

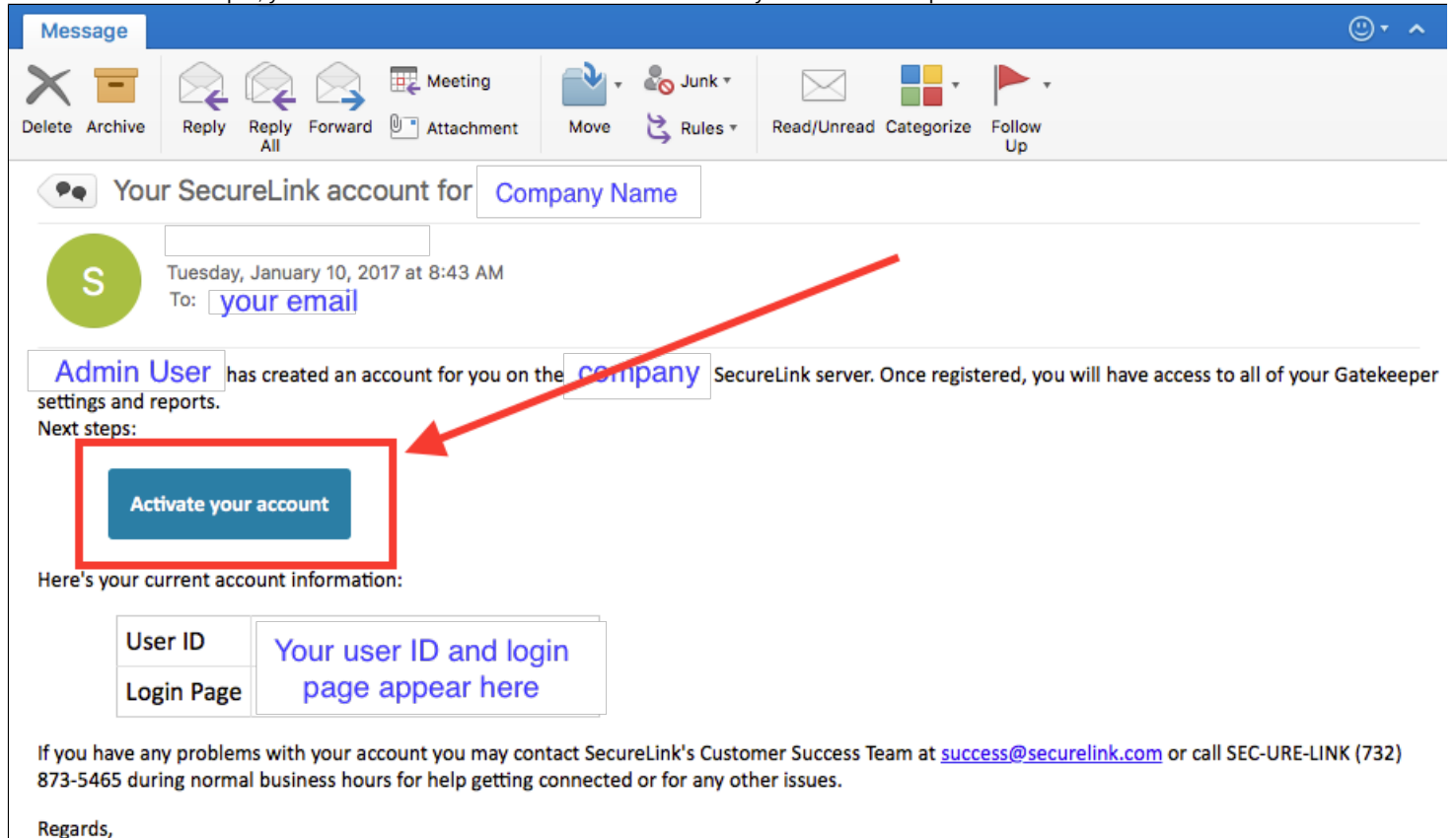
Getting started with the SecureLink Gatekeeper

This document is designed for users who will be managing a SecureLink Gatekeeper. It details the features and functionality included in the Gatekeeper and provides instructions for managing and auditing vendor access into your network.

