Splashtop Center
Administrator's Guide
v1.7

Table of Contents

Table of Contents 2
1. Introduction 7
1.1. About this Guide 7
1.2. What is Splashtop Enterprise? 7
1.3. Splashtop Center Features 9
1.4. For more information 11
1.4.1. Web pages 11
1.5. How Splashtop Center Works 12
2. Installing Splashtop Enterprise 14
2.1. System Requirements 14
2.2. Basic steps to set up the first connection 18
2.3. Installing Splashtop Center 19
2.3.1. Upgrading Splashtop Center 23
2.3.2. Trouble-Shooting Splashtop Center Installation Issues 24
2.3.2.1. If you cannot add Domain users from Active Directory: 25
2.4. Installing the Splashtop Enterprise App 26
2.4.1. Making a Remote Connection 32
2.5. Installing Splashtop Streamer 37
2.5.1. Illustrations of the other Splashtop Streamer tabs 41
2.5.2. Trouble-Shooting Splashtop Streamer Installation Issues 44
3. Deployment Guidelines 47
3.1. Installation Deployment Choices 47
3.1.1. Splashtop Center deployment in the DMZ 47
3.1.1.1. Internet firewall (for DMZ) 48
3.1.1.2. Intranet firewall 48
3.1.2. Splashtop Center deployment in a private network 49
3.1.2.1. Internet firewall (for a private network) 49
3.1.3. Physical vs. Virtual 49
4. Navigating the Splashtop Center Console 50
4.1. The User's Tab 51
4.1.1. Enabling or Disabling Users 51
4.1.2. Adding Gateway Users individually (using the Add button) 53
4.1.3. Adding Domain (Active Directory) users individually (Add button) 58
4.1.4. Bulk Import — Adding Gateway Users 61

4.1.5. Bulk Import ─ Adding Domain (Active Directory) users 67
4.2. Searching Users 73
4.3. The Devices Tab 74
4.3.1. Computers 74
4.3.2. Clients 76
4.4. Searching Computers or Clients 78
4.5. The Groups Tab 79
4.5.1. Adding Groups 81
4.6. The Logs Tab 84
4.7. The Policies Tab 88
4.7.1. Default Policy 88
4.7.1.1. Security tab 89
4.7.1.1.1. Password 90
4.7.1.1.2. MAC Address filtering 90
4.7.1.1.3. Mode Switching 92
4.7.1.1.4. Misc 93
4.7.1.2. Others tab 94
4.7.2. Adding a new policy 95
4.7.3. Editing an existing policy 96
4.7.4. Deleting a policy 97
4.8. The Settings Tab 98
4.8.1. General 98
4.8.1.1. Device Activation Codes 99
4.8.2. Security 103
4.8.2.1. Converting a certificate to PFX file format 106
4.8.3. Email 107
4.8.3.1. Email Templates 110
4.8.4. Software Update 111
4.8.4.1. Scheduling the forced update 113
4.8.5. Backup 114
4.8.6. License 116
4.8.6.1. Updating Online 118
4.8.6.2. Updating Offline 118
4.9. About 120
5. Navigating the Splashtop Center Web Portal 121
5.1. Accessing the Splashtop Center Web Portal 121

5.2. Logging in 122
5.3. Password tab 123
5.4. Downloads tab 124
5.5. RDS tab 126
5.5.1. Adding a Remote App 132
5.6. RDP Desktop tab 135
5.7. Help tab 139
6. Common Tasks 140
6.1. Changing Ports 140
6.2. Re-installing Splashtop Center 142
6.3. Activating a Mobile Device 143
6.4. Re-issuing Device Activation and Authentication Codes 145
6.5. Creating and Administrating Groups 146
6.5.1. Deleting a Group 149
6.5.2. Modifying a Group 150
6.6. How to perform Wake-on-LAN with Splashtop Enterprise 152
6.6.1. Settings on Streamers: 152
6.6.2. Steps to trigger Wake-on-Lan 155
6.6.3. Wake-on-LAN usage timing and limitations: 156
6.6.4. How it works in different topologies 158
6.7. Keep Splashtop Center running in case of disaster 161
6.8. Setting Up RDP Connector and Making a Connection 163
6.8.1. OS Compatibility 164
6.8.2. Scalability (Bandwidth Requirements) 164
6.8.3. How to set up remote desktop for an RDP-enabled computer 165
6.8.3.1. Windows setup 165
6.8.3.2. Splashtop Center setup 169
6.8.4. How to set up remote desktop from a Remote Desktop server with the RD Session Host configured 173
6.8.4.1. Windows setup 173
6.8.4.2. Splashtop Center setup 177
6.8.5. How to set up a remote application from Remote Desktop server with RD Session Host configured 181
6.8.5.1. Windows setup 181
6.8.5.2. Splashtop Center setup 188
7. Appendix 192
7.1. Splashtop Enterprise Architecture 192
7.1.1. Splashtop Enterprise App 192

