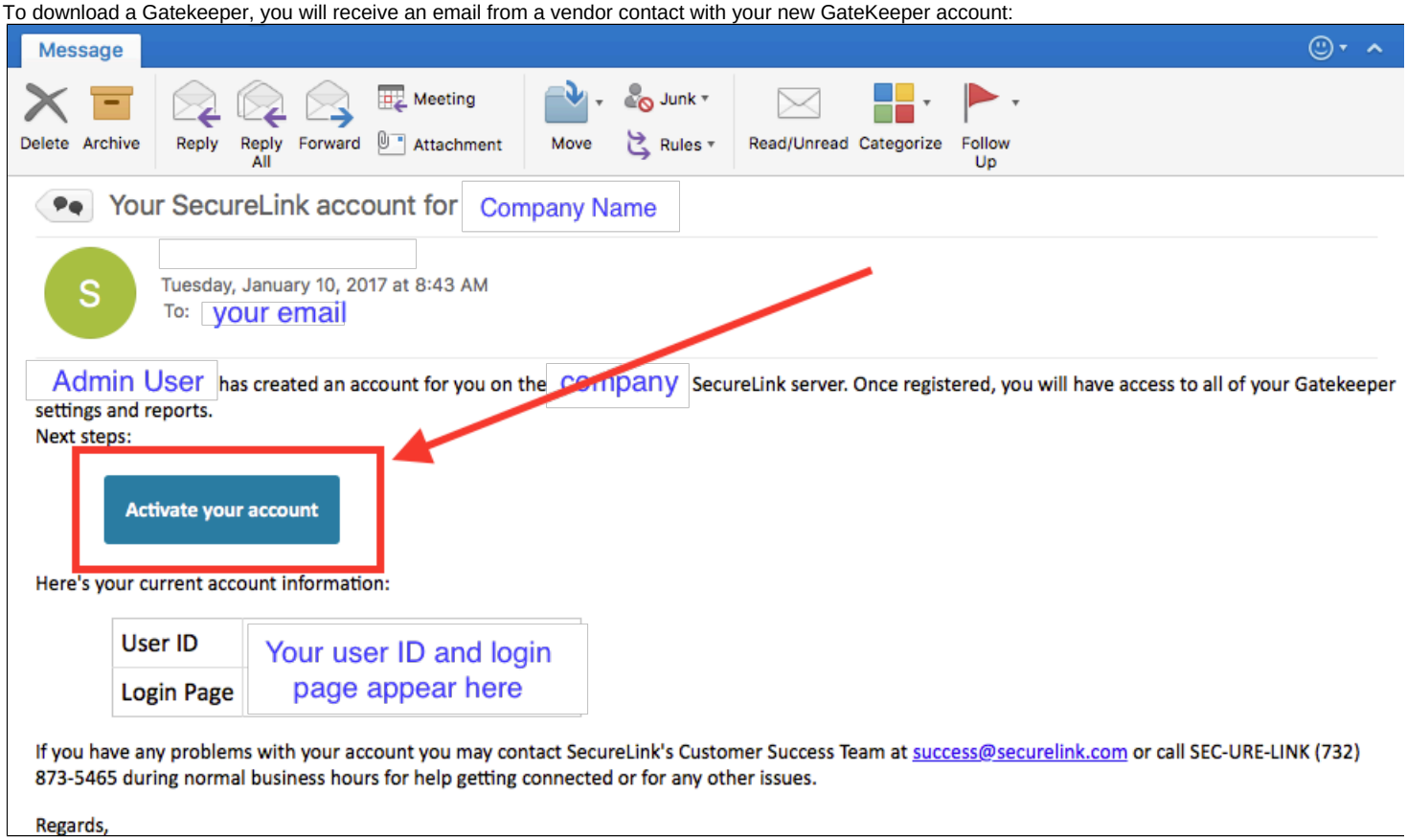
Getting started with the SecureLink Gatekeeper

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.

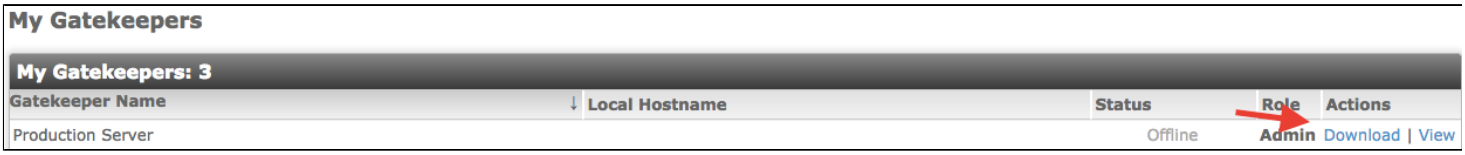
Downloading and Installing the Gatekeeper

