

SecureFactors

Table of Contents

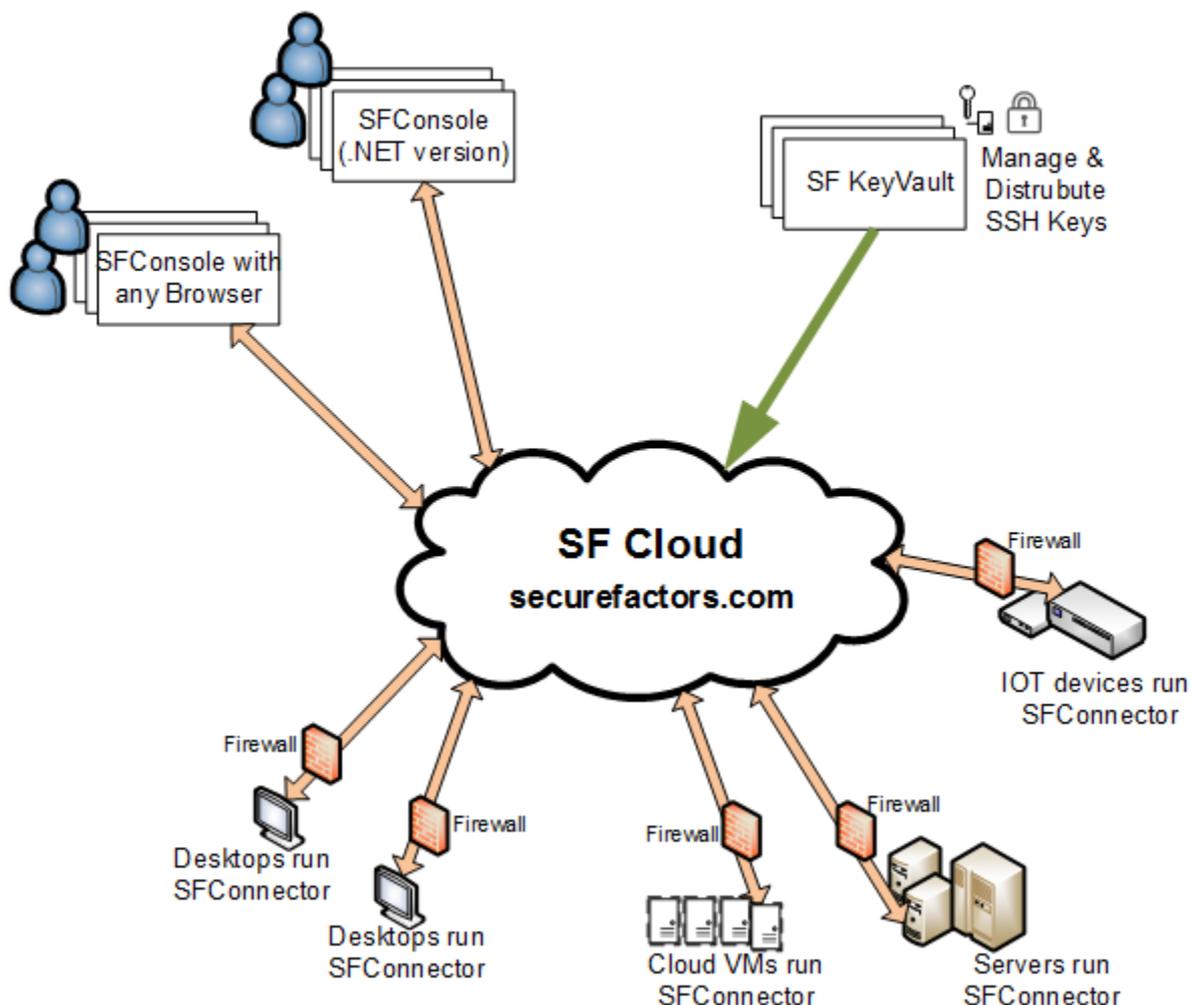
Introduction	2
How to Use	3
Run SF Connector to access systems	10
SF Console	11

SecureFactors(SF) is a new generation cloud system developed to securely access remote systems. It can be used by both end-users and systems administrators. SF's primary advantage is that all remote access is performed without a VPN. SF allows running modern IT tasks like secure remote access, systems management, customer support and SSH key distributions. Access and KeyVault are the first two applications released on SF. Using SF Console any systems linked to a SF cloud account can be accessed and managed anywhere in the world no matter where it is located - behind a firewall or in your enterprise local network, all without a VPN (Virtual Private Network). Access is authenticated and all data communications are secured with FIPS certified cryptographic encryption. SF KeyVault allows full life cycle management of SSH Keys and digital identities.

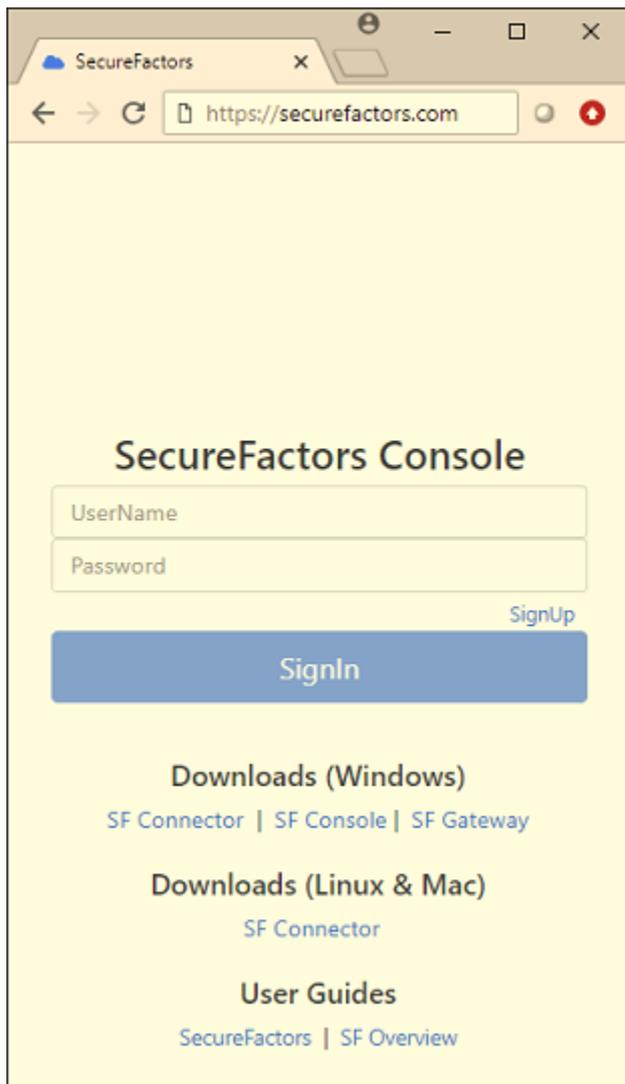
SF supports all Windows operating systems with a SF Connector that runs in all Windows platforms. SF Connector is also available for Linux/Unix/Apple MacOS/IOT devices. This portable version is written in Java programming language. Client side of SecureFactors is termed SF Console. Any web browser can be run as the SF Console allowing access of systems from any operating systems or mobile devices. Thus no software needs to be installed in the client side and a web SF Console is the primary user interface. However, an SF Console application is provided as an additional interface in Windows for sites that need higher resolution rendering of remote desktops than are available through a web browser.