For users who have installed a Gatekeeper prior to version 5.4, skip the download instructions and see **Logging Into the Gatekeeper Interface** as the first applicable section on managing your Gatekeeper.

Downloading and Installing the Gatekeeper

To download a Gatekeeper, you will receive an email from a vendor contact with your new GateKeeper account:



Message

Delete Archive Reply Reply All Forward Attachment Move Rules Read/Unread Categorize Follow Up

Your SecureLink account for **Company Name**

S Tuesday, January 10, 2017 at 8:43 AM
To: **your email**

Admin User has created an account for you on the **company** SecureLink server. Once registered, you will have access to all of your Gatekeeper settings and reports.

Next steps:

Activate your account

Here's your current account information:

User ID	Your user ID and login
Login Page	page appear here

If you have any problems with your account you may contact SecureLink's Customer Success Team at success@securelink.com or call SEC-URE-LINK (732) 873-5465 during normal business hours for help getting connected or for any other issues.

Regards,

Click **Activate your Account**

After logging in, you will be presented with a page similar to the following. Click the download link to see the available download options and Registration Code:

My Gatekeepers				
My Gatekeepers: 3				
Gatekeeper Name	Local Hostname	Status	Role	Actions
Production Server		Offline	Admin	Download View

My Gatekeepers » Download

By downloading and installing the Securelink Gatekeeper, you are agreeing to the terms and conditions contained in the [SecureLink End User License Agreement](#). For more information, contact **Stark Industries**.

Download Gatekeeper for platform

[Windows](#)

Registration Code

155f1210af

Once the download completes, run the installation wizard to complete the installation.

The final step of the installation process will request the registration code listed generated for your individual gatekeeper, which is available in the download section listed above.

Logging into the Gatekeeper User Interface

Once the Gatekeeper has been installed, click the **View** link to the right of the name to view the Gatekeeper menu:

My Gatekeepers » Production Fax Server

Connection Status

Gatekeeper access is enabled.

Reports

View audit trail information.

Users

Administer users with access to this Gatekeeper, and notification settings.

Settings

Adjust system settings, including stored credentials and vendor privileges.

Connection Status: Enabling and Disabling your Gatekeeper

Click the **Connection Status** menu option to enable and disable the Gatekeeper for your vendor:

My Gatekeepers » Jarvis » Connection Status

Access is ENABLED

Gatekeeper access is enabled via Schedule.

If you disable access, 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](#).

- ☐ Disable access now
☐ Disable access in hours
☐ Disable access at
☒ Use an Access Schedule

Access from until

	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sunday																								
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								

AM PM

Schedule Active

The Gatekeeper provides a number of options for enabling and disabling the Gatekeeper including:

- Enable and Disable manually
- Enable or Disable via an Access Window
- Disable or Enable at some point in the future
- Enable or Disable per an Access Schedule (when using the Access Schedule, you must click the **"Save & Activate"** button to enable the schedule. Once enabled, any manual override will require that you re-activate the schedule.)

Your vendor has no access to enable/disable capabilities and will have no way to reach a disabled Gatekeeper.

Reports

The Gatekeeper keeps a detailed audit of all your vendor access.

[Gatekeeper](#)
[My Account](#)
[Help](#)

My Gatekeepers » Test Environment » Reports

[Session History](#) | [Admin Log Events](#)
[« Previous](#) [Next »](#) 25 items per page

Session History For Site: Test Environment

Session Start	Duration	Owner	Users	Services	View
12/7/16 2:25 PM	0h6m0s	dwayne.slink.admin	Dwayne SLINK. Admin	rssDS	View
12/1/16 2:26 PM	0h4m30s	dwayne.slink.admin	Dwayne SLINK. Admin	0	View
12/1/16 2:11 PM	0h1m0s	dwayne.slink.admin	0	0	View
12/1/16 9:00 AM	0h1m0s	dwayne.slink.admin	0	0	View
12/1/16 7:59 AM	0h0m44s	dwayne.slink.admin	Dwayne SLINK. Admin	rssDS	View
12/1/16 7:48 AM	0h2m39s	dwayne.slink.admin	Dwayne SLINK. Admin	0	View
12/1/16 7:38 AM	0h6m29s	dwayne.slink.admin	2	2	View

