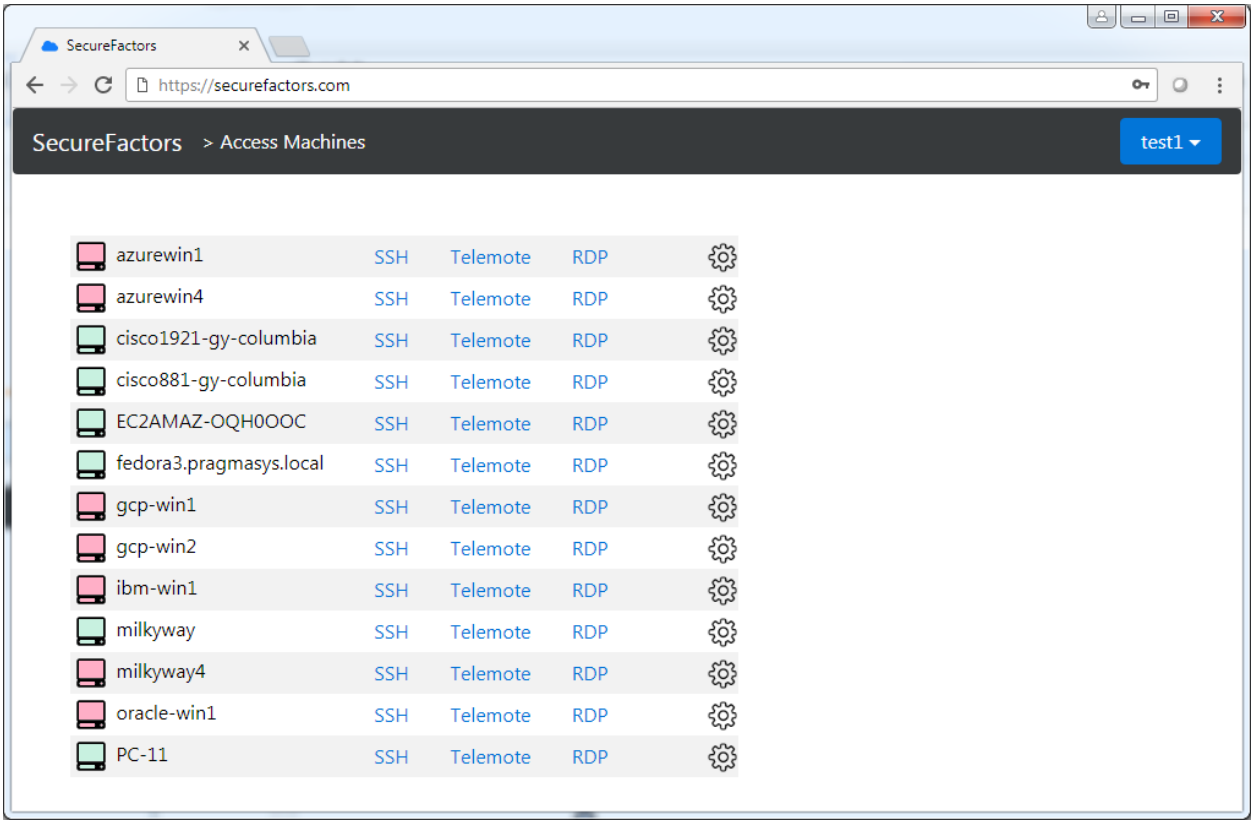
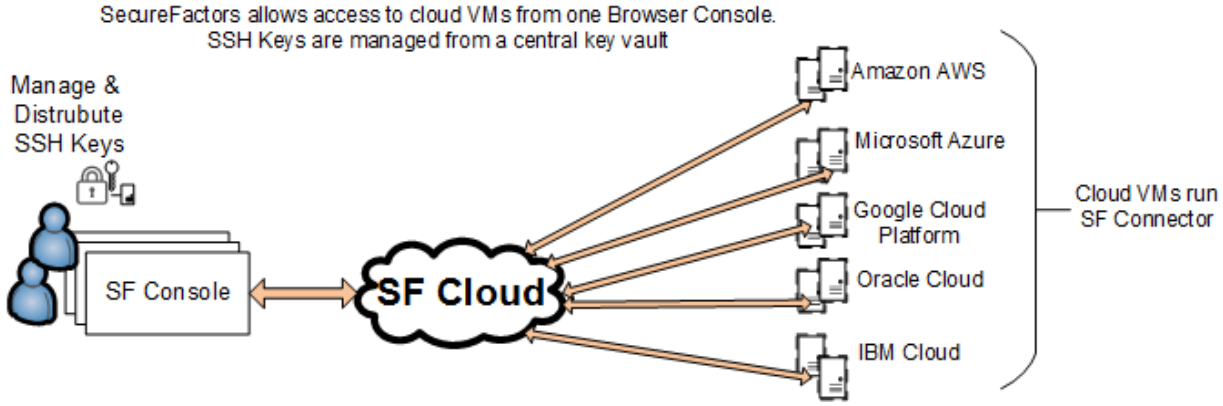
SecureFactors -- Cloud based Secure Access