7.1.2. Splashtop Center 193
7.1.3. Splashtop Streamer 193
7.2. Readiness / Installation Checklist 194
7.3. SSL Certificate Import / Export 196
7.3.1. Installing the SSL Certificate 196
7.3.1.1. On an Android tablet or Android phone (4.0): 196
7.3.1.2. From your Nexus 7 tablet's internal storage: 197
7.3.1.3. On an iPad or iPhone: 197
7.3.1.4. On a Mac PC or Notebook: 197
7.3.1.5. In Windows 198
7.4. Setting Up RDP and RDS in Microsoft Windows Server 2012 199
7.4.1. How to Enable Remote Desktop in Windows Server 2012 199
7.4.2. How to Configure Remote Desktop Services 200
7.4.2.1. Joining the Server to an Active Directory Domain 202
7.4.2.2. Remote Desktop Services Installation 203
7.4.2.3. Overview of Remote Desktop Services 206
7.4.2.4. Properties Settings of a Session Collection 207
7.4.2.5. Publishing RemoteApp Programs 210
7.5. If Your License Expires 215
7.6. Definitions 216
7.6.1. Users 216
7.6.2. SSL and TLS 216
7.6.3. NTLM 216
7.6.4. Seats 217
8. Index 219

Copyright Information

Fourth Edition July 2013

1. Introduction

1.1. About this Guide

This **Splashtop Center Administrator's Guide** ("*Admin Guide*") provides server, desktop, and network administrators with a detailed overview of Splashtop Enterprise with SplashApp technology, including installation, activation, configuration, and administration of Splashtop Center, devices, users, and groups. It contains details about how to perform Wake-on-LAN; how to get into the Splashtop Center Web Portal; and how to make a connection with our SplashApp/RDP Connector option. The Admin Guide also includes a discussion on deployment and best practice tips to get the most out of your Splashtop Enterprise solution.

1.2. What is Splashtop Enterprise?

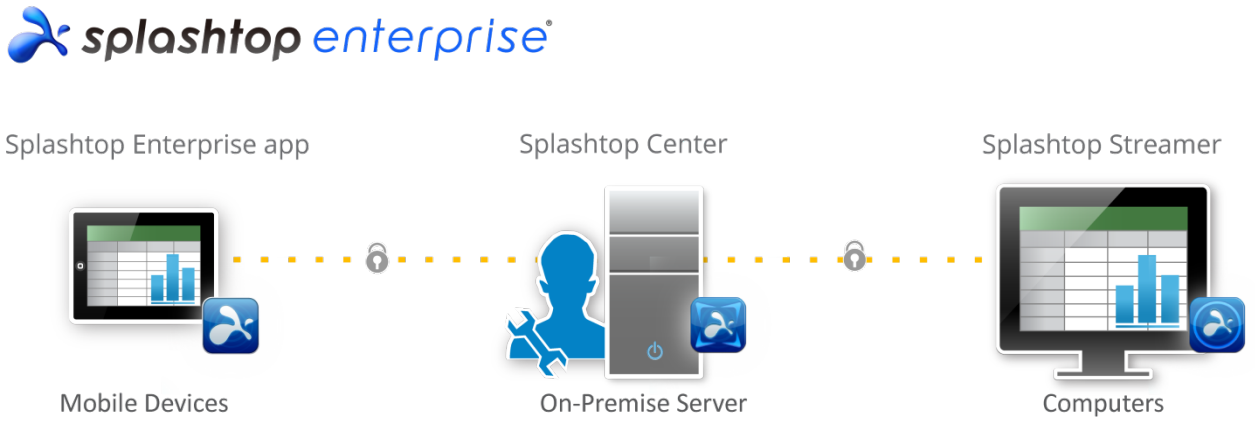
Splashtop Enterprise with SplashApp technology provides IT organizations with the tools necessary to securely and centrally manage how users remotely access their computers. It offers an on-premise managed capability allowing corporate users with tablets and hand-held devices (like the iPad and Android tablet) to remotely view and interact with their desktop or notebook work computers from outside the workplace.

Now, employees on-the-go can enjoy all the benefits of remotely accessing applications and data from their mobile devices as if they were in front of their computers.

- Centralize management so you can set user access policies and view session activity in real time.
- Host behind your firewall using your own Windows servers to protect sensitive user information and eliminate external monthly hosting fees.
- Enhance access and security so that your mobile users can be more productive by accessing important company files and software from the road or at home easily and securely.

This product is comprised of 3 components:

- **Splashtop Center** – Performs Gateway, Relay, user, and device management functions. This is the central server that authenticates, secures, and connects users and devices. It also provides a Console to configure (and report on) users and devices. It is installed on a Windows server.
- **Splashtop Enterprise** App makes it possible to connect your mobile device to the target computer running the Splashtop Streamer.
- **Splashtop Streamer** is the software which needs to be installed and running on the remote computer you want to access. It streams audio and video to the mobile client device.



1.3. 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.

High availability

- Keep your Splashtop Enterprise running: With this version, 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 ("Web portal") provides this 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. Please see Chapter 5 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.