Session details can be accessed by clicking the **View** link to the right of the desired session:

[Gatekeeper](#)
[My Account](#)
[Help](#)

My Gatekeepers » Test Environment » Session History

Session Information

Owner: dwayne.slink.admin
 Registration Code: 1a0ddb10af
 Date Created: Dec 7, 2016 2:25:08 PM CST
 Date Completed: Dec 7, 2016 2:31:08 PM CST
 Duration: 0h6m0s

Gatekeeper Information

Application: PUBLIC
 Description: Public Gatekeeper Group
 Version: 5.6.0RC19
 Local Host Name: DESKTOP-KUVPP6T
 Local IP Address: 172.16.128.128

Session Users

Name	Vendor	Remote IP Address	Start Time	End Time	Duration	Status
Dwayne SLINK. Admin	No Vendor	192.168.224.156	12/7/16 2:25 PM	12/7/16 2:30 PM	0h5m0s	Idle Timeout

Session Services

Desktop Sharing

Host Gatekeeper Port 5916

Desktop Sharing Access

Name	Start Time	End Time	Duration	Bytes Sent	Bytes Received	
Dwayne SLINK. Admin	12/7/16 2:25 PM	12/7/16 2:27 PM	0h1m16s	9.56 kB	223.79 kB	Not enabled

[Return to most recent activity](#)

To view GateKeeper user administrative events & logging click **Admin Log Events**:

My Gatekeepers » Jarvis » Reports

[Session History](#) | **Admin Log Events**

Admin Log Events

[All](#)
[CREATE](#)
[UPDATE](#)
[VIEW](#)

Showing 1 to 3 of 3 entries Search...

Time	Method	Object Type	Object Key	Extra Info	User ID
12/07/2016 2:30:17 PM	CREATE	UserSiteBind	19	Gatekeeper-User 'dwindham@securelink.com' was created for Site 58 (Test Environment)	dwayne.slink.admin
12/07/2016 2:41:50 PM	VIEW	UserSiteBind	19	HistAuditLog with rowId 44 viewed for Site 58 (Test Environment)	dwindham@securelink.com
12/08/2016 11:21:11 AM	UPDATE	UserSiteBind	19	C2 Name was updated for Site 58 (Test Environment)	dwindham@securelink.com

Users: Managing Additional Users

As an Administrative Gatekeeper user, you can manage users who have access to your Gatekeeper.

To add a new user, select **Add New Gatekeeper User** in the upper-right corner:

My Gatekeepers » Production Fax Server » Users » Add New User

Add New Gatekeeper User

* Email:

* Name:

Role: Read Only - view audit and info - enable/disable access

Phone:

Read Only - view audit and info - enable/disable access
Read Only - view audit and info - enable/disable access
Admin - edit Gatekeeper settings - enable / disable access
Email Only - receive notification emails only

User permission roles are as follows:

- **Read Only** users can login to view history, and toggle Gatekeeper access, but cannot create other Gatekeeper users or modify permissions.
- **Admin** can create, update, or delete all settings
- **Email Only** will not have login access, they will only be setup to receive connection notification emails

To edit or disable a Gatekeeper users, click the **View** link next to the users name, then click **Edit**.

Settings

The settings menu allows you to create credentials, manage vendor access / privileges, toggle report settings, and change the name of your Gatekeeper

My Gatekeepers » Production Fax Server » Settings

RDP/SSH/Telnet Credentials

Specify Credentials such as the username, password and domain for logging in to a RDP/SSH /Telnet service.

Vendor Privilege Settings

Modify the services accesible to your Vendor.

Report Settings

Enable or disable syslogd remote audit logging.

Set Name

Set or change the name of your Gatekeeper.