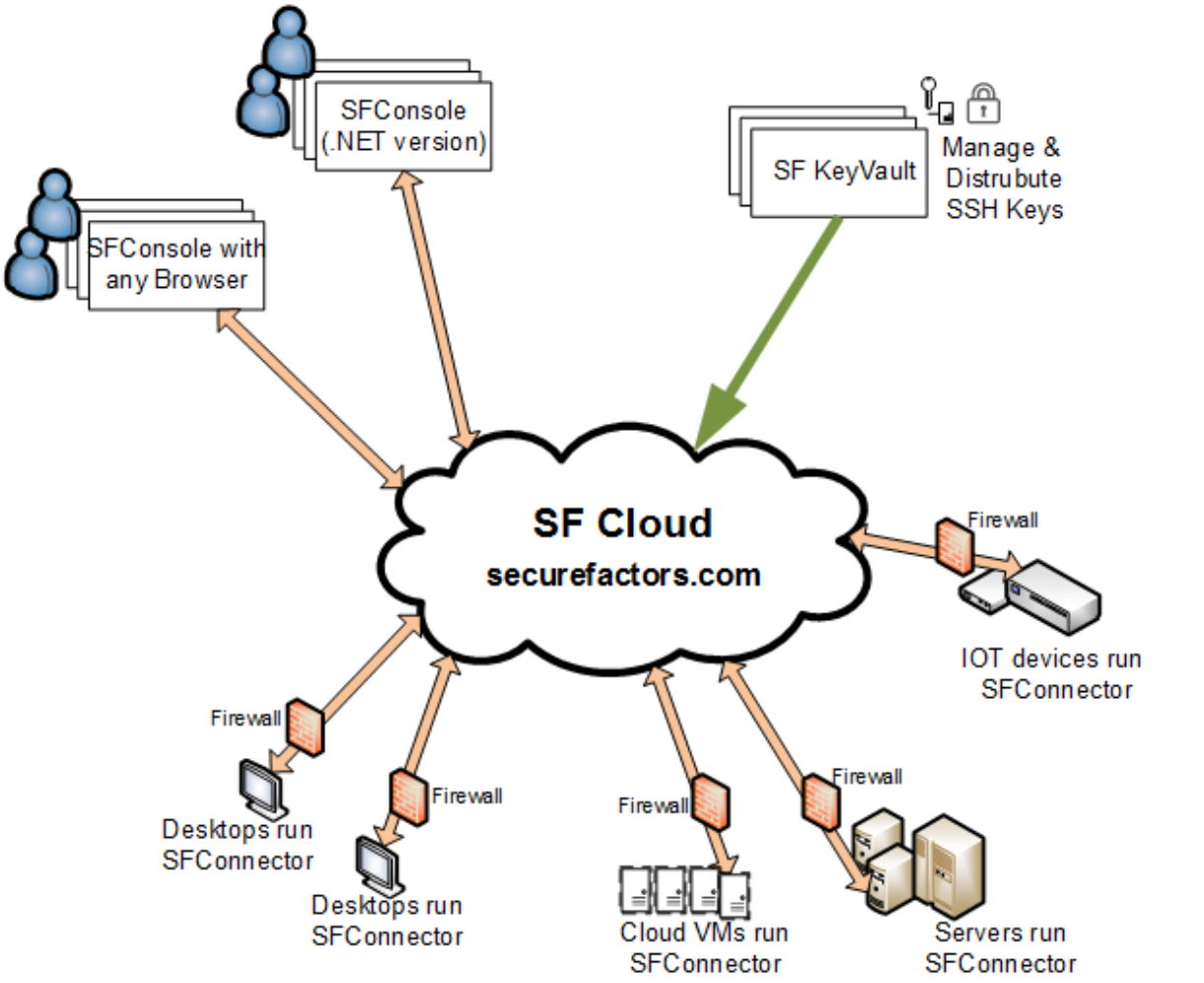


Background: Many traditional IT services and tasks are being reimagined and reinvented to make them work easier, efficient and lower cost using modern technologies like cloud platform, REST APIs and HTML5 browsers delivering to any size devices. Slack is an example of doing it for team messaging collaboration instead of traditional emails or old style collaboration software. SecureFactors reimagines remote access & systems administration. We have developed a secure platform to make access tasks incredibly easy for both IT enterprises and cloud based environment. One needs just a web browser to access. No software to install. No VPN needed.

