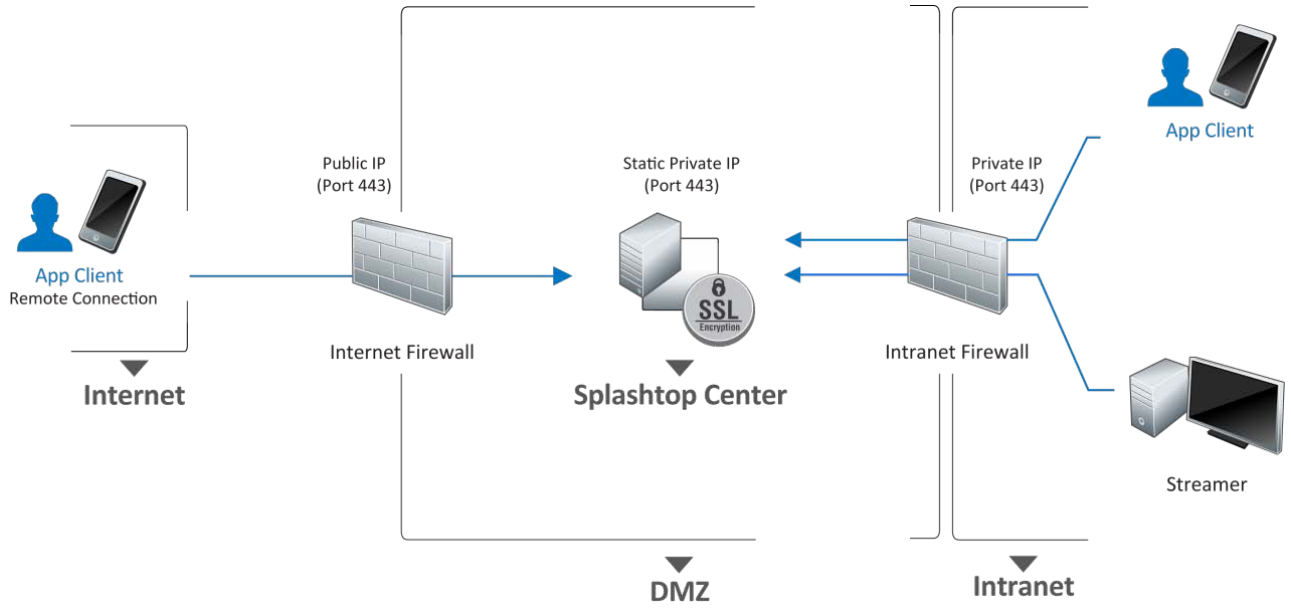
Introduction



For information about different deployment choices, please see chapter 3 of the full "Splashtop Center Administrator's Guide."

This product is comprised of three components:

(1) **Splashtop Center** is the central server that authenticates, secures, and connects users and devices. It also offers a console to configure and report on users and devices. It is installed on a Windows server.

(2) **Splashtop Streamer** streams audio and video to the mobile device and needs to be installed on all target computers that you want to be available for remote access.

(3) The **Splashtop Enterprise** app makes it possible for users to connect their mobile device(s) to the target streamer/computer remotely.

Splashtop Center Features

Splashtop Center allows enterprises to deploy management of enterprise-level remote desktop services to a private cloud environment. Following is the feature list of Splashtop Center.

Basic

- Gateway: Connect clients and Streamers.
- Relay: Supports cross-firewall connection.
- Multi-device support: Supports iPad, iPhone, Android tablets, Android phones, Macs, and PCs.

Security

Data Protection

- Secure session: Supports SSL certificates.

Authentication

- User authentication : There are 2 types of users.
  - Gateway users will be authenticated by Splashtop Center.
  - Domain users will need to go through the AD server for local authentication. Active Directory required.
- Device management: Supports device activation for client devices to gain access.

Tracking

- Session monitoring: Monitor employee usage to see which mobile device is connecting to which computer, time of connection, and duration of each session. View real-time connections and audit trails.
- Log/Reporting: Exportable log for auditing.

IT Manageability

- Centralized control: Set user and device access policies, activate/de-activate users and devices, create or import SSL certificates.
- User management: Add or delete user accounts. Add new users individually, or add multiple users all at once by importing a file. Reset user passwords.
- Automatic Email notification: Email will be sent to users automatically to make it easy for them to activate their mobile devices — the IT Administrator doesn't have to write it.
- Computer grouping: Set up a group to provide a pool of identically-configured computers for your employees.
- Manage Streamer updates: IT Administrators can easily manage new versions of the Splashtop Streamer, using the **Software Update** tab of Settings. It also allows you to silently push the update of the Streamer into users' computers. More importantly, you can schedule the forced-update to take place automatically after-hours or at any convenient non-peak time.
- IT Policy Control lets you more conveniently configure settings/permissions for each user.
- Backup: Import/export all configurations.

Applications and Desktop virtualization

- RDP Connector: Our new SplashApp/**RDP Connector** option is ready for remote application delivery. This option allows you to use RDP (Remote Desktop Protocol) for remote connection using Splashtop Enterprise clients and to share access via RDS (Remote Desktop Services). Details about this can be found in sections 5.5, 5.6, and 6.8 of the complete "**Splashtop Center Administrator's Guide**."