SF Cloud's modern design allows it to be dynamically partitioned to be run in a private or public cloud based on customer security needs. Amazon AWS, Microsoft Azure, Google Cloud Platform, Oracle Cloud and IBM Cloud are key cloud platforms that can host and run SF Cloud. Enterprise customers can also license SF cloud to host it in their own data centers or private cloud, giving maximum deployment flexibility. Managed or accessed systems can be located anywhere in an enterprise, in remote branch locations or in public cloud Virtual Machines or Containers.

SecureFactors allows access to systems anywhere – in Cloud VMs or in Enterprises



SecureFactors is available from <https://securefactors.com> and is used as a "software as a service". Your site administrator may have deployed SF in one of the public or private cloud. So check with your site administrator to find where your SF cloud points to.



To start using SF, first create a SecureFactors account by clicking "SignUp" and providing a username and password to serve as your identity. Username can be in simple name or email format - as long it is unique and the username has not been taken in that SF site, it is acceptable.



Then for the machines to be accessed or managed, download and run SFConnector to install the cloud connector in systems that are to be accessed via SF cloud. SF Connectors are available for a variety of operating systems. Once installed, double click the SFConnector icon to run it and provide the correct cloud account credentials you created during sign up to link the machine to your account.

For the person accessing systems or performing systems administrators tasks, there is nothing to download - all access is provided from any browser which serves as the SF Console. Login to <https://securefactors.com> with a web browser using your SF credentials. To turn on two-factor authentication to an account, click "TOTP" or "U2F Factor" in user setting. For TOTP two-factor authentication, download Google Authenticator from Apple IOS or Android store and take image shot of QR image shown in the SF user account. Then logoff and log back on again. Enter the six digit number from Google authenticators if TOTP two-factor authentication is active for the account after entering the password.

SecureFactors x

Secure | https://securefactors.com/#/users

SecureFactors > User Setting maryhall

First Name:

Last Name:

Userid:

Password:

Phone:

Email:

TOTP Factor:



U2F Factor: Register

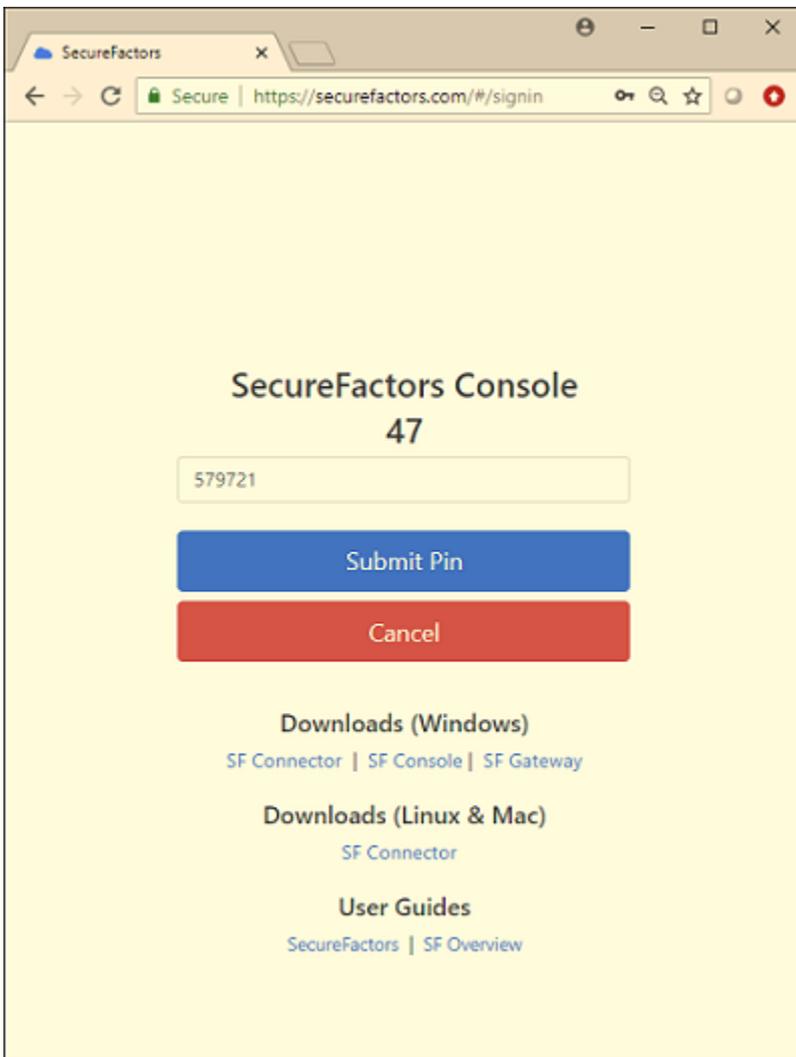
Admin Host Limit:

Default Auth User:

Default Auth Password:

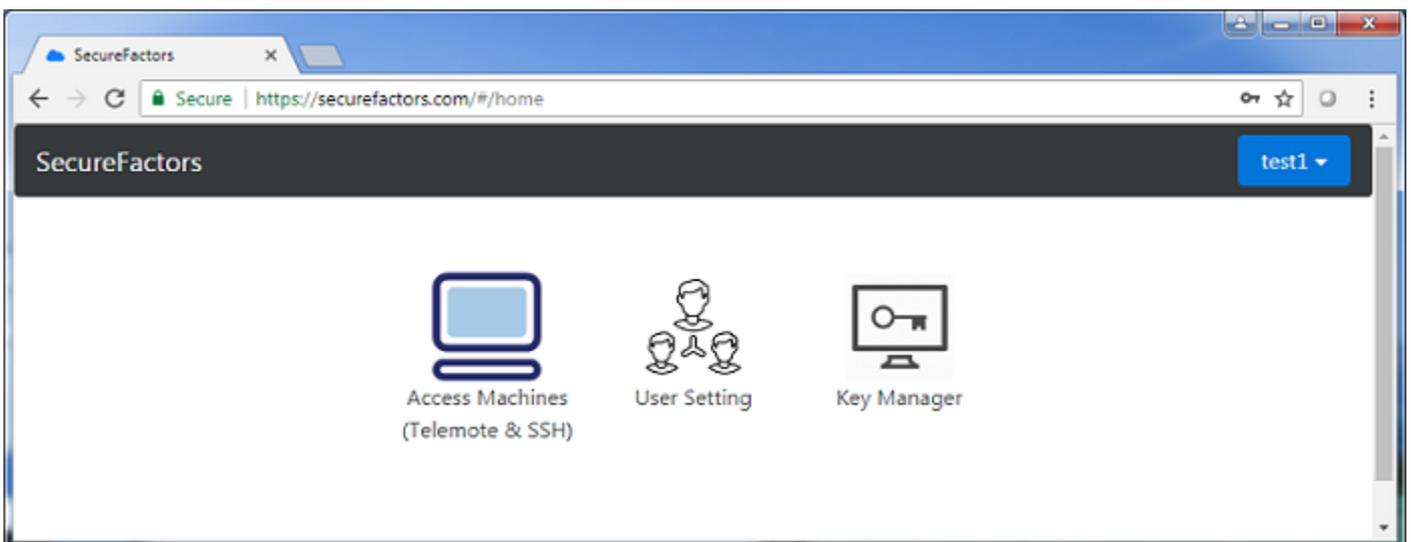
Default Auth PIN:

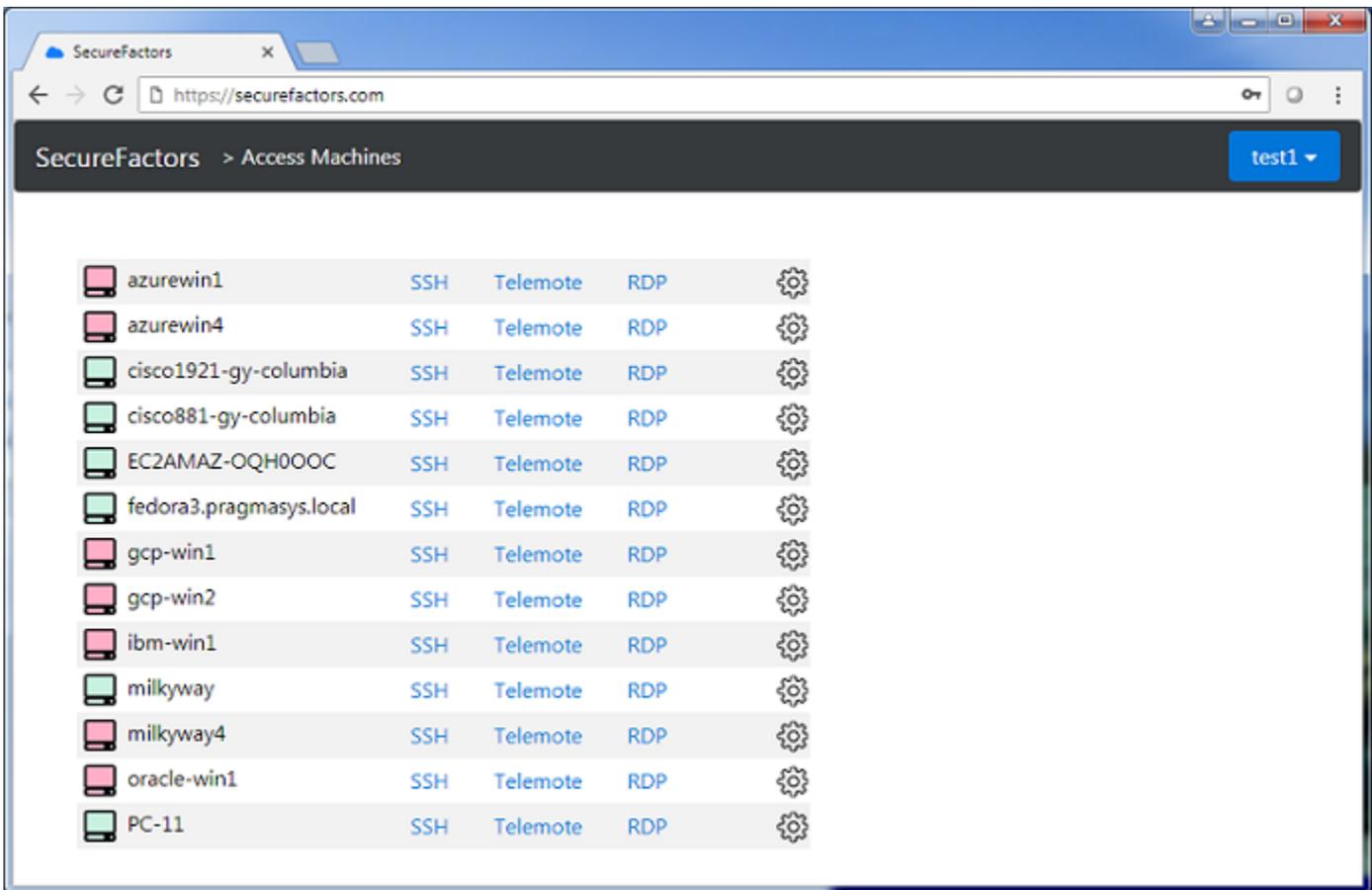
Save Changes Delete User



Six digit TOTP two factor is shown entered. The six digits are obtained for each login session by running Google Authenticator application in a mobile phone or device which has the account QR image listed.

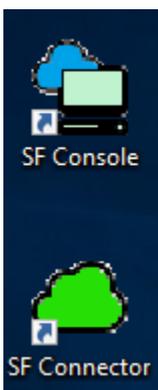
Once authenticated and logged into SecureFactors, one sees the machines that are connected to the SF account via SF Cloud. Choose "Access Machines" icon to see machines linked to an account. Choose "Key Manager" to enter SF KeyVault and manage SSH keys.