The core of SecureFactors is a new scalable cloud platform, SF Cloud, that is hosted in a public cloud or in-house in a company's data center. SF cloud platform takes machine geography limits away – machines can be behind corporate firewalls or virtual machines in a cloud. Machines to be accessed run a thin cloud connector software, SFConnector, and securely pulse to a SFCloud. SF Connectors are available for Windows, Linux, Mac and IoT systems (Rasberrypi & Windows IOT) allowing accessing of a wide variety of systems or end-points.

Using SecureFactors is easy. Any modern web browser can be used to access remote machines. No software is needed to be installed and no browser plug-ins are needed as we use modern HTML5 and javascript platform to render all access applications in a browser.

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



To use SF, login using a browser and SF account credentials. Once logged in, one sees the machines and end-points that are linked to that account. Click the action verb you like to use. Verbs supported are SSH command line, Telemote (remote desktop access like VNC but more advanced) and RDP (Microsoft Remote Desktop Protocol). SFTP secure file transfer and Digital Key Management are two other verbs that are very handy and available.

Architecture: The three core pieces of SecureFactors are:

1. **SF Connector**

   A small piece of software that runs in each systems to be managed. This software piece pulses to the cloud and allows access from remote authorized systems. Additional software pieces embedded in the connector are SSH, SFTP and Telemote servers for Windows or similar components needed for non-Windows systems.

   Download the connector from securefactors.com that is applicable for your operating systems and install it. SF Connectors are available for Windows, Linux, Unix, Mac, RasberryPi, Windows IOT & other IOTs.

2. **SF Console**

   Any web browser serves as the SF Console, no software is needed to be installed. All remote access and functions can be performed from the SF Console. The web browser based console is the primary user interface for SecureFactors for both users and systems administrators.

   Additionally, a SF Console application for Windows is offered for customers who want to use highly graphics intensive applications in their remote systems (e.g. Medical radiology imaging applications) which need higher precision than offered by web browsers for screen rendering. SF Console application can be downloaded from securefactors.com web site and installed in Microsoft Windows systems. Login and access of remote machines operates the same way no matter which SF console one uses (browser based or Windows version).

3. **SF Cloud**

   SF cloud platform is a core piece of our invention. It is a new, modern, scalable, switchable, robust cloud platform that can run on bare metal hardware and is built with our cloud intellectual property (IP) code and proven modern web technologies. Linux, MySQL, AMQ messaging systems, Tomcat application framework, Java and REST APIs are used to build SF Cloud. Our cloud and IP is fully tested to run on our own data center servers or in Amazon AWS, Microsoft Azure, Google Cloud, IBM Cloud and Oracle Cloud, giving customers the choice where to host their SF Cloud. SF Cloud's current architecture only needs VMs or bare metals of a cloud provider or a customer data center. This configuration flexibility is one of the hallmarks of SecureFactors and is a key advantage compared to our pre-cloud era competitors (LogMeIn, TeamViewer, ServiceNow).