High availability

- Keep your Splashtop Enterprise running: We have devised a specific configuration that we call "High Availability," which is intended as our suggestion for setting up a Splashtop Center fall-back system to keep it up and running in case of unforeseen lost connection. That is, if your main Server running Splashtop Center goes down, the backup Server you set up (using our "High Availability" instructions) will take over, so you can keep using Splashtop Enterprise with no interruption in remote connection service (and ideally no loss of data). For complete details, please see our *separate document* entitled "**Splashtop Center High-Availability Setup Guide**."

User accessibility

- "User Portal" — As your Splashtop Center Customer Portal, the Splashtop Center Web Interface provides this "Web portal" web page for an alternative way to change passwords, download Splashtop Enterprise applications, and optionally to set up SplashApp/RDP Connector. After you have logged in, you will have at least two tabs always available — **Password** and **Downloads** — even if you have not obtained the RDP Connector option (AD Domain users only have the **Downloads** tab). Please see Chapter 5 of the complete "**Splashtop Center Administrator's Guide**."for how to log in, and other details.

Energy Saving

- A "Wake Up This Computer" function is provided, to allow a user to wake up the target remote computer from a sleeping state. That is, Splashtop Center will wake up the Streamer on behalf of the client, provided the computer supports WoL (Wake on LAN) and the option has been enabled, and that the computer is connected by Ethernet, not WiFi.

For more details

- For more information , please visit our **Splashtop Enterprise web pages** at: www.splashtop.com/enterprise

- For the full "**Splashtop Center Administrator's Guide**" in PDF format, which provides complete information about the functions of Splashtop Center, please go to the "**Downloads**" tab in our Splashtop Center Web Portal page at: http://support-splashtopforbusiness.splashtop.com/home Please note that User Registration is required for login to **Download**.

- For **Help**, **Frequently Asked Questions**, **Community Forums** and **trouble-shooting tips**, please visit "**Knowledge Base**" also found at the above URL address.

Setup Overview

In the list below, the rightmost column shows the section number(s) in the complete" **Splashtop Center Administrator's Guide v1.7**," where you can find more details about the related step. (The **System Requirements** section begins on page 9 of this Quick Start Guide.)

Step no.	Performed by:	Tasks to be performed:	Ref. section in Admin Guide:
1	IT Admin.	Installs and sets up Splashtop Center on the company network. This includes activating the License Key, preparing an IP address and TCP port (port 443 by default) for Splashtop Center, and importing or generating an SSL (Secured Socket Layer) certificate.	2.3, 4.8.1, 4.8.2, 4.8.6, 6.1, 7.3
2	IT Admin.	Creates user accounts, and sends "Invitation Email" to all users to notify them that they have been added to Splashtop Center, and provides their activation code.	4.1, 4.8.1.1, 4.8.3
3	IT Admin.	Downloads the Streamer and installs it on all the computers which he or she wants to be available to users for remote access.	2.5
4	IT Admin.	Groups the computers as desired, and sets user permissions accordingly. To see an example, please refer to section 6.5, **Creating and Administrating Groups**, in the complete Splashtop Center Administrator's Guide. (Each computer in the group also needs to have the Streamer logged into using the IT Administrator's account, in order for users to remote-connect to it.)	4.5., 6.5
5	User	The user then downloads the Splashtop Enterprise client app to his/her mobile device, and installs it.	2.4
6	User	The user invokes the client app on his/her mobile device and logs in using the password given by you, the IT Administrator. The user must enter the activation code which you provided for the that mobile device, plus his/her Splashtop Center Email address and the Splashtop Center URL. The user can then make a remote connection to a computer.	2.4.1, 6.3

Installing Splashtop Center

NOTE: The **System Requirements** section begins on page 9 of this Quick Start Guide.

1. To begin, go to our *Splashtop Enterprise* web site at: http://www.splashtop.com/enterprise.

2. Click the **Request a Free 30-Day Trial** button, and proceed with sign-up accordingly. Once complete, check your Inbox for your "*Splashtop Enterprise — Customer Portal* Welcome e-mail." In the e-mail, click on the hyperlink to open our "Create Password" web page for your trial account.

3. Create the password you want to use for your *Splashtop Enterprise* trial account.

4. After entering your password, click the **Verify my e-mail address** button. This will open the **Download** page (hosted in conjunction with ZenDesk). Follow the instructions on the screen. (Note that in this screen, you can access the full "**Splashtop Center Administrator's Guide**" under **Documentation**. You can also click **Knowledge Base** to access the FAQ and other helpful documentation.)

5. Download your program and double-click on the EXE file to begin installing via the standard Windows InstallShield Wizard.

6. After the installation is finished, go to the License keys / Tickets page to retrieve the License Key which you will need in order to activate Splashtop Center. (The **License Manager** tab of the Splashtop Center Console window is explained in section 4.8.6 of the "**Splashtop Center Administrator's Guide**.")

NOTE: Alternatively, if you are a Trial user, you can activate/query the Trial license via the "First Time" Wizard during installation.

Installing the Splashtop Enterprise App

This is the App that is installed on the user's mobile client device, which makes remote access possible. We have used the iPad as our example mobile device in the steps below.

1. Find the **Splashtop Enterprise** App in the Apple App Store using your iPad. You can type "Splashtop Enterprise" in the Search box to find it.

2. Tap the **Splashtop Enterprise** icon or the **Install App** button to begin installing on your iPad.

3. After the **Splashtop Enterprise** App has finished installing, the user should have received some Invitation Email which contains an "auto-launcher link." If the user opens the Invitation Email on the target device for Splashtop Enterprise, he or she only needs to click on this link. Splashtop Enterprise will start, and the required information will be input into the fields automatically.