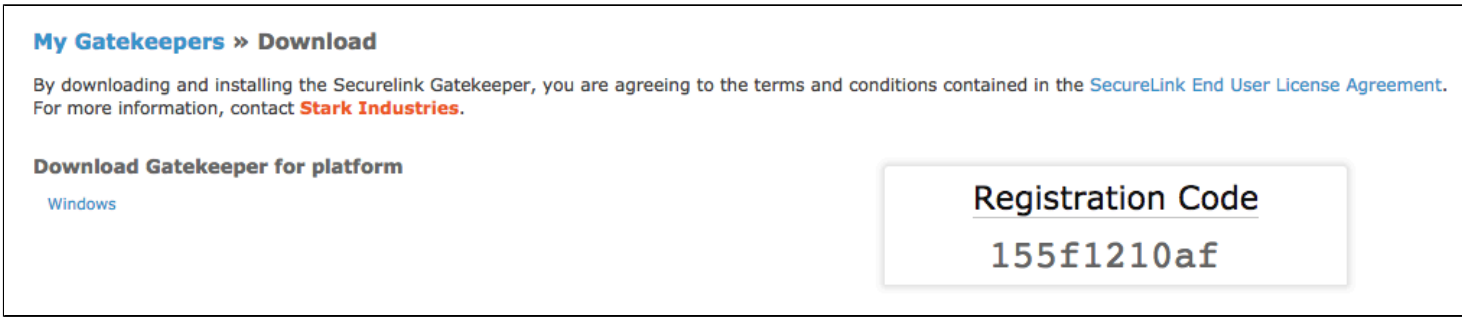
To download a Gatekeeper, you will receive an email from a vendor contact with your new GateKeeper account:



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:



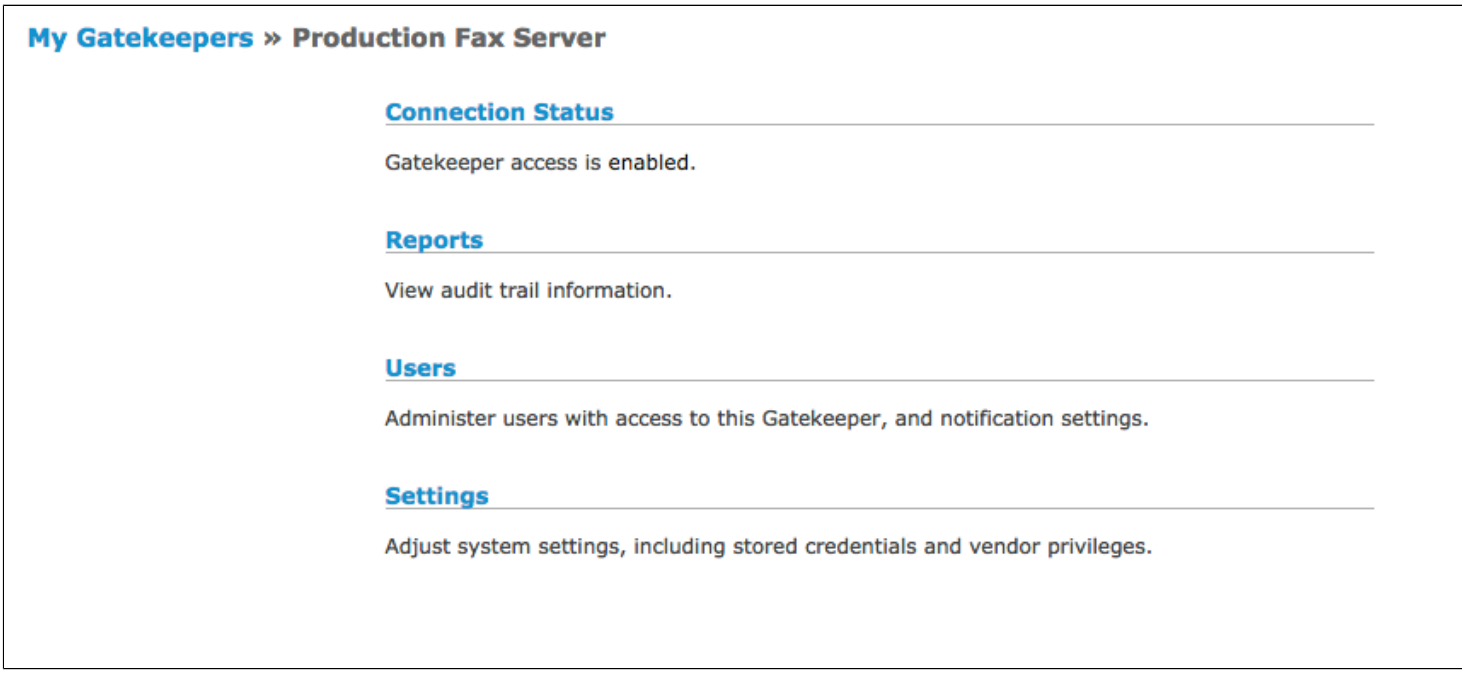


Once the download completes, run the installation wizard to complete the installation.

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.