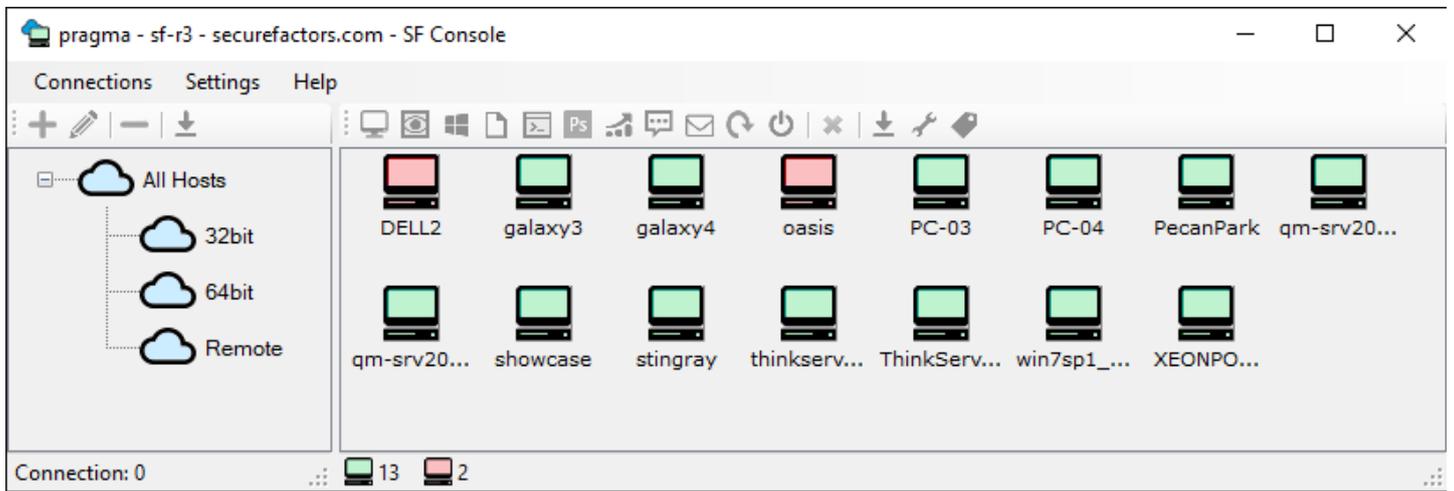




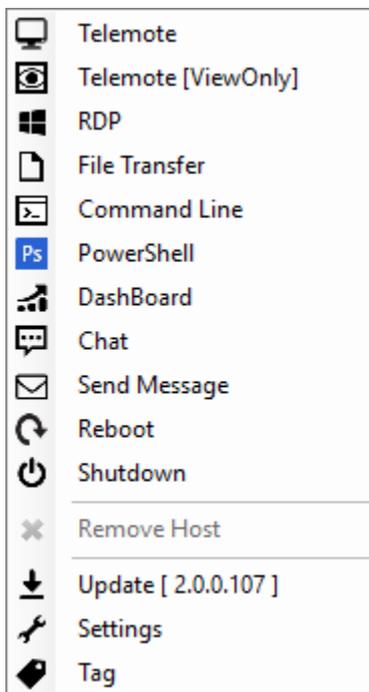
In Access Machines page, click Telemote or RDP verb to access that machine remotely. Telemote provides richer interface and features than RDP. "SSH" verb gives command line access to the machine to perform sysadmin tasks or run shell scripts.

For Windows systems, a SF Console application is additionally offered. For remote systems that need finer graphics and screen control than available from a web browser, one would use this SF Console Windows application. SF Console application is downloaded from securefactors.com and installed in a Windows machine. Once installed, double click "SF Console" to launch it. Then login to an SF account from "Connections" drop down menu. Use with the same credential used for browser based logins to login with Windows SF Console. After login, all machines connected to the account will be visible.

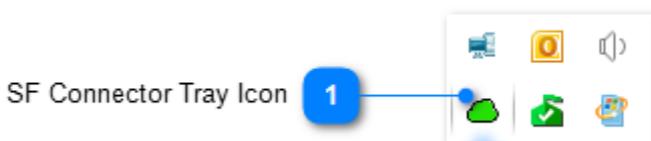


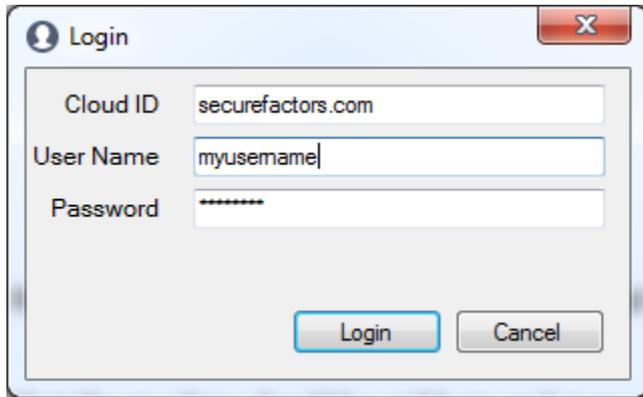
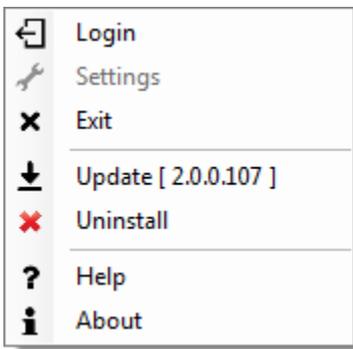


In Windows SF Console, right clicking on a machine shows all actions that can be performed on the machine and permitted: Full graphical access to the remote desktop (what we term "Telemote"), Microsoft RDP, remote PowerShell session, FileTransfer, Command Line session, DashBoard sysadmin interface, Reboot/Shutdown, Updating the SF Connector remote software, Reboot & Shutdown. Telemote is available for all platforms. RDP is available for Windows machines only.