4. After entering the Splashtop Center URL or IP Address, the **Email** address you use in conjunction with **Splashtop Center**, and the Password (a "Set Your Password" screen will appear if you have not yet set up a password), tap **Log In**. If a warning message pops up when you tap **Log In**, telling you that your SSL (Secure Socket Layer) certificate is not from a trusted certifying authority, it is likely that the SSL certificate is self-generated, and you can choose to ignore it.

5. If you continue to get an error message stating "Account Login Failed; This product isn't activated," it means the IT department has enabled an option that requires users to activate Splashtop Enterprise on this client device before the **Splashtop Enterprise** App can be used.

6. If you log in successfully, you will either see a list of the computers that you are allowed to remote-connect to, using this iPad; **or**, you may just see a screen which does not list any specific computers. In this case, follow the instructions on the screen. You can also click the "**?**" button in the lower right corner of the screen for helpful tips, or click the "gear" icon in the upper right corner of the screen to open the **Settings/Options** tab.

If users have a problem at any given point during the installation, they should be encouraged to contact the IT Department for assistance.

Installing the Splashtop Streamer

The Splashtop Streamer is the streaming source for remote access. Install the Streamer on any computer that you want to make capable of being accessed remotely. Then users (who are authorized within Splashtop Center) can access the content of the host computer using their mobile device (client) running the Splashtop app. You, as the IT Administrator, will send Invitation Email to the users, and they will use that Email to do the Streamer installation themselves as explained below.

1. The Streamer is hosted in the Splashtop Center. When the user receives the invitation Email from you with instructions, he or she will click on the URL (https://sc_url[port]/html/getstreamer.html) in the Email to begin the download/installation of the **Splashtop Streamer**.

2. After the user clicks **Finish** to close the InstallShield Wizard window, the Splashtop *Terms of Service* agreement will display. You will need to click **Accept** to continue. The **Status** tab of the **Splashtop Streamer** window will then display.

3. The user needs to enter the Splashtop Center URL, Email address used in conjunction with Splashtop Center, and his/her password. This is the password that was entered when installing the Splashtop Enterprise App on the mobile device (in Step 4 of the previous section, entitled “Installing the Splashtop Enterprise App”).

- Splashtop Center and Splashtop Streamer can be installed on the same Windows server. In fact, this is a good idea because it would provide remote access to that server in case you need to change settings or restart the Splashtop Center service someday.
- Streamer now supports both Basic and NTLM authentication when connecting to a Proxy server.

⚠ You cannot have multiple **Mac** Streamers installed. If you already had any other version of Splashtop Streamer installed, the Installer will ask you if you want to uninstall it.

System Requirements for the three components

Splashtop Center — Server Requirements

Minimum requirements are listed in the middle column below. However, if you want a remote connection at optimal experience/performance, we recommend using the requirements listed in the rightmost column.

Splashtop Center

	Minimum requirements	Recommended Specification
CPU	Intel i5 2.0Ghz or above	Intel i7, Xeon E31220, or other high-end CPU
RAM	4 GB or more	8 GB or more
Disk Space	20 GB (During installation, additional disk space may be required for hosting temporary data.)	50 GB
Operating Systems	Windows 7 Professional, Windows 7 Enterprise Windows 7 Ultimate Windows 8	Windows Server 2012 Windows Server 2008 R2 Standard Windows Servers 2008 R2 Enterprise Windows Servers 2008 R2 DataCenter Windows Servers 2008 R2 Web Edition
.NET Framework	Microsoft .NET 3.5 SP1 or later	Microsoft .NET 3.5 SP1 or later
Others	• Java 7 (Installer bundles by default) • Run with Windows Administrator privilege	• Java 7 (Installer bundles by default) • Run with Windows Administrator privilege

Splashtop Enterprise App — Client (Mobile Device) Requirements

You will need a **network connection**, plus the following requirements (depending on your specific mobile device). Minimum requirements are listed; however, if you want a remote connection at optimal experience/performance, we recommend using the requirements listed under the "**Recommended**" column.

iOS (iPad/iPhone) Client

	iPad (Minimum requirements)	iPad (Recommended)	iPhone (Minimum requirements)	iPhone (Recommended)
Hardware	iPad	iPad 2	iPhone 3GS	iPhone 5
Resolution	1024 x 768	1024 x 768 or above	480 x 320	1136 x 640
Operating System	iOS 5.0 or above	iOS 6.0 or above	iOS 5.0 or above	iOS 6.0 or above

Android (tablet/phone) Client

	Android tablet (Minimum requirements)	Android tablet (Recommended)	Android phone (Minimum requirements)	Android phone (Recommended)
Hardware	The currently-available Android CPU.	nVidia Tegra family. (For optimization, Tegra, Tegra-2, and Tegra-3 based tablets/devices are preferred.)	Smartphone capable of running Android v4.0 or above	nVidia Tegra family. (For optimization, Tegra, Tegra-2, and Tegra-3 based tablets/devices are preferred.)
Resolution	480 x 800	1280 x 800	–	–
Operating System	v3.1 or above	v4.0 or above	v4.0 or above	v4.0 or above

Windows/Mac (PC and Notebook) Client

	Windows Client (Minimum requirements)	Windows Client (Recommended)	Mac Client (Minimum requirements)	Mac Client (Recommended for optimal performance)
CPU	Intel Atom family CPU	Intel i7	1.6 GHz dual-core	Intel i7
Memory	1 GB	4 GB	1 GB	4 GB or more
Graphics	GMA	nVidia GeForce	–	–
Resolution	1024 x 600	1024 x 600 or above	–	–
Operating System	Windows Vista or XP	Windows 7 or 8	Mac OS X 10.6	Mac OS X 10.8 and above

Network Requirements

- One IP address and domain name:
  If you need a cross-firewall remote session, please prepare a public IP address for the Splashtop Center, or set port forwarding from the public IP to private IP in your firewall.
- One port:
  On-premise Gateway and Relay port: 443 (default)
  Please make sure port 443 is not blocked by your firewall.