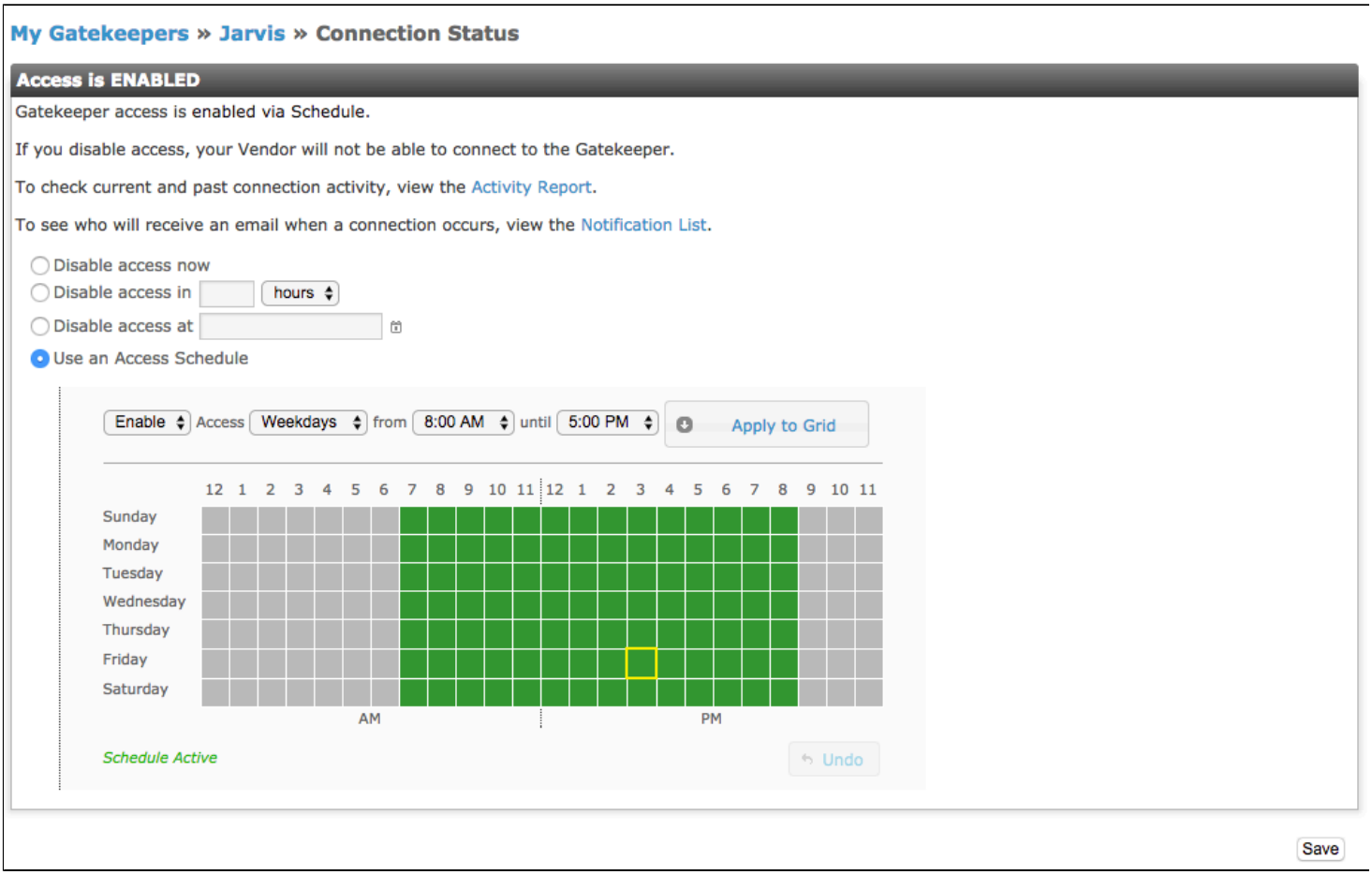
Logging into the Gatekeeper User Interface

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



Connection Status: Enabling and Disabling your Gatekeeper

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



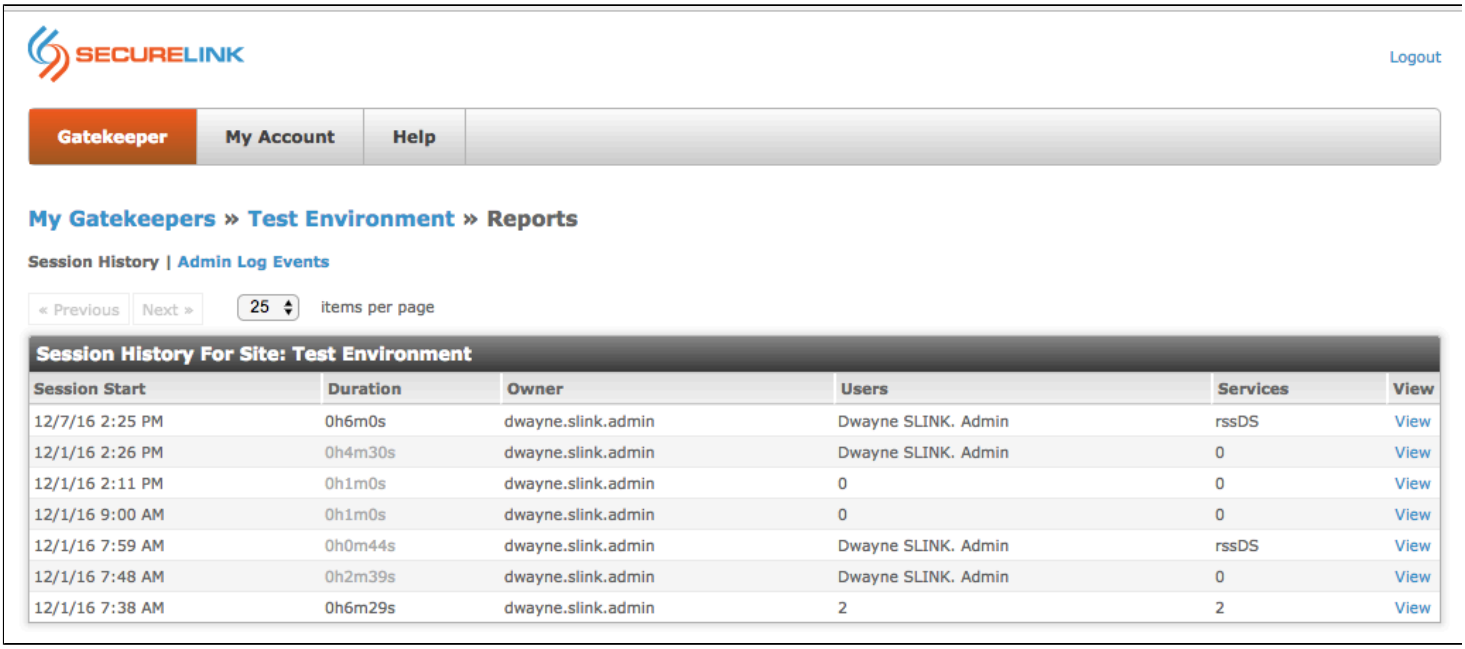
The Gatekeeper provides a number of options for enabling and disabling the Gatekeeper including:

- 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.)

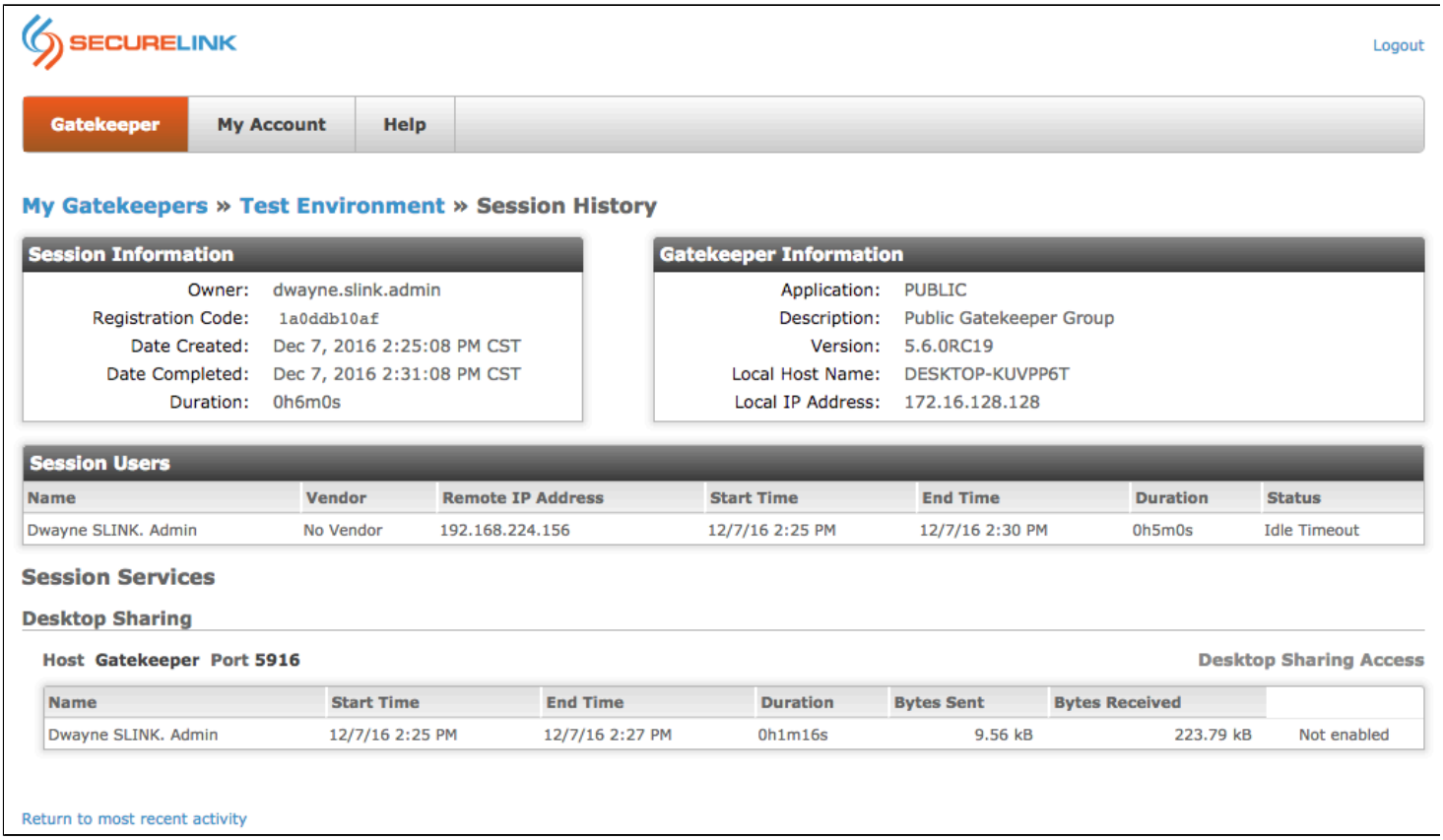
Your vendor has no access to enable/disable capabilities and will have no way to reach a disabled Gatekeeper.