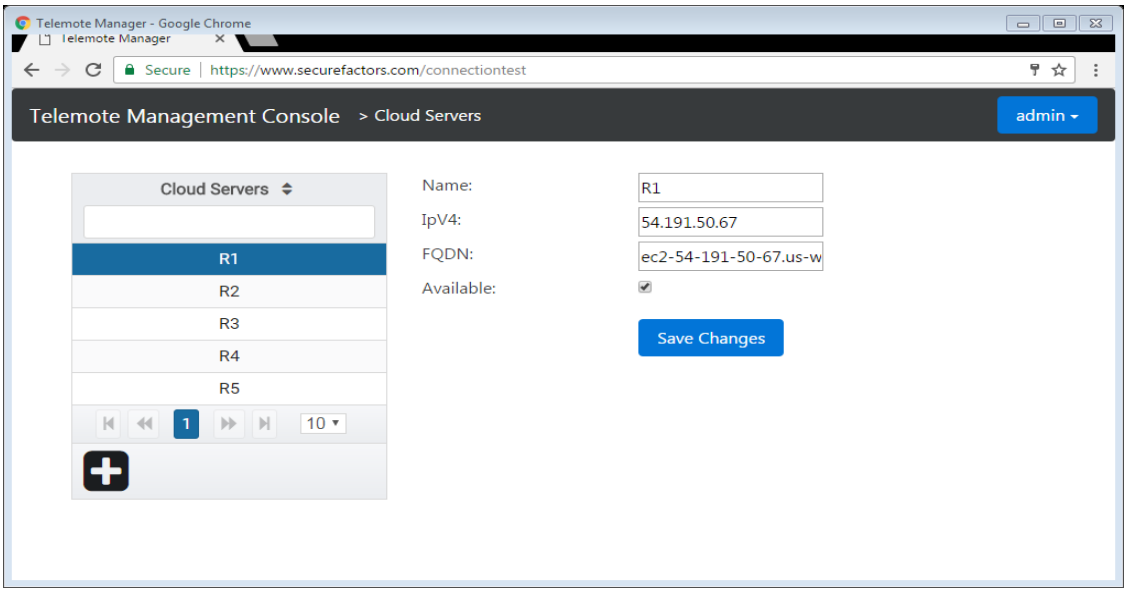
   Users access securefactors by creating an account in SF Cloud and providing billing info (credit card that we will charge monthly or annually) for payments to be charged. Then SF Connector needs to be installed in machines to be accessed and seeded with the user's SF account credentials. Login using SF Console and one will see all machines that are linked to the SF

account. Perform desktop access, application running, file transfer, sysadmin, SSH command line and DevOps tasks securely from anywhere without any VPN. SF Console provides access to your systems and applications securely with just a web browser.

SF cloud architecture allows cloud and data partitioning for maximum operations flexibility and customer deployment security needs. SF Cloud can operate in a private cloud, public cloud or in an enterprise data center. General customers are served by our farm of servers working behind ***securefactors.com.*** Customers needing a preferred major public cloud provider can choose from one of these five: ***azure.securefactors.com, aws.securefactors.com, google.securefactors.com, oracle.securefactors.com*** or ***ibmcloud.securefactors.com***. Licensing is also offered to large customers to host SF in their own cloud or data-centers.

An inside view of SF Cloud Platform

Here we provide a short internal view of our cloud platform. Our actual operating servers are called “R” servers. For our primary cloud, we have deployed a good set of core servers to which we add/deduct servers as customer use increases/decreases. For our own data center based cloud, we use N “R” servers of Dell PowerEdge 630 class allowing N x 1000 user accounts. More “R” servers are added as our user base increases. New “R” servers are imaged with our Docker package and simply added to our cloud via listing in the “R” server list in our SF Network Operation Center (NOC) web console with the “R” servers IP address listed. Every “R” server needs a public IP address. These “R” servers can be bare metal servers in our own data center or located in Amazon AWS, Google GCP, Microsoft Azure, IBM Cloud or Oracle Cloud. Below shows an AWS server added as R1 server through our SF Management Console NOC web application.



SF Network Operator Console (NOC)

SF NOC is an AngularJS2 based web application that is used to perform all DevOps functions to build and operate securefactors.com public cloud or xyz.securefactors.com sub-cloud or private cloud. NOC is meant for use only by our own operators or large customer accounts who need to manage their own users and “R” computing servers. Operators logon through their “admin” level accounts which are created by the first seed admin account.