1.4. For more information

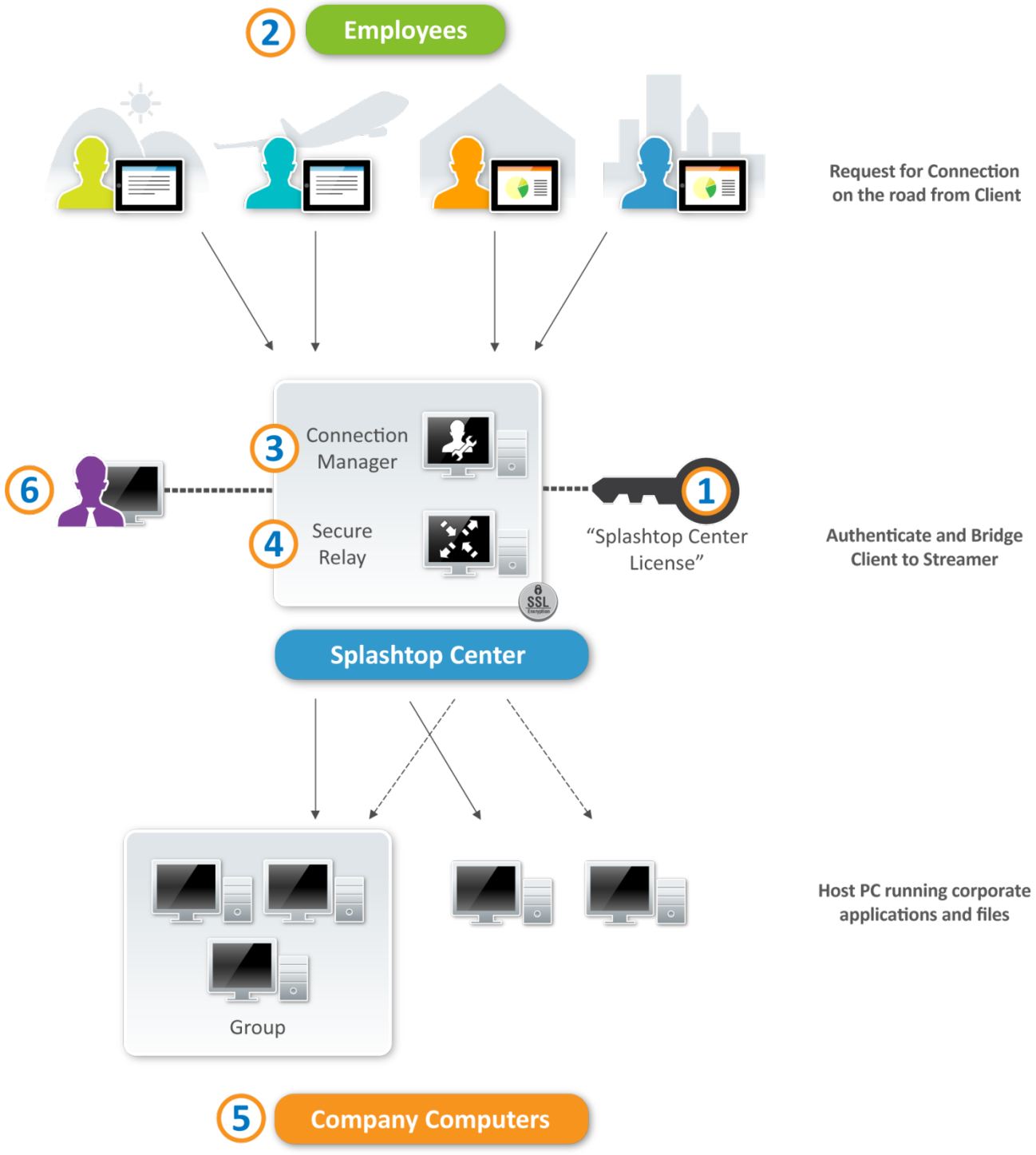
1.4.1. Web pages

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

In addition, for **Help**, **Frequently Asked Questions**, **Community Forums** and **trouble-shooting tips**, please visit:
http://support-splashtopenterprise.splashtop.com/home

1.5. How Splashtop Center Works

The Splashtop Center "connection flow diagram" below shows how Splashtop Center fulfills the needs of users in the mobile workforce to remotely access files and applications from their office computers.



(1) First, activate the Splashtop Center Gateway with a proper license key.

(2) Users enroll their device in Splashtop Center, then will be able to log in and initiate a remote access request from a client on their mobile devices.

(3) Once a mobile client device is logged in and authenticated by the connection manager with a valid account assigned by you, the IT Administrator, it will be able to query the status of both the mobile device and the target computers. This is done transparently to the user.

(4) Upon initiating a remote session, Secure Relay does the actual bridging of the encrypted packets between a mobile device which is away from the local network, and host computer. The whole data path is secured by Secured Socket Layer (SSL) with AES 256 encryption. Splashtop Center can import a certificate from a trusted SSL certificate provider, or generate a self-signed SSL certificate. SSL uses the public and private key encryption system to ensure security between a client and Streamer.

(5) The computers in your company on which you have installed the Streamer can be accessed remotely by the authorized users either within the same network, or over the Internet.
For local connection (within the same network), the mobile client device and the Streamer will establish a direct session with the best performance in the local network. If SSL encryption is a concern in the local network, please enable the **Force SSL on Local LAN connections** option in the Security settings.
For remote connection (over the Internet), the mobile client device and Streamer will establish an SSL session by going through Secure Relay.

(6) Using the management console enabled by the Splashtop Center Gateway, the IT Administrator can monitor sessions at any time, as well as manage user and device privileges and policies.

2. Installing Splashtop Enterprise

2.1. System Requirements

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.

2.2. Basic steps to set up the first connection

The basic steps to get up and running will typically look like this. The first five steps should be done by you, the IT Administrator, and the remaining two will be done by the users.