Splashtop Center Scalability (Bandwidth Requirements)

- Required productivity usage bandwidth per session is: **300 kbps, and reserve 800 kbps for optimal performance**

  Test HW of Splashtop Center:
  CPU: Xeon E31220
  Memory: 4 gigabytes of RAM
  3000 users, 6000 Streamers, 300 concurrent relay sessions

Splashtop Streamer Requirements

You will need a **network connection**, plus the following requirements. Minimum requirements are listed in the middle column of each table below. However, if you want a remote connection at optimal experience/performance, we recommend using the requirements listed in the rightmost column.

Windows/Mac (PC and Notebook) Streamer

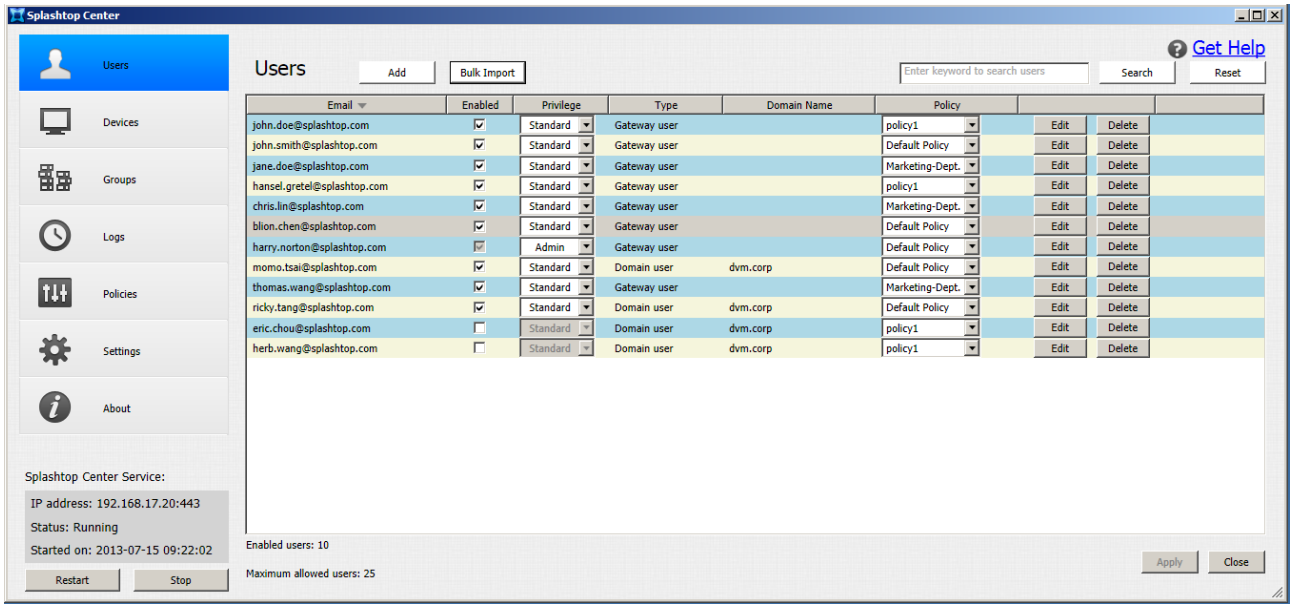
	Windows Streamer (Minimum requirements)	Windows Streamer (Recommended for optimal performance)	Mac Streamer (Minimum requirements)	Mac Streamer (Recommended for optimal performance)
CPU	1.6 GHz dual-core	Intel i7	1.6 GHz dual-core	Intel i7
RAM	1 GB	4 GB or more	1 GB	8 GB or more
Graphics	GPU	nVidia*	–	–
Resolution	1024 x 600	1024 x 600 or above	–	–
Operating Systems	Windows XP	Windows 7 or 8	Mac OS X 10.6	Mac OS X 10.8 and above

* For graphics optimization/acceleration, the following **nVidia** graphic series cards will enhance the overall performance:

GeForce 200, 300, 400, 500 series notebook or desktop GPUs, with at least 512 MB Frame Buffer.

The Splashtop Center Console

The Splashtop Center Console is a screen containing seven tabs in the left sidebar: **Users**, **Devices**, **Groups**, **Logs**, **Policies**, **Settings**, and **About**, as shown below.



Use the **Add** button or **Bulk Import** button in the **Users** tab to add new users. Thereafter, when opened, this tab will display all the users who have already been added, as shown in the example illustration above. From this list, you can conveniently change the **Privilege** setting at any time, **Enable/Disable** users, or **Delete** users. You can also click **Edit** and change the user's password or Email address, change the policy applied to this user, and generate additional activation codes (in the event that the user has obtained additional mobile devices which you want to authorize to utilize Splashtop Enterprise). One activation code can be used with only one mobile client device.

Splashtop Center supports two types of users: **Gateway** users and **Domain** (Active Directory) users.