Fig. SF NOC main entry showing various functions to run to operate SF cloud

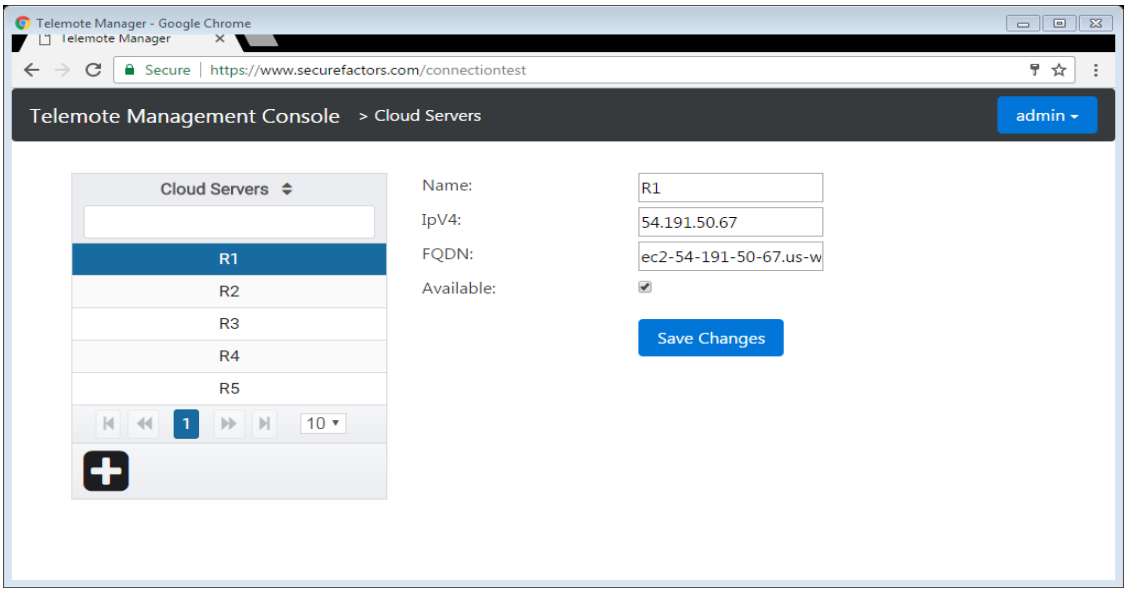
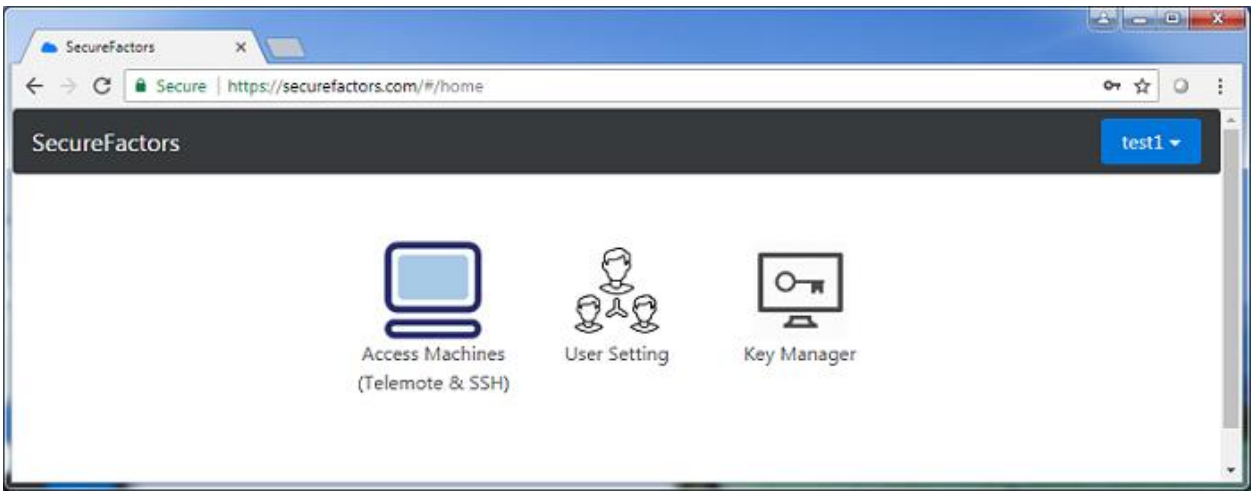