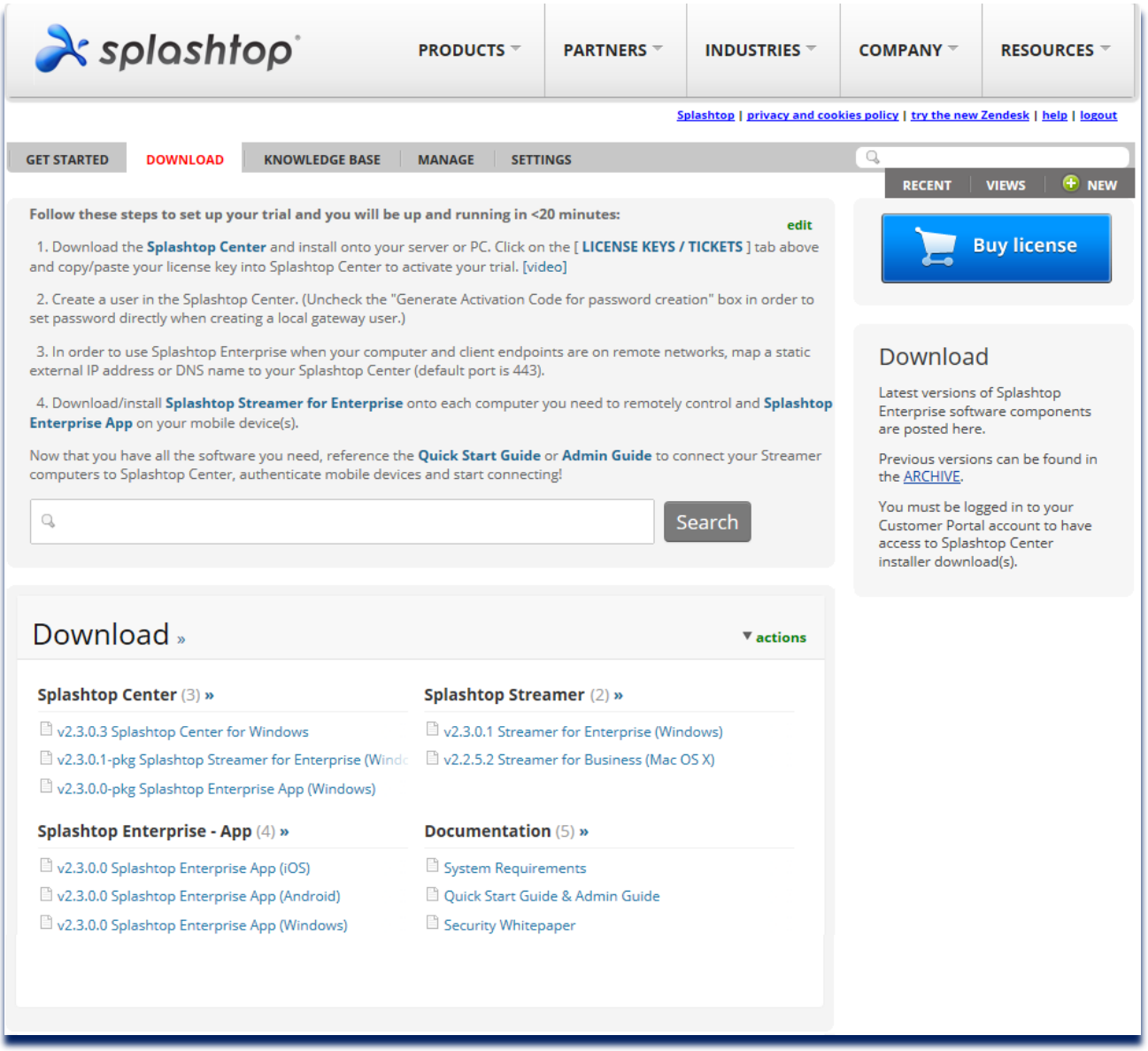
1. The IT Administrator sets up Splashtop Center on the company network.
2. The IT Administrator groups the computers as desired, and sets user permissions accordingly. For an example "use case," please see section 6.5, **Creating and Administrating Groups**.
3. The IT Administrator creates user accounts.
4. The IT Administrator notifies users that they have been added to Splashtop Center, and provides specific credentials to them such as activation code and/or password.
5. The IT Administrator downloads the Streamer and installs it on all the computers which he or she wants to be available to users for remote access.
6. The user downloads the Splashtop Enterprise client app to his/her mobile device and installs it.
7. The user invokes the client app on his/her mobile device and logs in using the password given by IT Admin. The user can then make a remote connection to a computer in the office.

Splashtop Center and Splashtop Steamer 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.

For your convenience, the installation sub-sections below also contain some trouble-shooting tips from our online FAQ and Knowledge Base. For more information, please visit our Support pages at: http://support-splashtopforbusiness.splashtop.com/forums