- A **Gateway User** is a Splashtop Center user account that only exists on the Splashtop Center gateway module. This is the typical account for Splashtop Center, unless you use Active Directory.
- A **Domain User** is an Active Directory (AD) user which is managed by the IT Administrator. IT Administrators can integrate AD users into Splashtop Center.

A **Search** field has been added in the upper right corner of the **Users** tab. In it, you can enter the characters you want to search for Users with data matching the search-string will be listed in the **Users** tab.

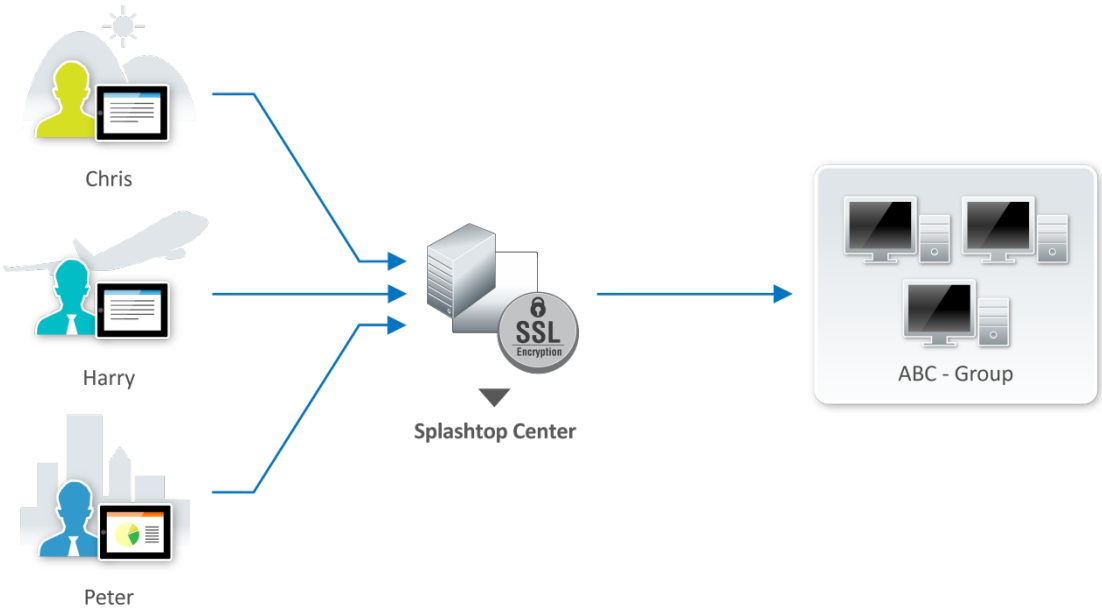
For details about how to add individual users, or add multiple users all at once, see section 4.1 and all of its sub-sections in the complete "**Splashtop Center Administrator's Guide**."

Devices Tab

Clicking **Devices** in the left sidebar of the Splashtop Center Console screen allows you to access the **Computers** and **Clients** tabs. The **Computers** tab (shown at the bottom of page 18) displays information about the computers in Splashtop Center that have the Splashtop Streamer installed, and the **Clients** tab displays information about the mobile client devices that currently have the Splashtop Enterprise app installed and activated. You can **de-**activate a device here also, if desired, either temporarily or permanently. And, like the **Users** tab shown on the previous page, a **Search** field has been added in the upper right of the screen.

The Groups Tab

The **Groups** tab lets you create new groups and edit them. It displays a list of existing group names; the users who have been added to those groups; and the computers they are allowed to use. A group named "Default" is created for you during the Splashtop Center installation. Grouping is a major benefit of Splashtop Center, as it lets the IT Administrator manage and grant access permissions to a selection of users, who can then use their mobile devices to connect to and share the remote computers (Streamers) designated for that group. The **Groups** tab also allows for quick enabling/disabling of groups, deleting them, or editing the properties.



The Logs Tab

The **Logs** tab displays online sessions as well as already-disconnected sessions. It shows the Start time, Client name, Client IP address, Client MAC address, User account, Client Platform, Computer (Streamer) name, Computer MAC address, Group, Duration of the session, type of connection, and what caused the disconnection of that session. A **Search** field has also been added in the upper right of the screen; all of the data mentioned above will be searched for a match. Logs are recorded from the first day of running Splashtop Center, so dates can be tracked back to "day one." A function is provided for Export/backup. Log files are archived on a per-day basis. If you do not want to display all existing log files, you can filter them to display for a period of one day/three days/one week/one month. There are no size limits for log files.

The Policies Tab

As the IT Administrator, you will be able to use the **Policies** tab to specify various settings, then save this configuration of settings to a "policy name," and then conveniently assign the policy to multiple users (instead of assigning the settings individually, to users individually). A policy named "**Default Policy**" is created for you during the Splashtop Center installation. If you have not yet created any other policies, then the settings configured in this policy will be applied to users by default.

The Settings Tab

The **Settings** tab contains six sub-tabs (**General**, **Security**, **Email**, **Software update**, **Backup**, and **License**).

General

The first time you launch Splashtop Center, the Settings/**General** tab will display by default. The **Port** number used by Splashtop Center is specified here. Also, if the **Enable Device Activation** option is enabled, then when adding a new user, you will have the "How many devices to activate?" option available. If the **Enable Device Activation** checkbox is not checked, then when you add new users, you will not have the option to automatically generate Activation Codes for the user's mobile device(s) at that time.