Reports

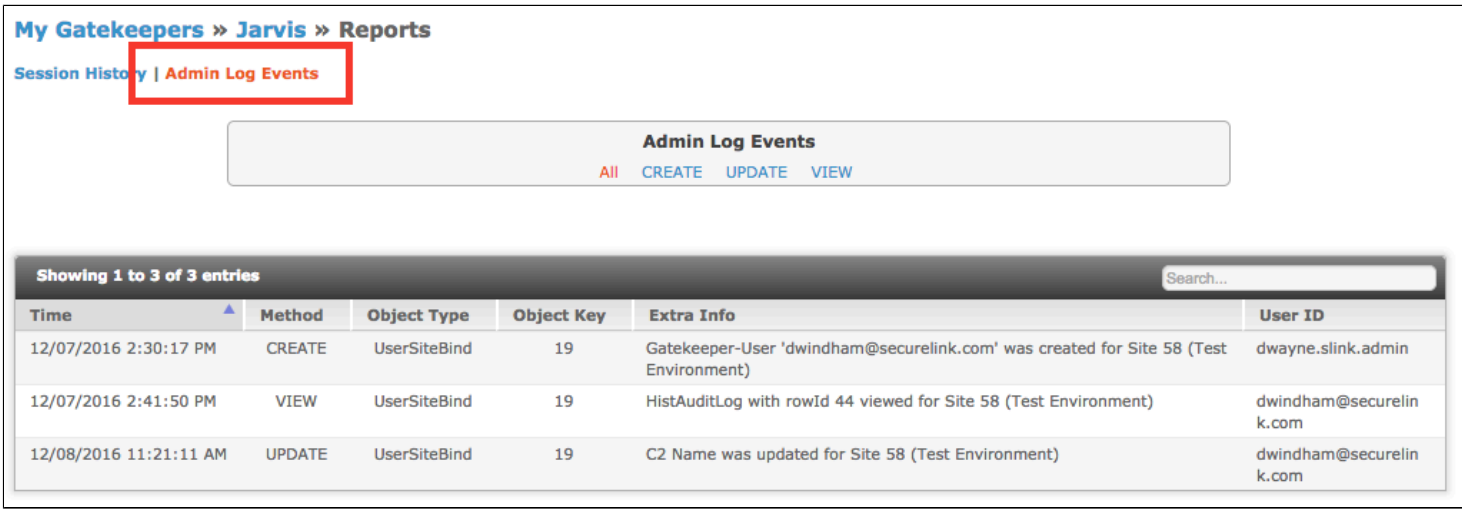
The Gatekeeper keeps a detailed audit of all your vendor access.



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



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



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:

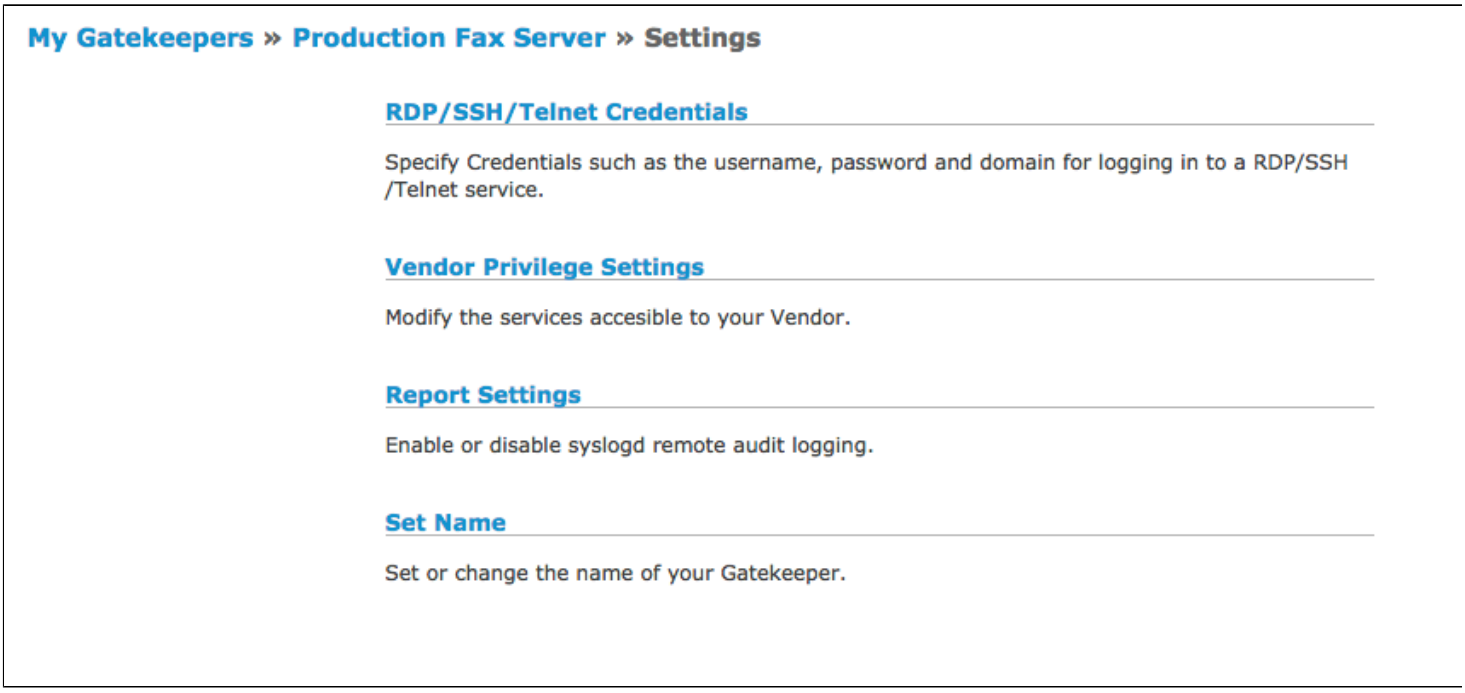
User permission roles are as follows:

- **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



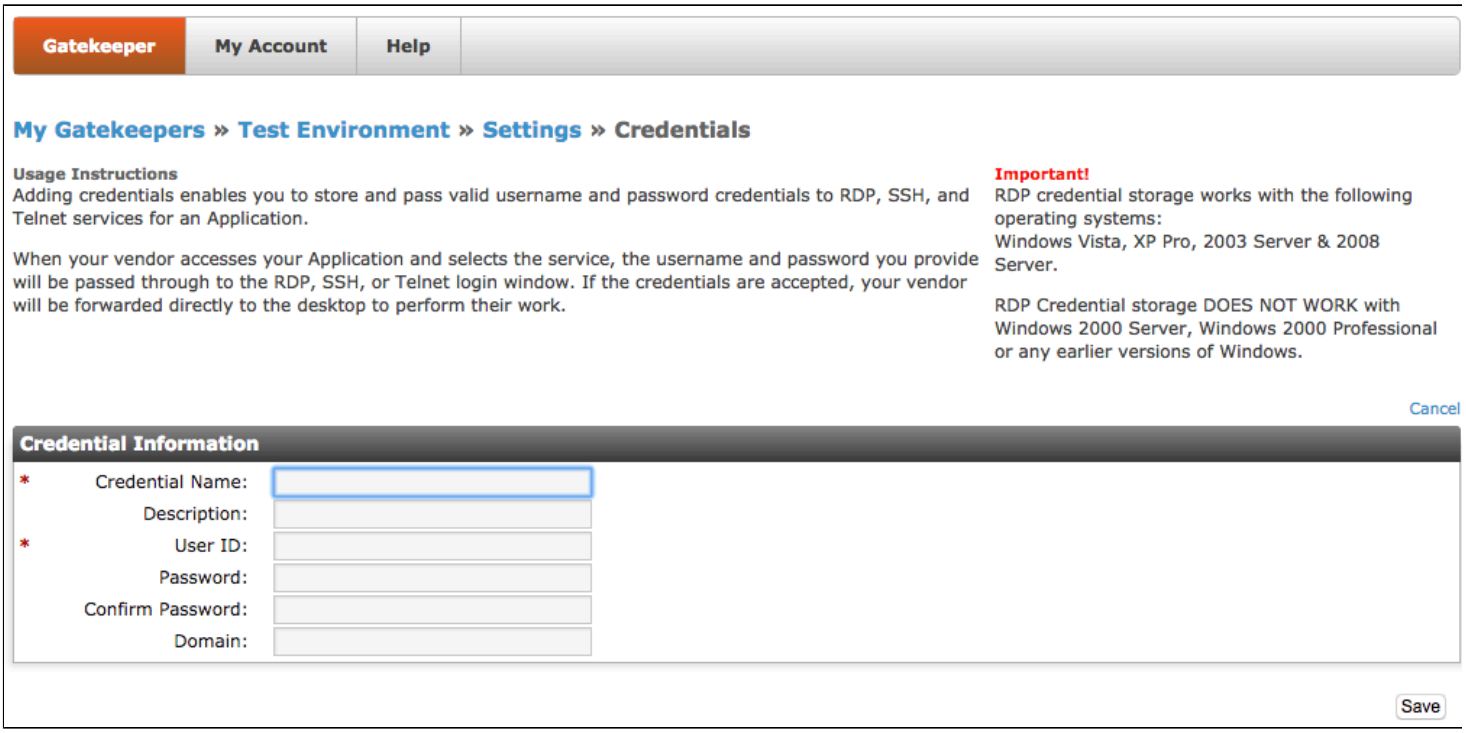
RDP/SSH/ Telnet Credentials:

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**.