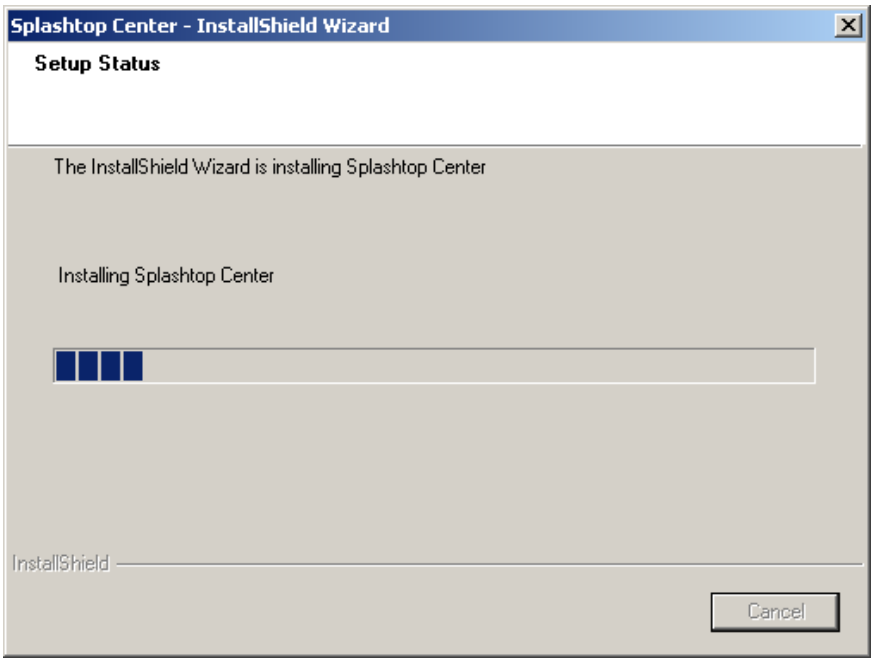
2.3. Installing Splashtop Center

1. To begin, go to our *Splashtop Enterprise* web site at: http://www.splashtop.com/enterprise.
2. Click the **Request for 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), which will look similar to the sample illustration below. Follow the instructions on the screen.



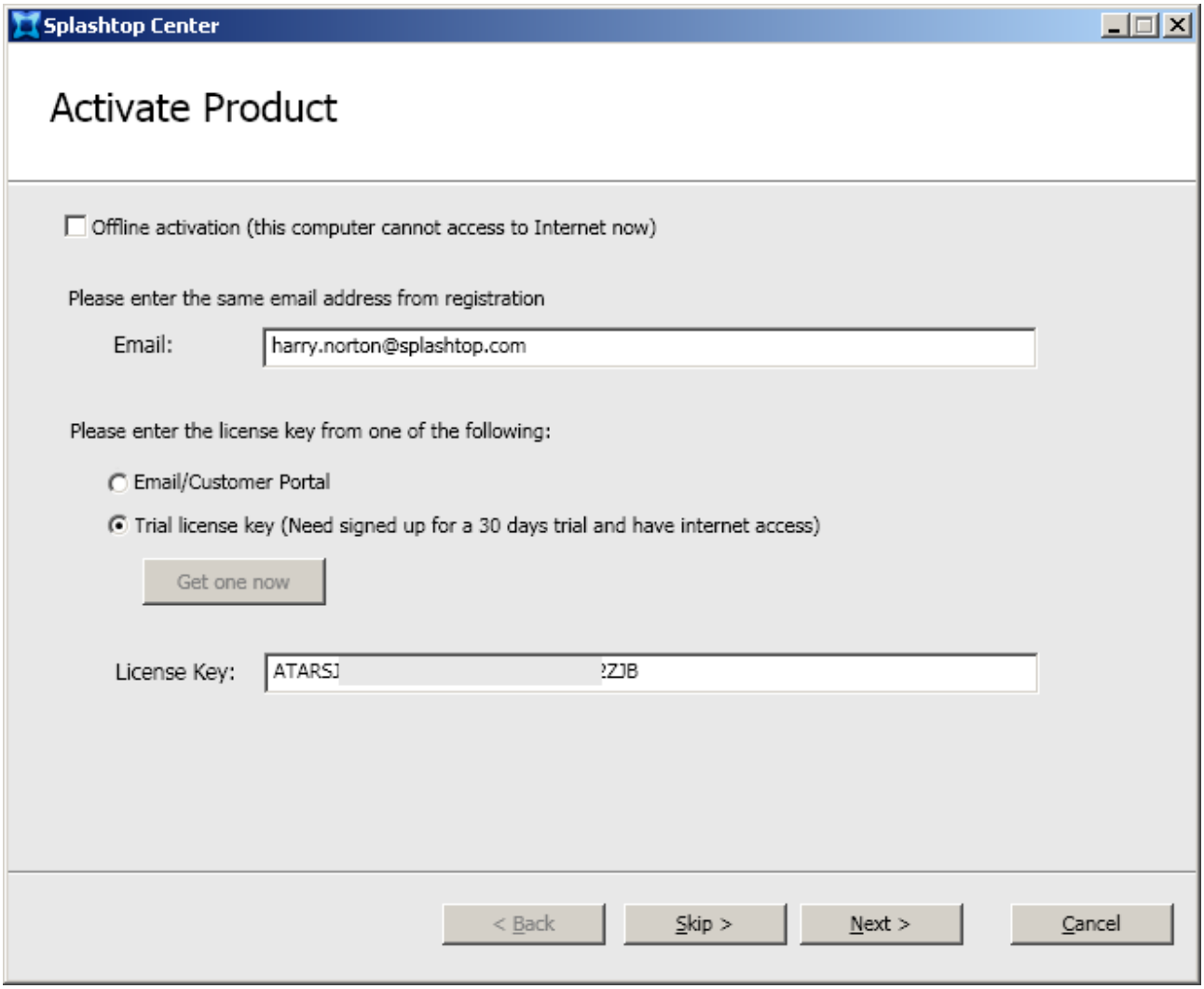
Note above that you can also access the full *Splashtop Center Administrator's Guide*, and the *Quick Start Guide*, under **Documentation**. You can also click **Knowledge Base** to access the FAQ and other helpful documentation.