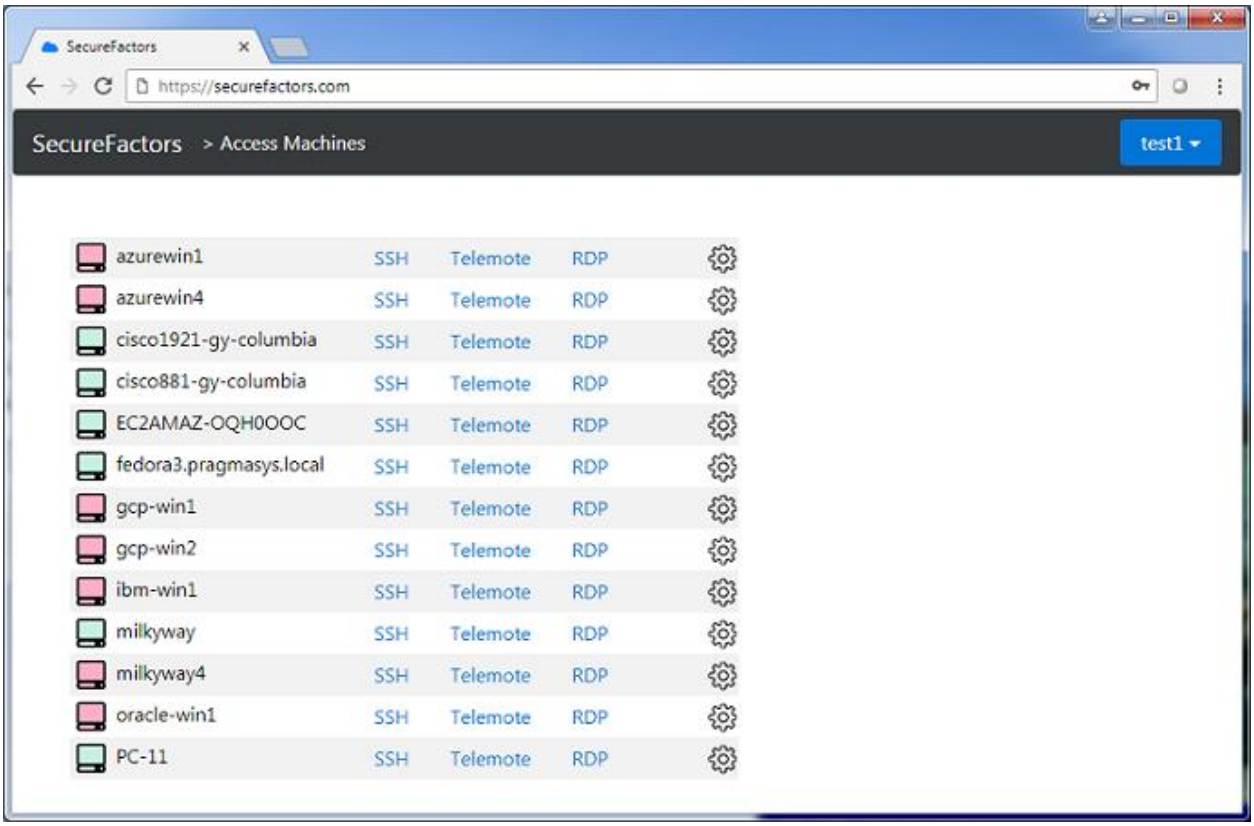
Fig. SF NOC to manage R computing servers of SF cloud. Here R1 is an Amazon AWS node

SF Console

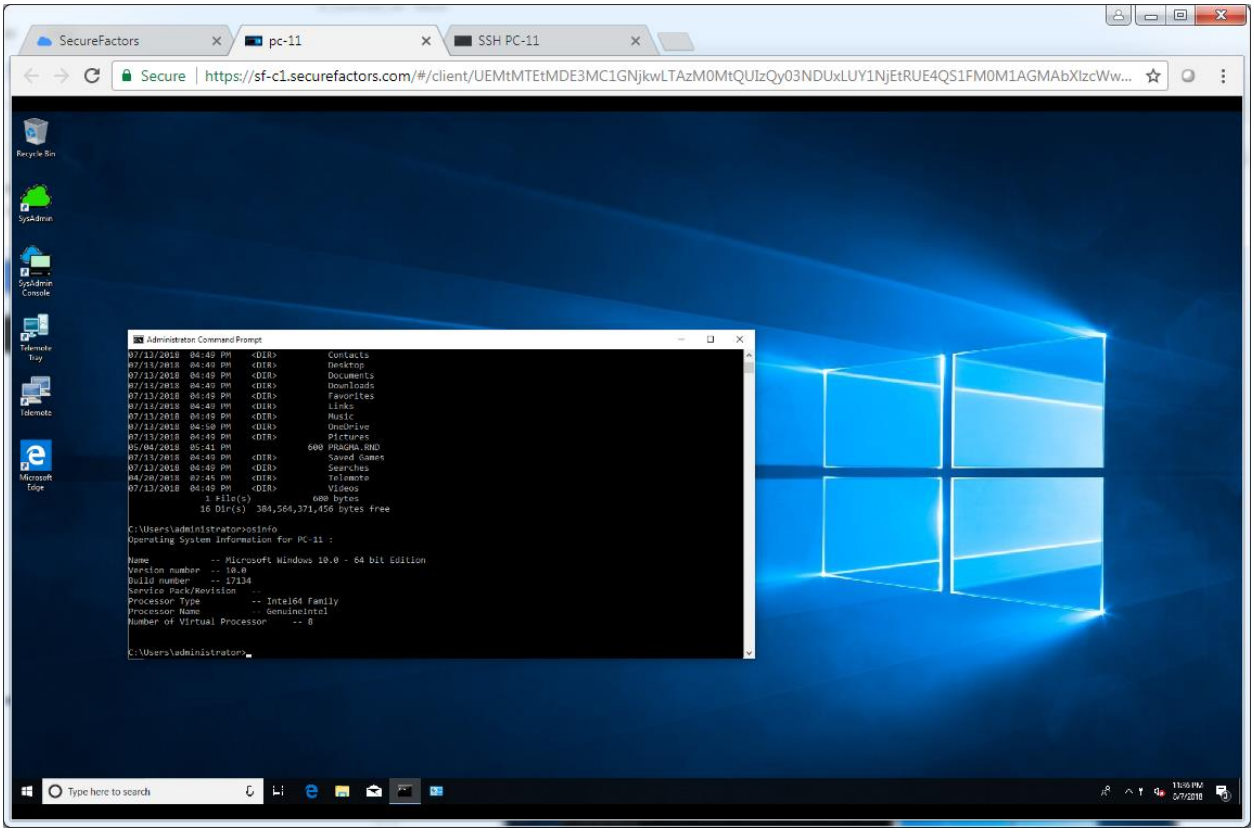
Users view the systems they can access with a web browser which operates as an SF Console after login. SF Logins are done typically with two factor authentication for tighter security. After login, select “Access Machines” to see the machines that can be accessed. User Setting and Key Manager are other choices available for changing account information and entering SF KeyVault to manage SSH keys.

