Host](#)

* Host (or IP): WIN-HKPHDCLVPCD Alias: Host Description:

Add a port to this new host.

Port Information

Available Services: RDP

* Service Name: RDP

* Description: Windows Remote Desktop Protocol

* Port: 3389 Type: RDP

Default Local Port: 9389

Credential Type: No Credential

Credential Name:

Save

To learn more about using the SecureLink Gatekeeper, please visit the following link for additional FAQs, a video demonstrating usage as well as a contact form if you have additional questions.

<https://www.securelink.com/gatekeeper-upgrade/>