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

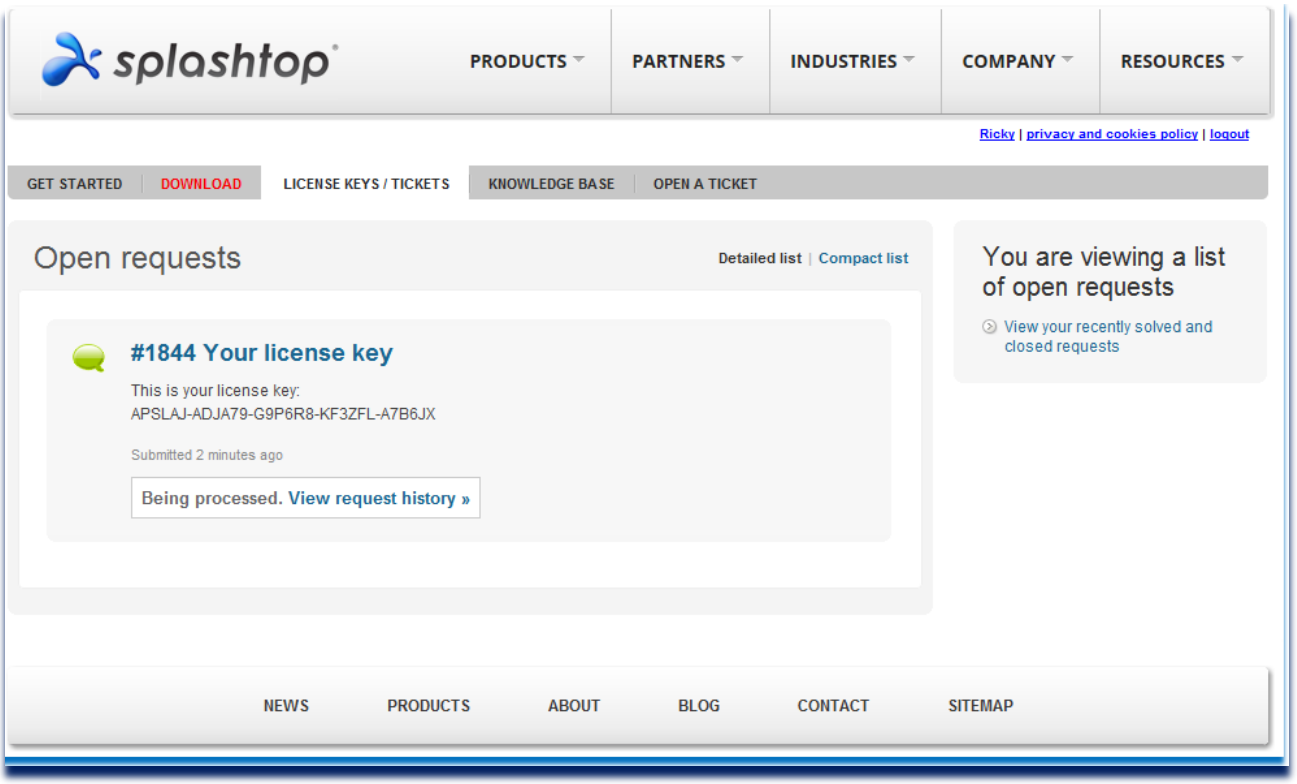


6. After the installation is finished, go to the License keys / Tickets page to retrieve the License Key which you will need in order to activate Splashtop Center. (The **License Manager** tab of the Splashtop Center Console window is explained in section 4.8.6.)

Alternatively, if you are a Trial user, you can activate/query the Trial license via the "First Time" Wizard during installation, using the dialog box shown below. You can retrieve your Trial key from here:



Or, you can go through the License/Tickets page in the Customer Portal to set up the License Key, and then manually enter it in the **License** tab of **Settings**, in the Splashtop Center window, as mentioned earlier.



2.3.1. Upgrading Splashtop Center

Newer versions of Splashtop Center are periodically released. If you have already installed Splashtop Center and want to upgrade to a newer version:

1. We recommend that you perform a backup of the Splashtop Center settings using the **Backup** tab in **Settings**, which is shown in section 4.8.5. Optionally, you may want to export your SSL certificate (**Export** button in **Security** tab, section 4.8.2) and Logs (**Export** button in the **Logs** tab, section 4.6), in case of any upgrade issues. However, please note that if your License Key has expired, you won't be able to use the **Backup** function. You can check the expiration date of your License Key in the **License** tab of **Settings** (illustrated in section 4.8.6.).
2. Download the newest version of Splashtop Center.
3. Install the newest version of Splashtop Center. The upgrade process will start automatically. All Splashtop Center settings will be retained after the upgrade.
4. Perform any additional changes or configurations to Splashtop Center if desired.
5. Start the Splashtop Center service (it does not start running automatically after updated).

See also section 4.8.4 for information about how to use the **Software Update** tab of **Settings** to host the newest versions of Splashtop Enterprise, and Splashtop Streamer, via the Splashtop Center console. You can use this feature to push a forced Streamer update to all (or selected) users, and can also schedule it to automatically take place at a certain date and time.