Security

The **Security** tab in **Settings** makes the optional **SSL certificate** configuration available to you. You can import your SSL certificate to enhance the security protection of Splashtop Center. Splashtop Center accepts **PFX** (Personal Information Exchange) format for SSL certificates. You can also use **Security** to conveniently generate a certificate if you don't have one. If the Force SSL on Local LAN connections option is enabled, it will be used as an alternative if the Streamer and client cannot successfully establish a new SSL LAN connection.

Email

This feature, if you choose to enable it, will automatically send email to users for account/password setup and device authentication whenever you:

- Add new users
- Reset or change a user's password
- Generate additional activation codes for a user's additional mobile devices

These pre-written Emails will contain the related information and give the users instructions on how to proceed. In addition, if necessary you can freely edit the templates as desired to meet your specific needs. This is a convenient time-saver for the IT Administrator. If the Email feature is not enabled, the IT Administrator will need to write individual Email to users manually for all of these cases. Please note that in order to use the **Bulk Import** feature in the **Users** tab (to add multiple users), the Email/SMTP configuration in this tab needs to be set up first.

Software Update

The newest Splashtop Enterprise (for Windows and Mac), and Splashtop Streamer (for Windows and Mac), can be hosted in Splashtop Center. The Installer needs to be downloaded from the Web Portal or obtained from Splashtop and stored on the local drive for Splashtop Center to host the software. At his/her discretion, the IT Administrator can use the **Force Streamer Update** button in the **Software Update** tab of **Settings** to forcibly push a Windows Streamer update to certain selected computers, or to all (maximum of five concurrent downloads). In addition, you can schedule the forced Streamer update to take place at a specific, more convenient time, such as non-peak or after-office hours.

Backup

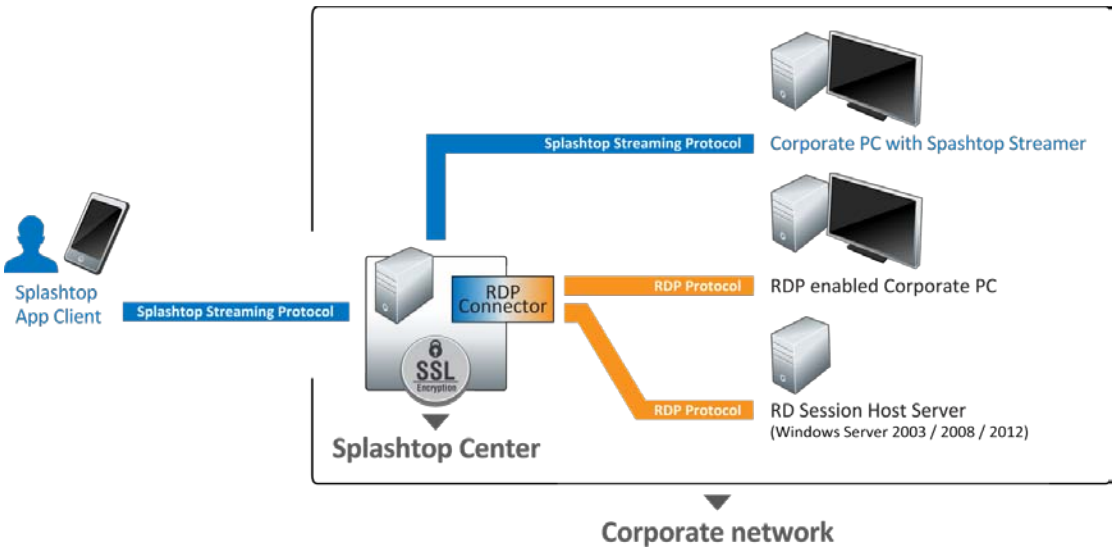
The **Save all settings to file** button in the **Backup** tab will open a dialog box that lets you save all your settings (the whole Splashtop Center database) to an SQL file. Please keep this backup file in case you need to recover your settings someday, or as a precaution when upgrading Splashtop Center. You can retrieve the data using the **Restore all settings from file** button.

License

The **License** tab will display your License Key, the Key status, Expiration date, Unlocked features (if any), maximum allowed user accounts ("Seats"), and maximum allowed computers. Click the **Assign License** button to activate your License Key either online or offline. Click the **Release License** button to remove the current License Key. If you were to upgrade or get a new license agreement someday (for example, you purchased additional Seats), click **Update License**. Enter Email address and License Key, then click **Activate**.

Get our optional RDP Connector!

Our SplashApp/**RDP Connector** option is ready for remote application delivery. This option allows you to use RDP (Remote Desktop Protocol) for remote connection using Splashtop Enterprise clients and to share access via RDS (Remote Desktop Services) on Windows-based machines from **Splashtop Enterprise app** clients. With **RDS**, a server is hosting simultaneous remote sessions and remote access to individual applications; whereas **RDP Desktop** allows one user to remotely access a host PC via Remote Desktop Protocol.