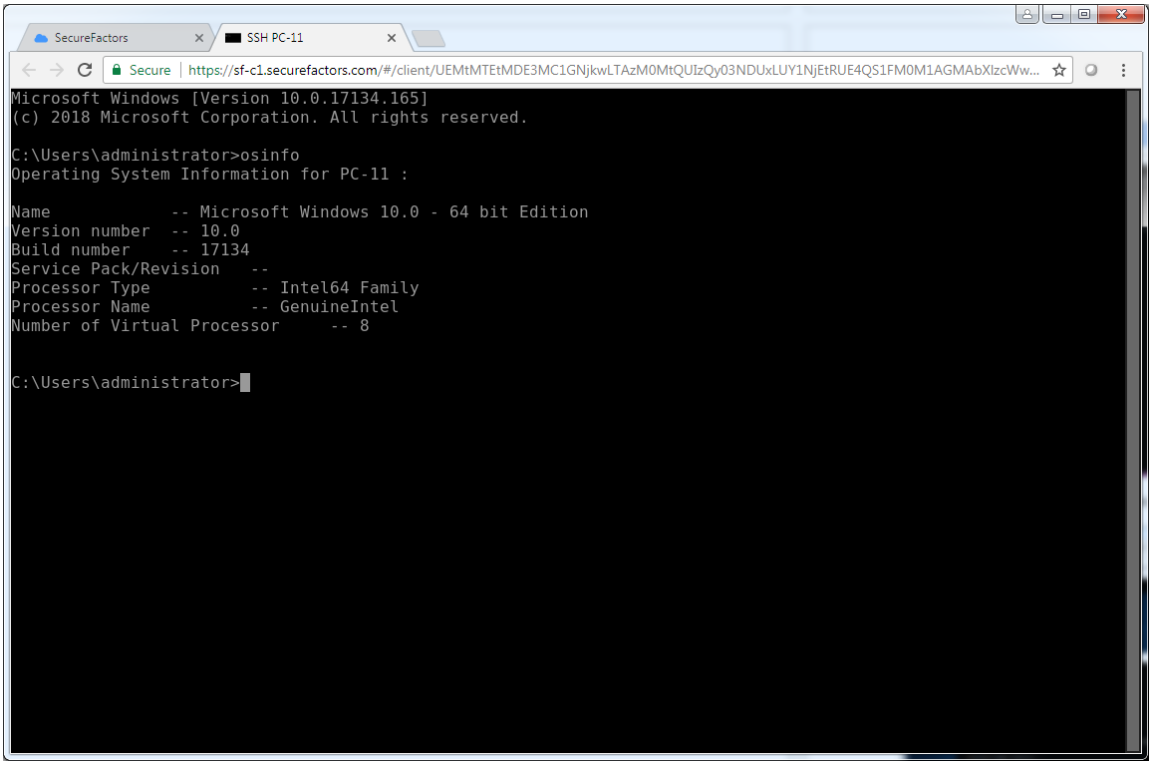


Green colored machines mean active systems. Red colored machines mean machines not connected.