2.3.2. Trouble-Shooting Splashtop Center Installation Issues

If the installation fails to complete:

The Splashtop Center installer will attempt to configure and install companion components in order to allow the service to function properly. If problems are encountered, the installation process will usually inform you, and offer instructions that may assist you. The examples below show some typical situations that you may encounter:

* Missing Microsoft .NET Framework 3.5 SP1

Please download and install Microsoft .NET Framework 3.5 SP1 before proceeding with the Splashtop Center installation (link: http://www.microsoft.com/en-us/download/details.aspx?id=22).

* Unable to auto install Java 7 Update 3

If you run into this error, please run the Splashtop Center installer again in "command line mode" with the instruction:

setup.exe /v"INSTALL_JAVA=1"

* Insufficient disk space

Splashtop Center requires a minimum of 200 MB of disk space. However, during the installation, keep in mind that it may require additional disk space for hosting temporary uncompressed data.

If you get a "port error" message:

You will receive the following warning message if you restart the Splashtop Center service after having selected a network port that is occupied by other software within the host OS:

"The specified port: {_port_number_} is occupied by {_software_process_name_}. Please close or change the port settings in {_software_process_name_}. Or, configure the Gateway settings in Splashtop Center in order for the Splashtop Center service to function properly."

If you encounter this warning message, try to use another network port either for Splashtop Center or for that software application.

Please note that port changes in Splashtop Center require a restart of the Splashtop Center service, as well as the clients and Streamers needed, to update the Splashtop Center address accordingly.

2.3.2.1. If you cannot add Domain users from Active Directory:

If you are unable to find a Domain user to add into Splashtop Center, please check the following:

- Is the server running Splashtop Center on the same domain as the Active Directory server? It needs to be.
- When you check for a user, does it show a user, but not the user account you are looking for? You may need to type in the full domain name before clicking "**Check**".
- Do the license details show Active Directory support?

NOTE: When logging in with a Domain user account, make sure to use the Email address — not the domain address. More info about adding Domain users can be found in section 4.1.3.

2.4. Installing the Splashtop Enterprise App

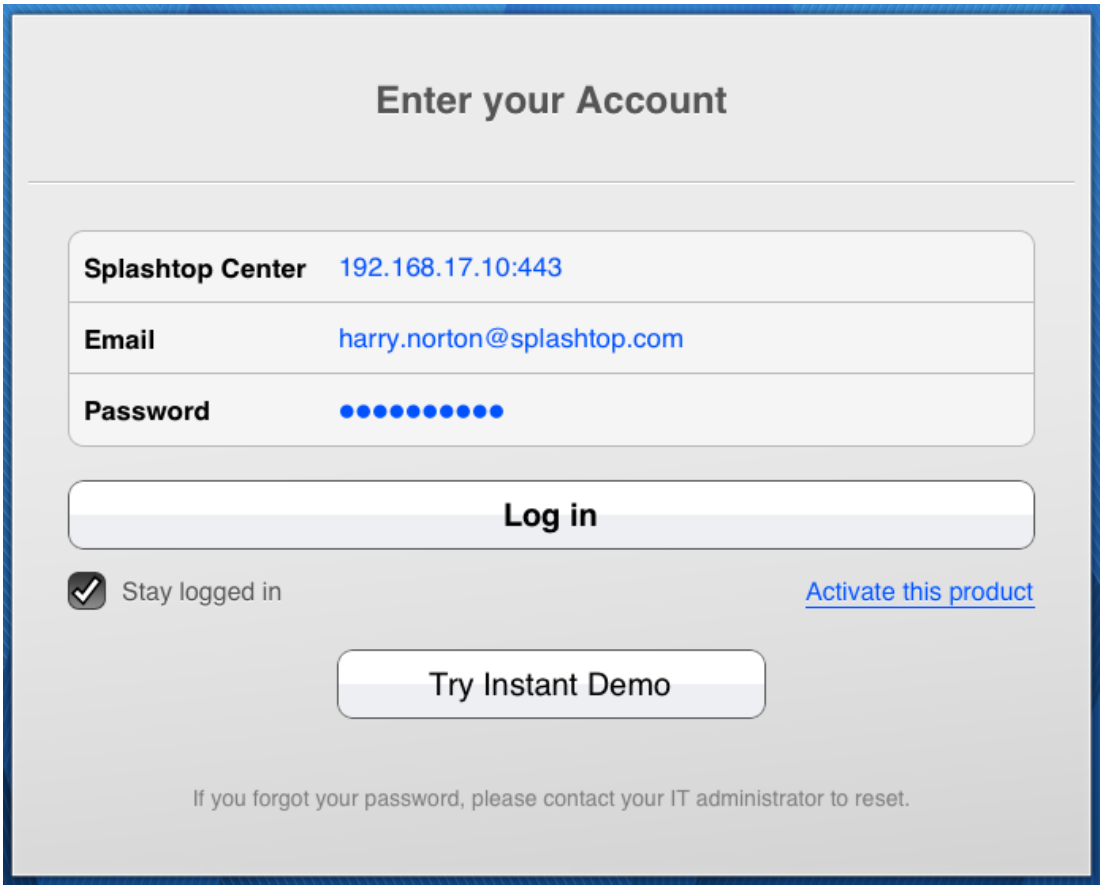
This is the App that is installed on the user's mobile client device (supported devices were listed earlier in section 2.1). Remote access requests will be initiated from this App in the mobile device, to the Streamer on the remote computer, through Splashtop Center.