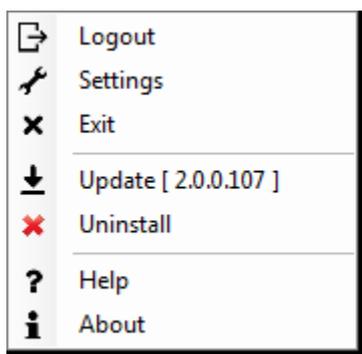
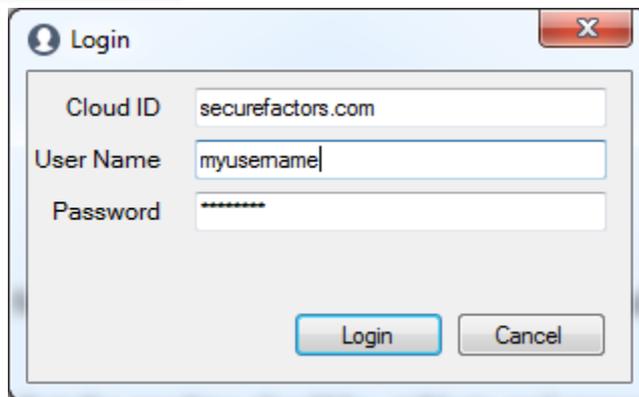
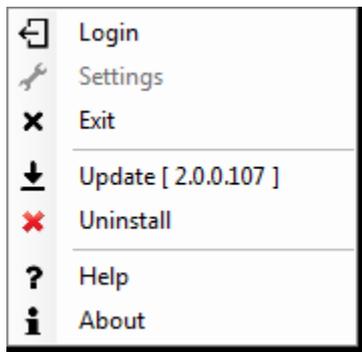
In each of the machines to be managed, you need to provide the SF cloud account name and password that the machine should be visible to. This has to be done just once by double clicking "SFConnector" desktop icon and selecting Login menu in the SFConnector Tray icon UI as shown below. Cloud ID is securefactors.com or where your site administrator has hosted your SF Cloud.





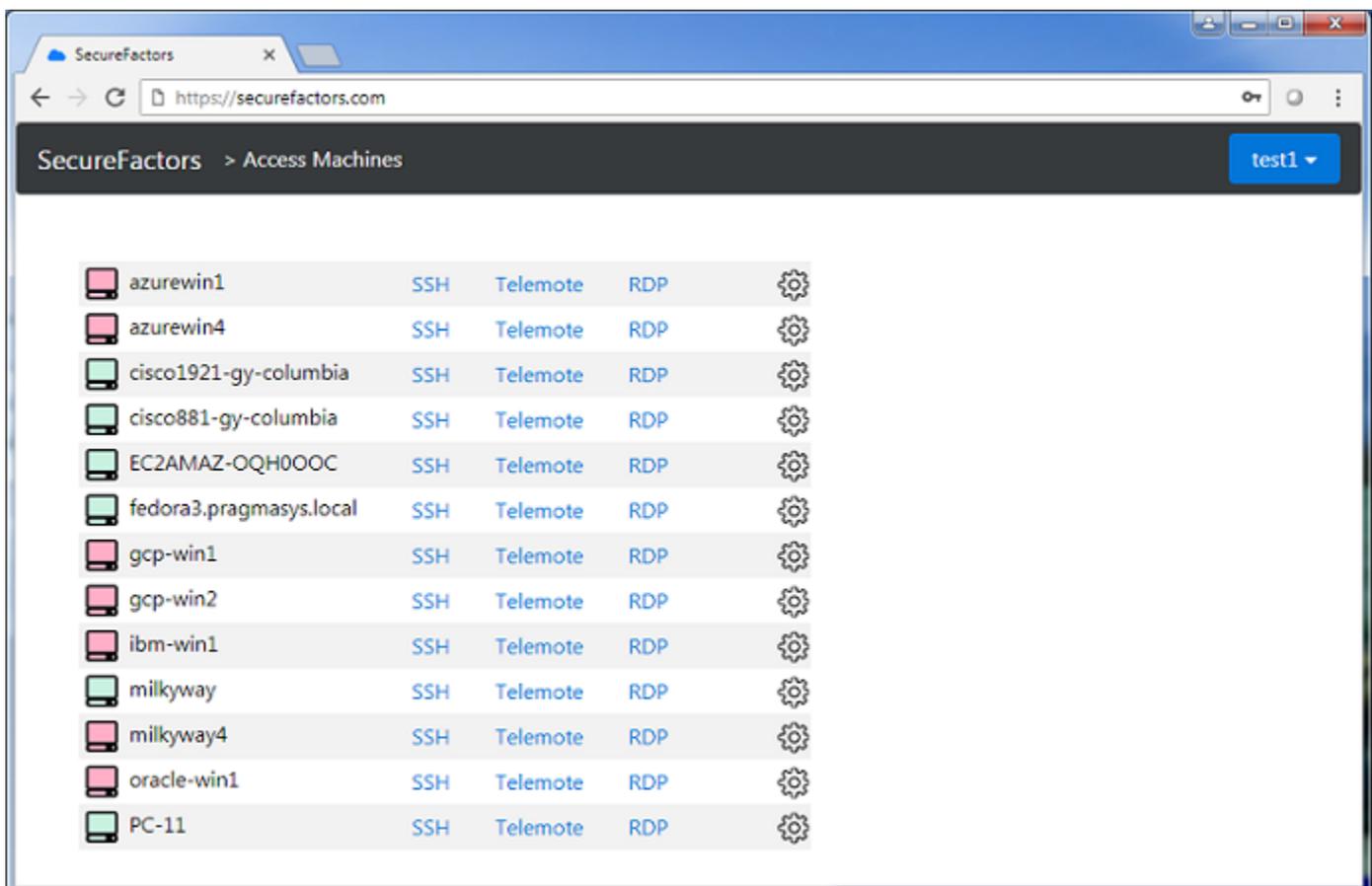
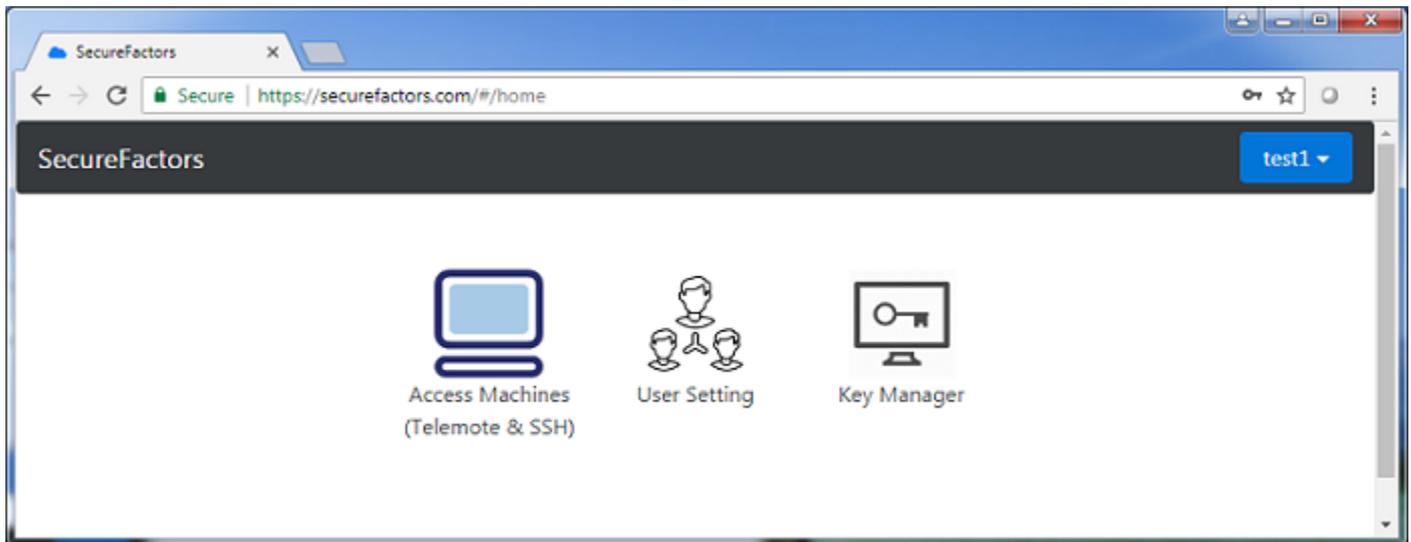
SF accessed systems