RDP Connector supports various configurations of Remote Desktop service from host machines including:

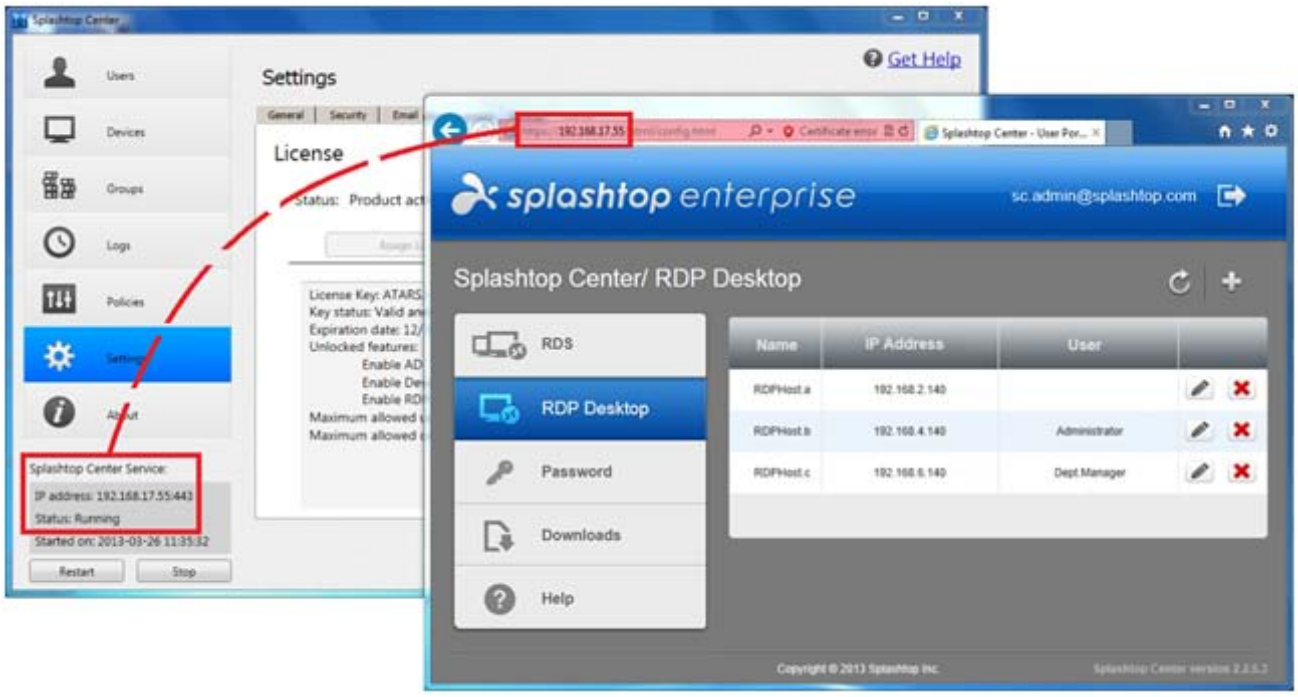
- RDP-enabled computers **(RDP to individual PC)**
- Remote Desktop server with RD Session Host configured for remote desktop **(RDP Desktop)**
- Remote Desktop server with RD Session Host configured for remote applications **(RDS RemoteApp)**

In general, **RDP Connector** is compatible with the RDP from host machines running:

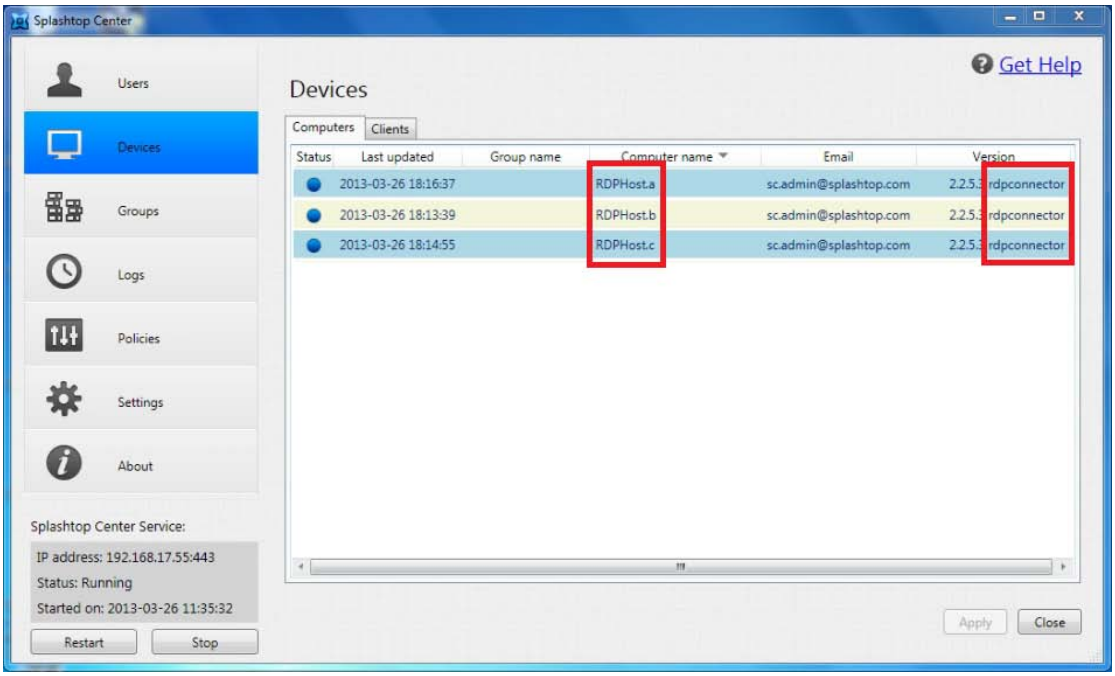
Microsoft Windows 2000 Server
Microsoft Windows XP (*including Professional, Service Pack 2, and Service Pack 3*)
Microsoft Windows Vista (*including Service Pack 1*)
Microsoft Windows 7 (*including Service Pack 1*)
Microsoft Windows 8
Microsoft Windows Server 2003 (*including Service Pack 1, Service Pack 2*)
Microsoft Windows Server 2008 (*including R2, R2 Service Pack 1*)
Microsoft Windows Server 2012 … , and above.