RDP/SSH/ Telnet Credentials:

The Gatekeeper can securely store, mask, and pass credentials for your vendor to hosts inside your network.

Credentials can be passed for the following services:

- RDP
- SSH
- Telnet
- FTP (v5.4.2 and above)

Add your credential name, user ID, password, and domain (if a domain credential) and **Save**.

My Gatekeepers » Test Environment » 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:	

[Save](#)

After the credential has been created, it can be applied to hosts / services in **Vendor Privilege Settings**

Managing Vendor Privilege Settings

Within **Vendor Privilege Settings**, you can define what hosts, services, and ports your vendor can access and apply stored credentials.

Additionally, you can control whether or not your vendor can add or modify the hosts / services they have access to.

To apply credentials to an existing service, hover the mouse over the service then the Port Information & Credentials box will appear.

Host: Gatekeeper
 Alias:
Save
+ Add New Port

Description:

Serial#:

Service	Port	Port Information
Desktop Sharing Access	5916	
Primary File Transfer Port	18021	
Windows Remote Desktop Protocol	3389	Service Name: RDP Description: Windows Remote Desktop Protocol Port: 3389 Type: RDP Default Local Port: 9389 Launch via: Mapped interface Credentials + Add - Remove

Save

In this section, you can also add new hosts / services or disable services.

Disabling Vendors from Creating / Defining Services

In the event that your organization does not want a vendor to be able to add additional services , change the radio button to limit this ability:

Allow Vendor-defined Services

☐ Enabled
☒ Disabled

Service Access List

Rules can be established to either explicitly permit or deny access to hosts / IP's or ports so that vendors can have pre-configured access or restrictions to these options:

Service Access Rules

Vendors can access only the above defined Services. Enable Vendor-defined services to restrict Vendors to hosts and ports in this table.

[Add New Access Rule](#)

Service Access List

New Access Rule

Host (or IP): ☐ ANY
Port #: ☐ ANY
Access:

No Service Access Rules defined

Managing report settings

Under **Report Settings**, you can enable Syslog Remote Audit Logging via Hostname or IP (requires UDP port 514 between the gatekeeper and the syslog server)

Gatekeeper My Account Help

My Gatekeepers » Test Environment » Settings » Report Settings

Remote Audit Logging
☒ Enable syslogd remote audit logging
Host (or IP):

Save

Change your Gatekeeper name

Under **Name**, you can change the Gatekeeper name:

 **SECURELINK** Logout

Gatekeeper My Account Help

My Gatekeepers » Test Environment » Settings » Name

Set Gatekeeper Name

Save

Local Gatekeeper Management

There are several tasks that may need to be performed on your local Gatekeeper installation. The Settings menu includes the "Connectivity Settings" section with 4 optional settings:

Connectivity Settings

Proxy Information

- ☒ This machine connects directly to the internet.
☐ Use a Proxy

HTTP Tunneling mode

This selects the method the Gatekeeper uses to communicate to the SecureLink server when direct connection is not possible. If tunneling is needed, the [Connectivity Test](#) will automatically select the most efficient method for your network.

- ☒ Use new-style "alternate" HTTP tunneling
☐ Use original HTTP tunneling mode

Encryption Cipher

- ☒ 128-bit AES (Recommended)
☐ 192-bit AES
☐ 256-bit AES
☐ Triple DES (3DES)
☐ Blowfish

Automatic Update

- ☐ Enabled
☒ Disabled



1. **Proxy Information** - Very rarely will this setting be required. It is only necessary to choose "Use a Proxy" when access to your proxy server requires credentials and the SecureLink Gatekeeper is unable to utilize credentials stored in your browser.
2. **HTTP Tunneling Mode** - You should never need to toggle this setting as it happens automatically during the Connectivity Test
3. **Encryption Cipher** - This can be toggled if you wish to use a cipher other than the default. Be aware that choosing other options may effect the speed and performance of your vendor's experience.
4. **Automatic Update** - It is recommended to leave this enabled as, throughout the year, your vendor will receive server upgrades that include updated code for your Gatekeeper which may include various functionality and security improvements