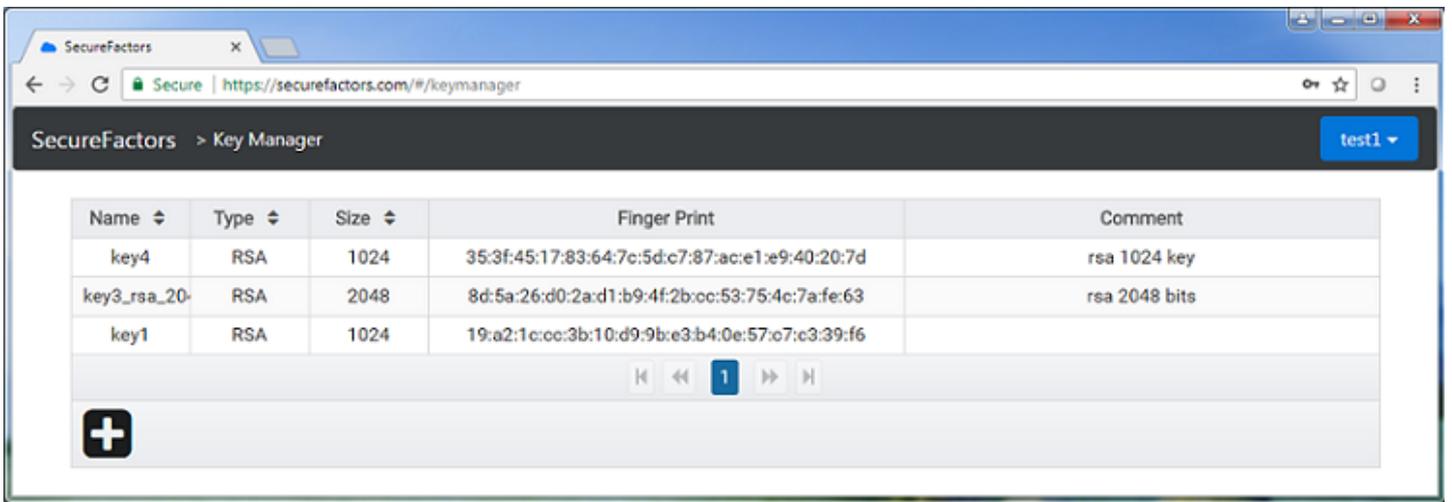
All systems needing to be accessed or managed run "SFConnector" small piece of software, which securely pulses to the SecureFactors cloud to an assigned SF account. This process makes the node visible and manageable from a SF Console (both browser based or .NET version). A system can pulse to only a single SF account which is provided during the first run but can be changed by clicking the SF Connector tray icon. If a system is not connected to the cloud, double click the "SFConnector" icon to start it or right-click the tray icon for it to get to the Login menu to activate login providing the SF username and password if it has not been provided before. Unless one needs to change it, this authentication information are stored securely and never has to be provided even after reboot. Thus this node or system becomes a fully remotely accessed and managed SF system. All activities, including updates of the SF Connector software, can be done remotely from a SF Console. In the CloudID field, type securefactors.com or CloudID provided by your site administrator (e.g. azure.securefactors.com, oracle.securefactors.com, aws.securefactors.com, google.securefactors.com, ibmcloud.securefactors.com, etc. are other possible CloudID). CloudID should be where your SF cloud account was created.



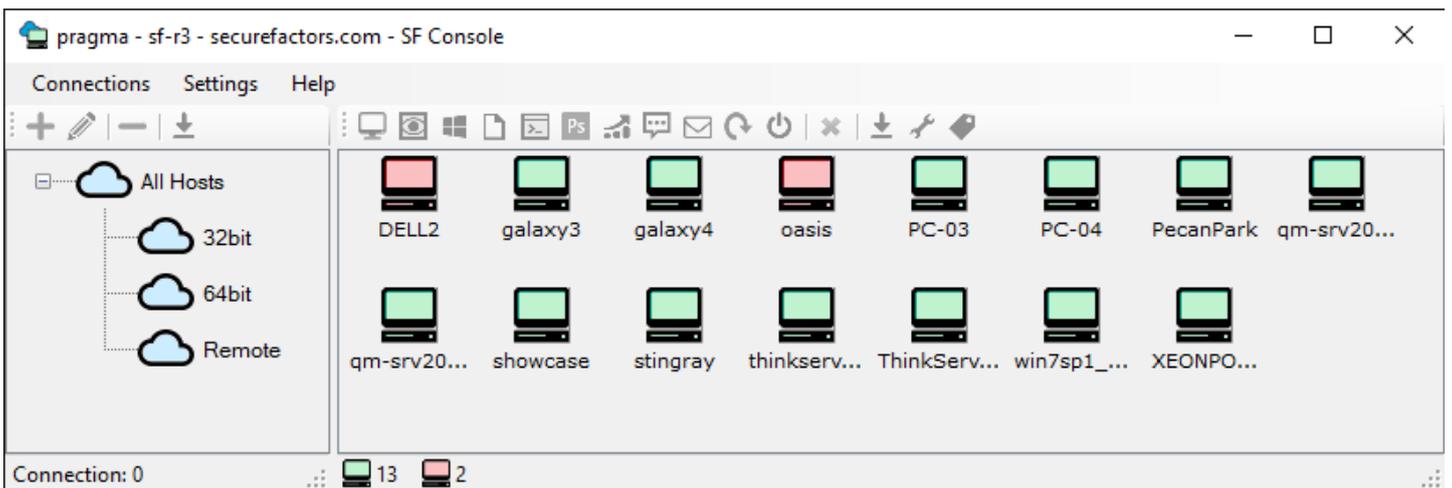
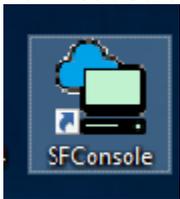
SF Console

Users or systems administrators doing remote access, run a web browser and login to their cloud account to run browser based SF Console. Browser based access is the primary way to access and run all SecureFactors functions and features. Access Machines, User Setting and Key Manager (SF KeyVault) are the three entry functions in web SF Console.