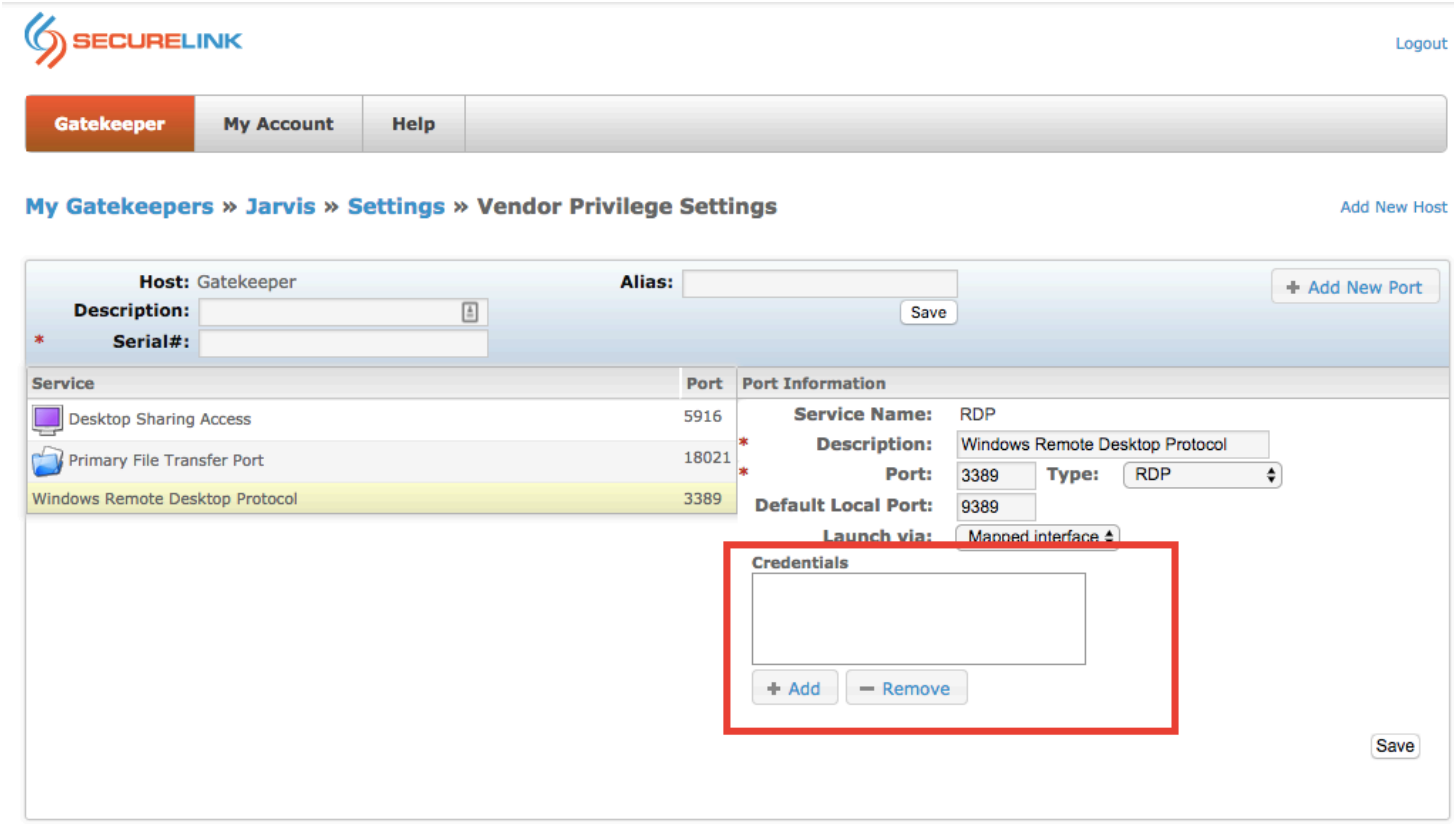
After the credential has been created, it can be applied to hosts / services in **Vendor Privilege Settings**

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.

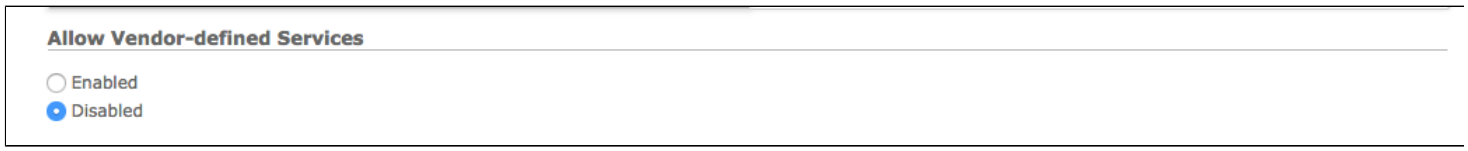
To apply credentials to an existing service, **hover the mouse over the service** then the Port Information & Credentials box will appear.