However, for **RemoteApp**, only **Microsoft Windows Server 2008** (**Terminal Services**), **Windows Server 2008 R2**, and above, can support it.

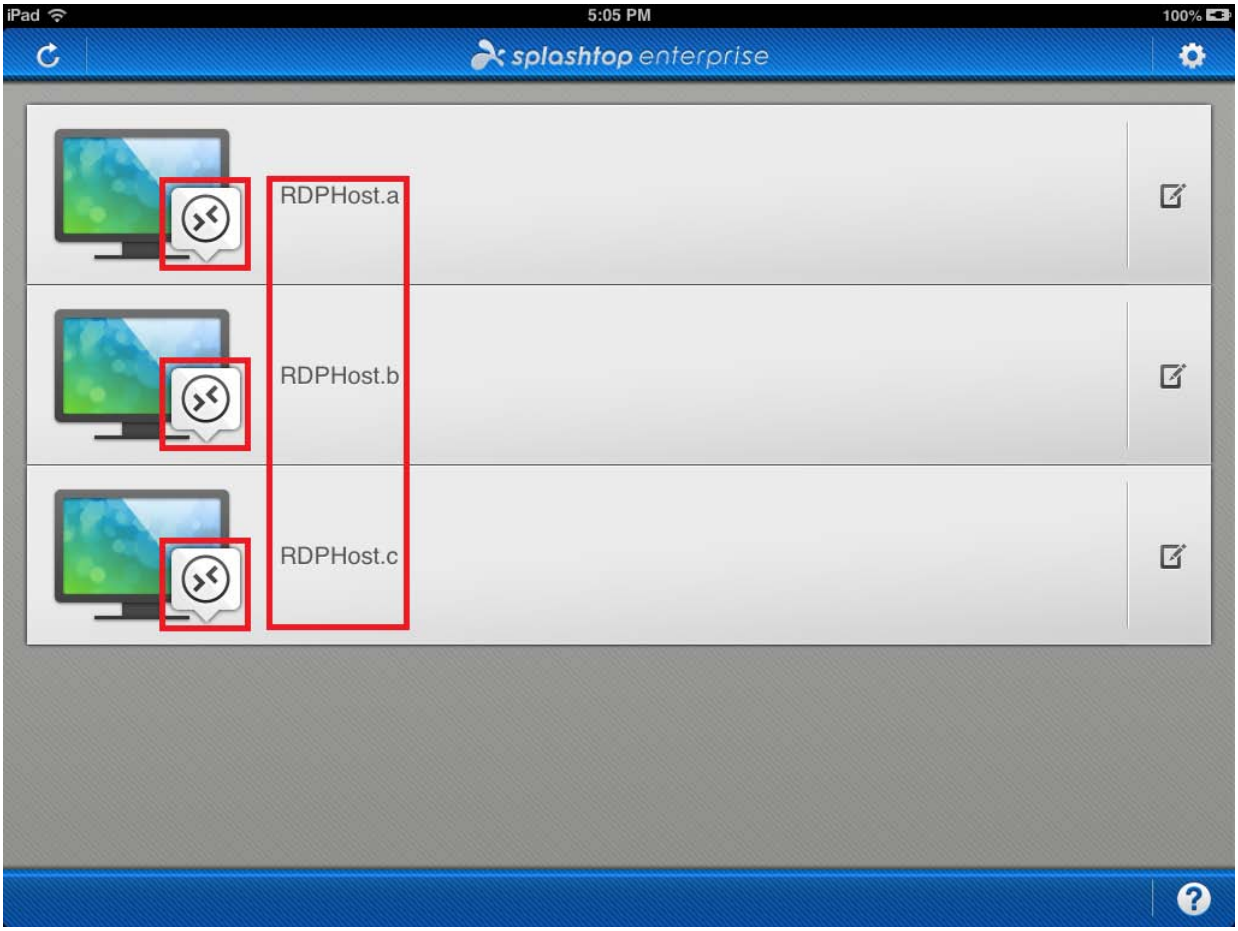
If you have obtained **RDP Connector**, you can access it by logging in to the **Splashtop Center Web portal** with the Administrator account. The URL for login contains the IP Address of your Splashtop Center (explained in detail in Chapter 5 of the complete "**Splashtop Center Administrator's Guide**"). You will then be able to see the **RDS** and **RDP Desktop** tabs, as shown in the example below, for adding the single or shared RDP machine(s).



After adding computers via the **Splashtop Center Web portal**, the **Devices** / **Computers** tab of the Splashtop Center Console will list them, as shown in the example below.



On the **Splashtop Enterprise app** side, all RDP-enabled computers that have been set up will be shown in the Computer List. The example below shows an iPad screen. Tapping the RDP remote desktop computer icon  in the Computer List will establish a connection to that RDP-enabled computer, via the RDP protocol.



NOTE: Logging in with an Administrator account gives full access to the functions of the Splashtop Center Web portal, including the **RDS** and **RDP Desktop** tabs. Regular Gateway users will only have access to the **Password** and **Downloads** tab, while Domain users will only have the **Downloads** tab available.

More information and examples can be found in Chapter 5 and Chapter 6 of the full "**Splashtop Center Administrator's Guide**".