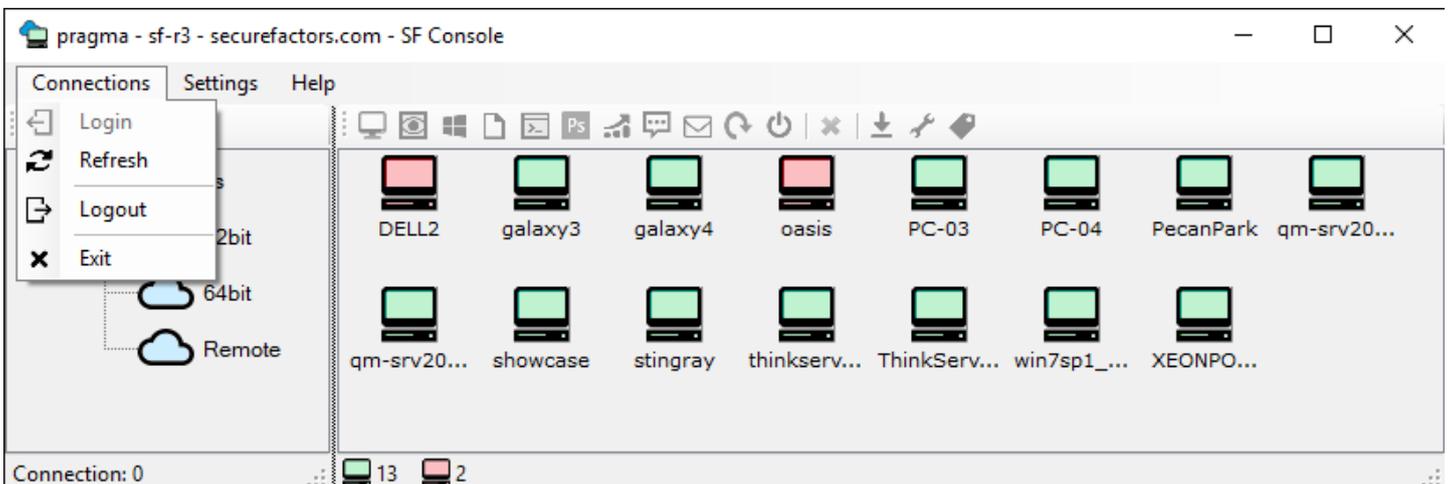




To run the Windows version of SF Console, double click its icon on the desktop after SF Console application is downloaded and installed.

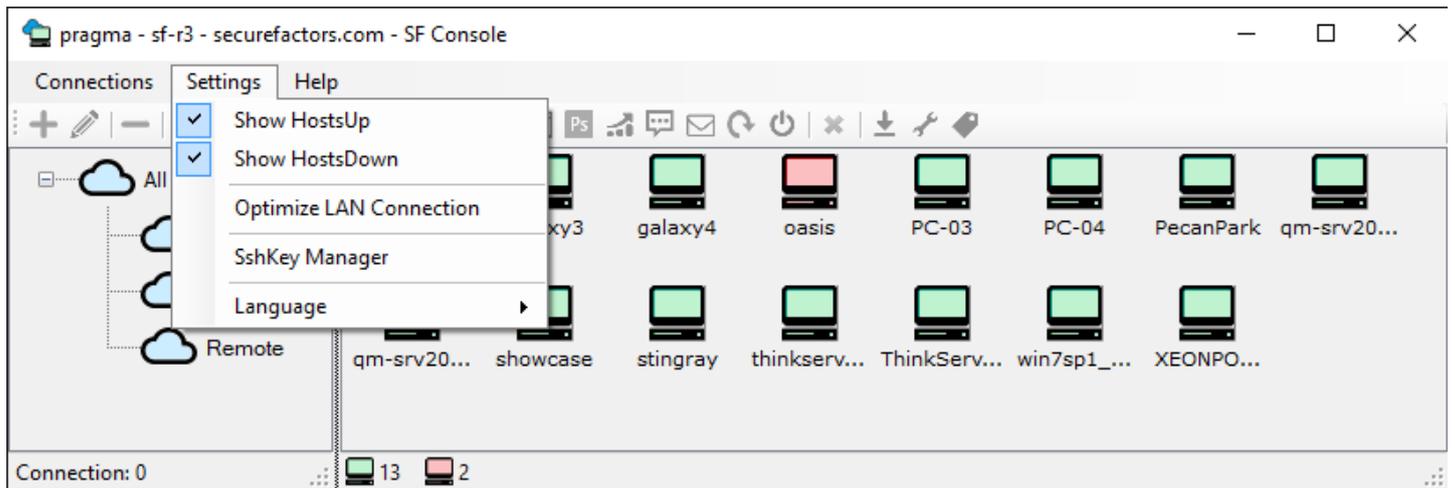


Provide the username and password in the "Login" menu of the "Connections" menu drop down. Enter the two-factor when prompted.