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:

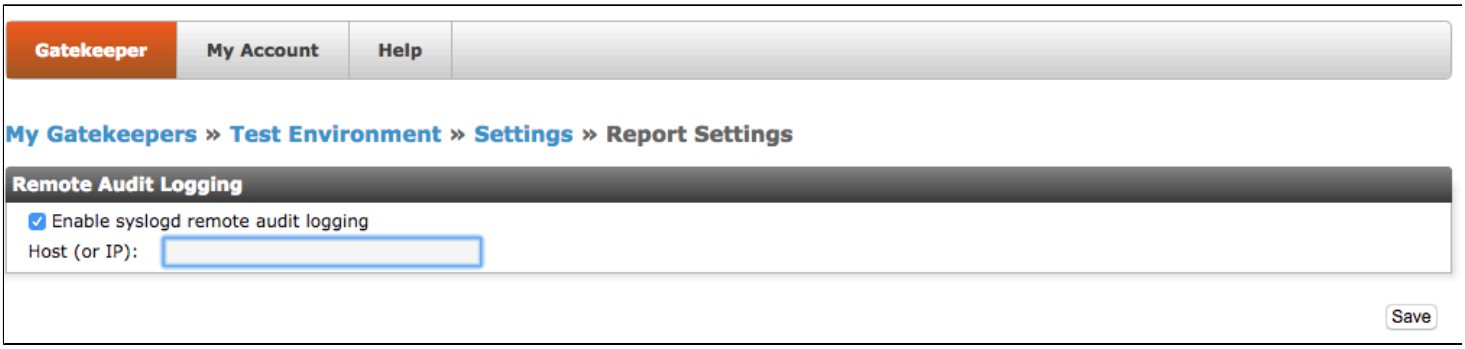


Service Access List

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:

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)

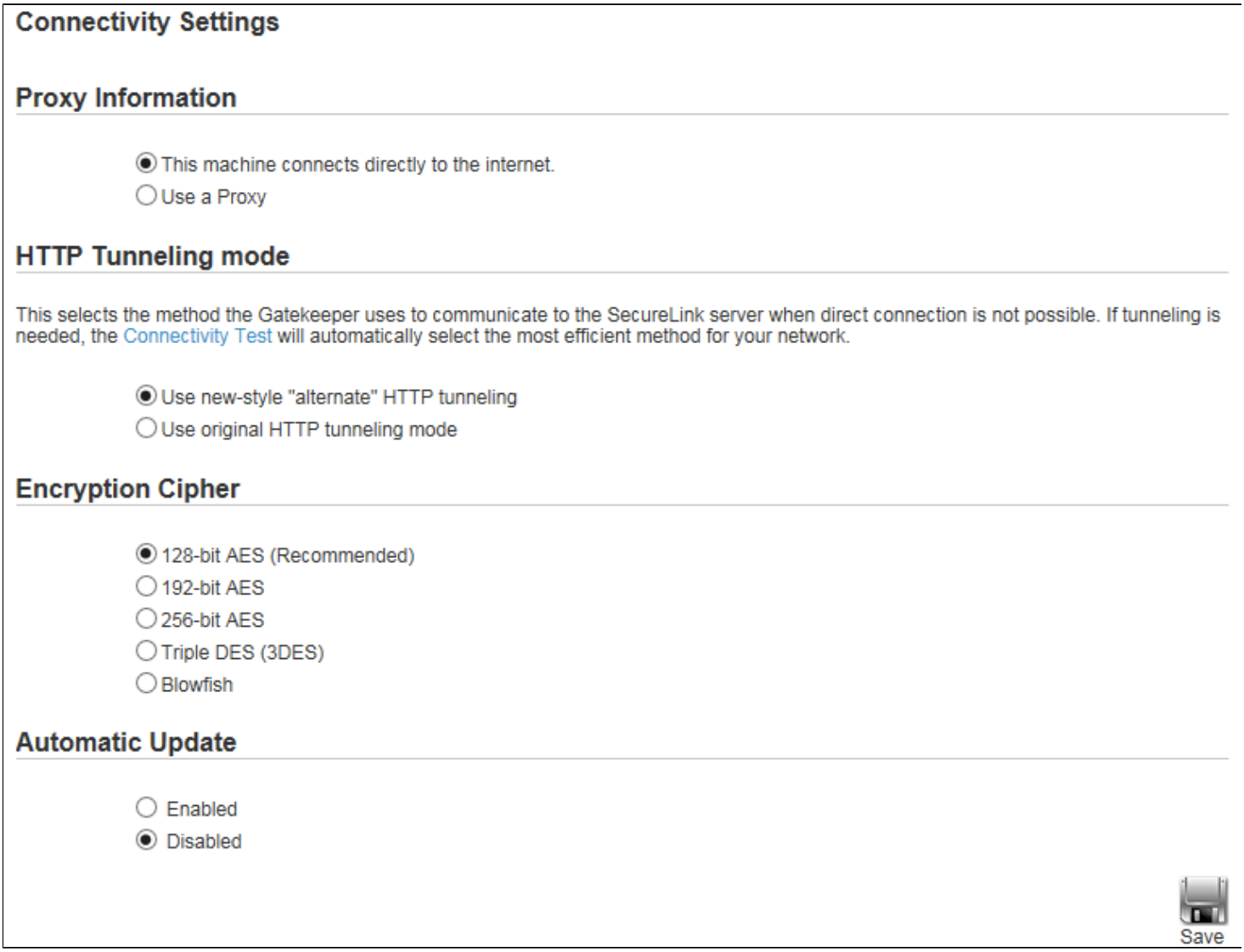


Change your Gatekeeper name

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

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:



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