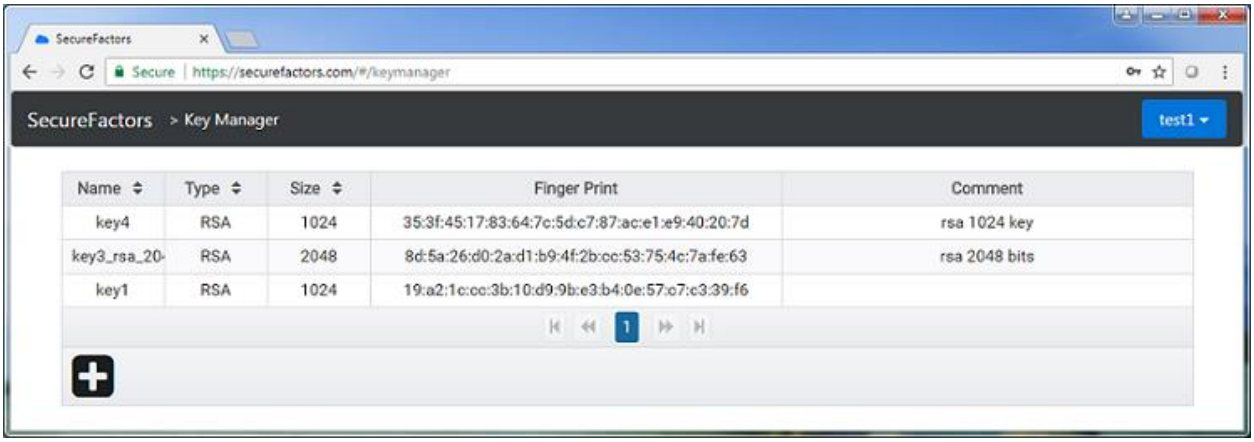


Click Telemote or RDP for a remote screen session. Click SSH for command line session. Each session will be opened in a tab in the browser. Close a tab to end that session.





SF KeyVault manages full life cycle of SSH keys for users storing them in a secure cloud vault centrally. But the keys can be used anywhere in SF Cloud securely.



SF Console app version for Windows

For users needing access to SF connected machines with features not currently available in our browser (e.g. monitor selection in multi-monitor systems, machine tagging to create groups), we provide a full-featured .NET SF Console that runs in any Windows systems. SF Console is downloaded from securefactors.com site. Users view the systems they are managing by double clicking SFConsole icon in the desktop and then login with a SF account credentials. Green colored machines mean active systems. Red colored machines mean machines not connected or not accessible through the cloud.

Machines can be tagged like “photo tagging in Facebook” to group them into category groups shown on the left pane for easy navigation and organization when the number of machines get large. Right-click to access its action verbs to invoke (SSH, Telemote, RDP, FileTransfer, PowerShell, Dashboard).

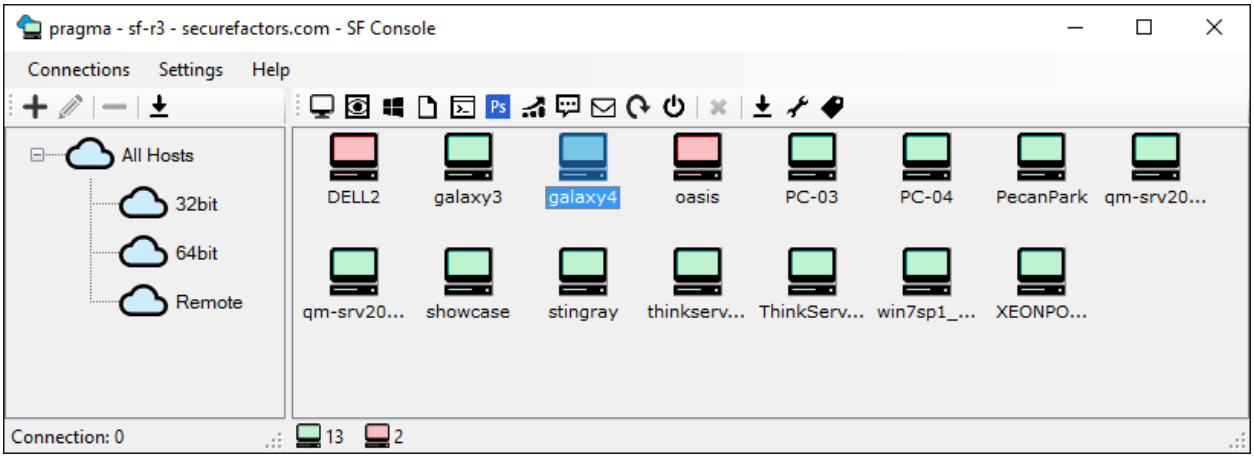


Fig. SF Console .NET version shows the machines linked to the account that can be accessed