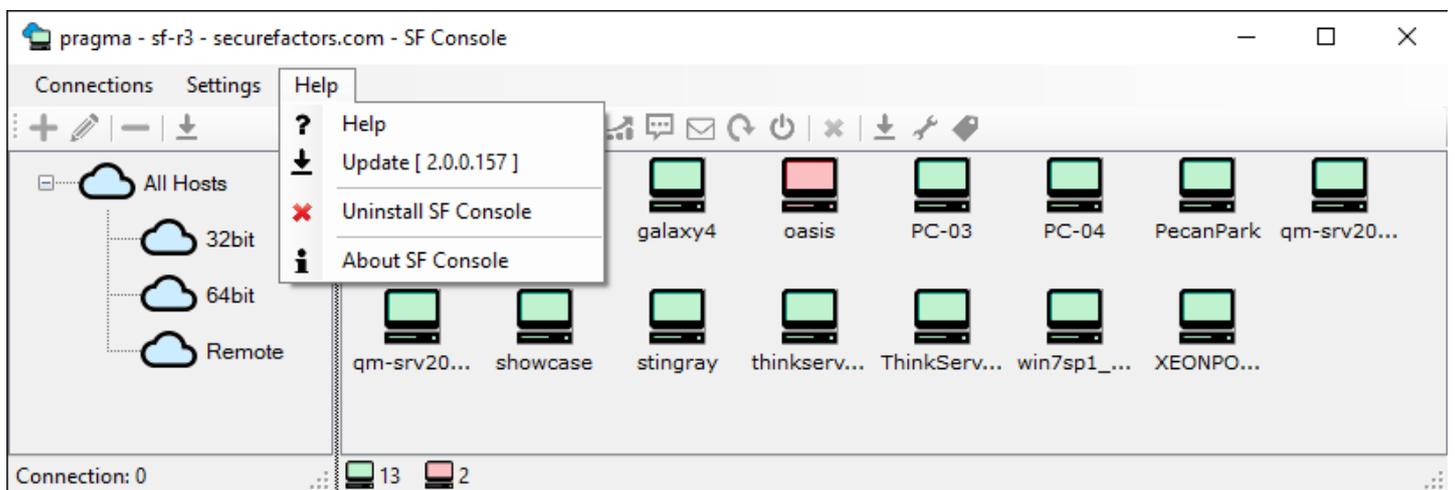


Various settings can be changed in the "Settings" menu drop down. "Optimize LAN Connection" is an importing setting turned on by default that reduces cloud traffic by sensing that a managed machine is on

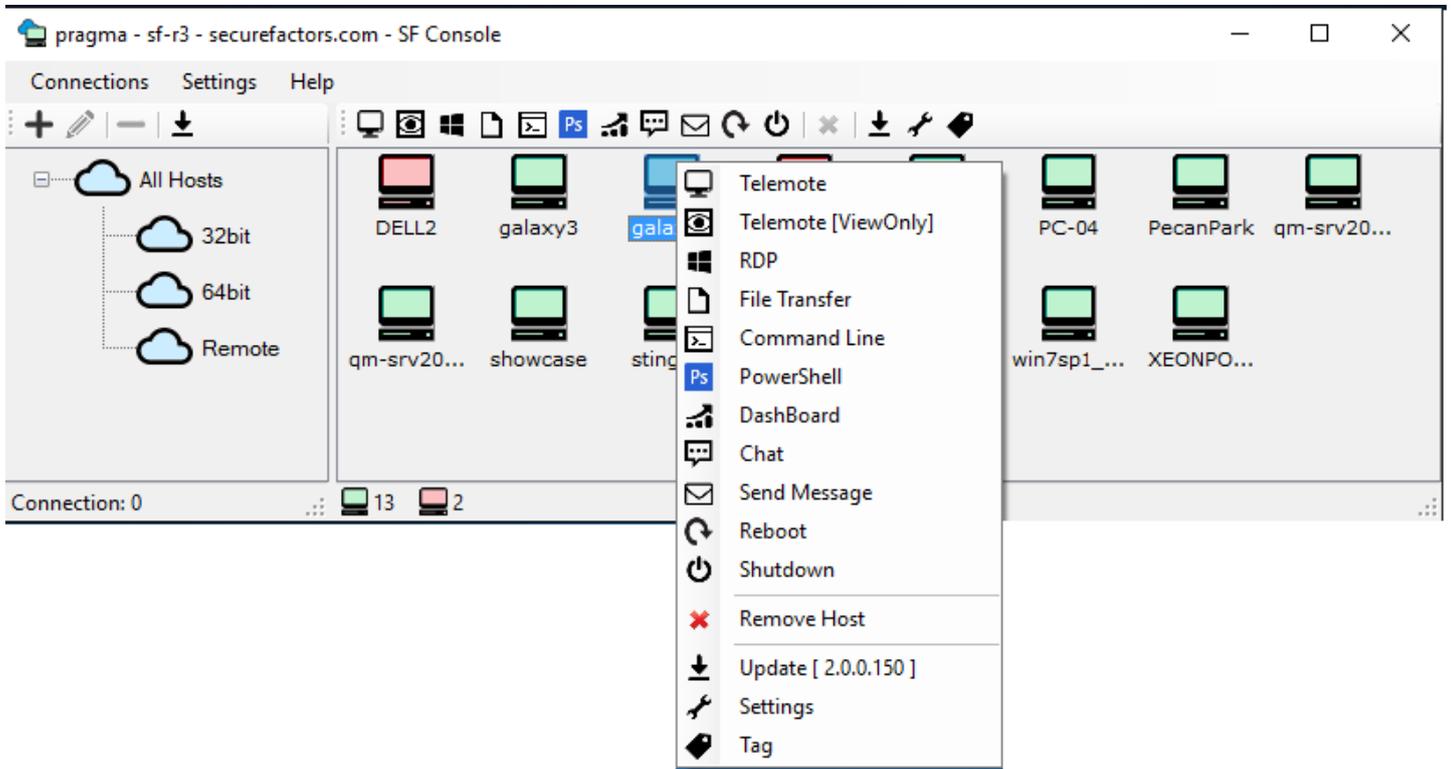
the local LAN and if so would send data to it directly (but encrypted and secure), thus speeding up access.



Help drop down provides SF Console software update and uninstall option as well as on-line help.



Right clicking on a machine shows all actions that can be performed on the machine and one can execute any action that is permitted. Full graphical access to the remote desktop (what we term "Telemote"), Microsoft RDP, remote PowerShell session, FileTransfer, Command Line session, Dashboard sysadmin interface, Reboot/Shutdown, Updating the remote SF Connector software - all IT and DevOps management tasks can be performed on the remote machine.



Tag a Machine

SecureFactors brings "photo tagging" like ease into machine tagging to organize machines into groups and sub-groups. Machines can be organized into tagged groups and sub-groups on the left pane for ease in management. Right-click a machine on the right pane to "Tag" it just like photo tagging. "All Hosts" is the root group that is created automatically by SF and will always contain all machines pulsing to that account. Right-click "All-Hosts" and then select "Add" to add a new tag group underneath "All-Hosts" that you can name. Tagging group and subgroups can be created this way by right-clicking any group or sub-group with unlimited level of nesting allowed. Below shows tagging of a machine named "galaxy2" which is tagged to be in "Servers" and "64-bit" groups. Clicking check-mark will add the machine in that group or take it away from that group if it was marked before.



Right-clicking a group on the left pane, one can run actions on all machines in that group. For example, "Update" verb on that group will mean all machines in that group will be updated with the most recent release of the SF Connector software, all done remotely and in parallel. This allows zero-touch remote management of SF machines spread throughout an enterprise/geography/cloud-infrastructure once the first versions of SF are installed.