For illustrative purposes, we have used the iPad as our example mobile device in the following steps.

1. Find the **Splashtop Enterprise** App in the Apple App Store using your iPad. You can type "Splashtop Enterprise" in the *Search* box (shown in the upper right corner of the illustration below) to find it.

2. Tap the **Splashtop Enterprise** icon or the **Install App** button to begin installing on your iPad. A dialog box may appear, asking you to input your Apple account ID and Password. If so, you will need to do so to proceed.

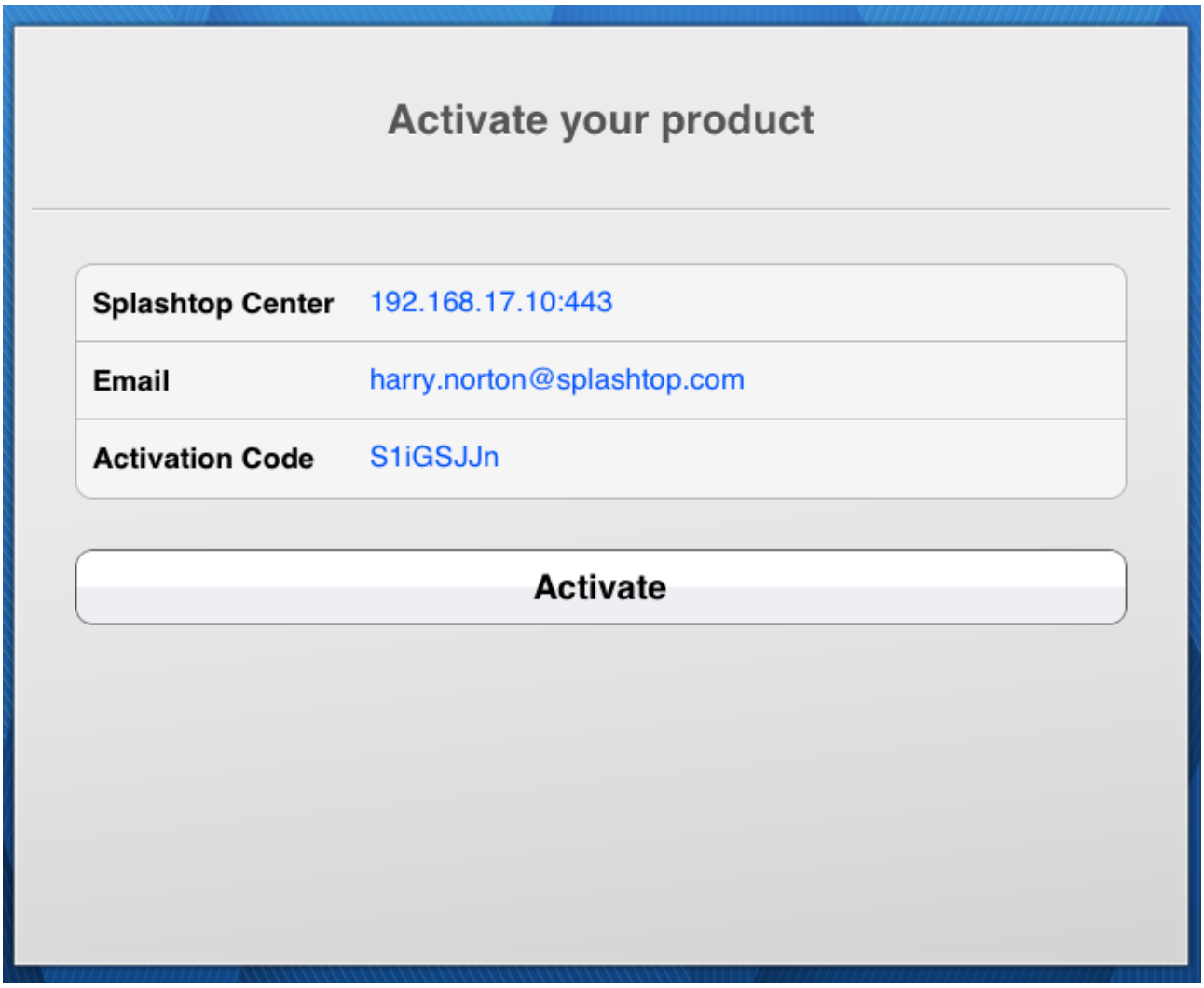
3. After the **Splashtop Enterprise** App has finished installing, there are a couple of different approaches that can be used to launch the App. With Splashtop Enterprise, the user should receive some Invitation Email which contains an "auto-launcher link." If the user opens the Invitation Email on the target device for Splashtop Enterprise, he or she only needs to click on this link. Splashtop Enterprise will start, and then you can input the Splashtop Center Server's IP address, and the Email address you use in conjunction with Splashtop Center. Users who don't have this information will need to ask the IT department for it.



4. After entering the information in the fields of the *Enter Your Account* dialog box, tap **Log In**. If a warning message pops up when you tap **Log In**, telling you that your SSL 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. However, we recommend that users who have encountered this message popping up should contact their IT department for the proper guidelines in handling this situation.

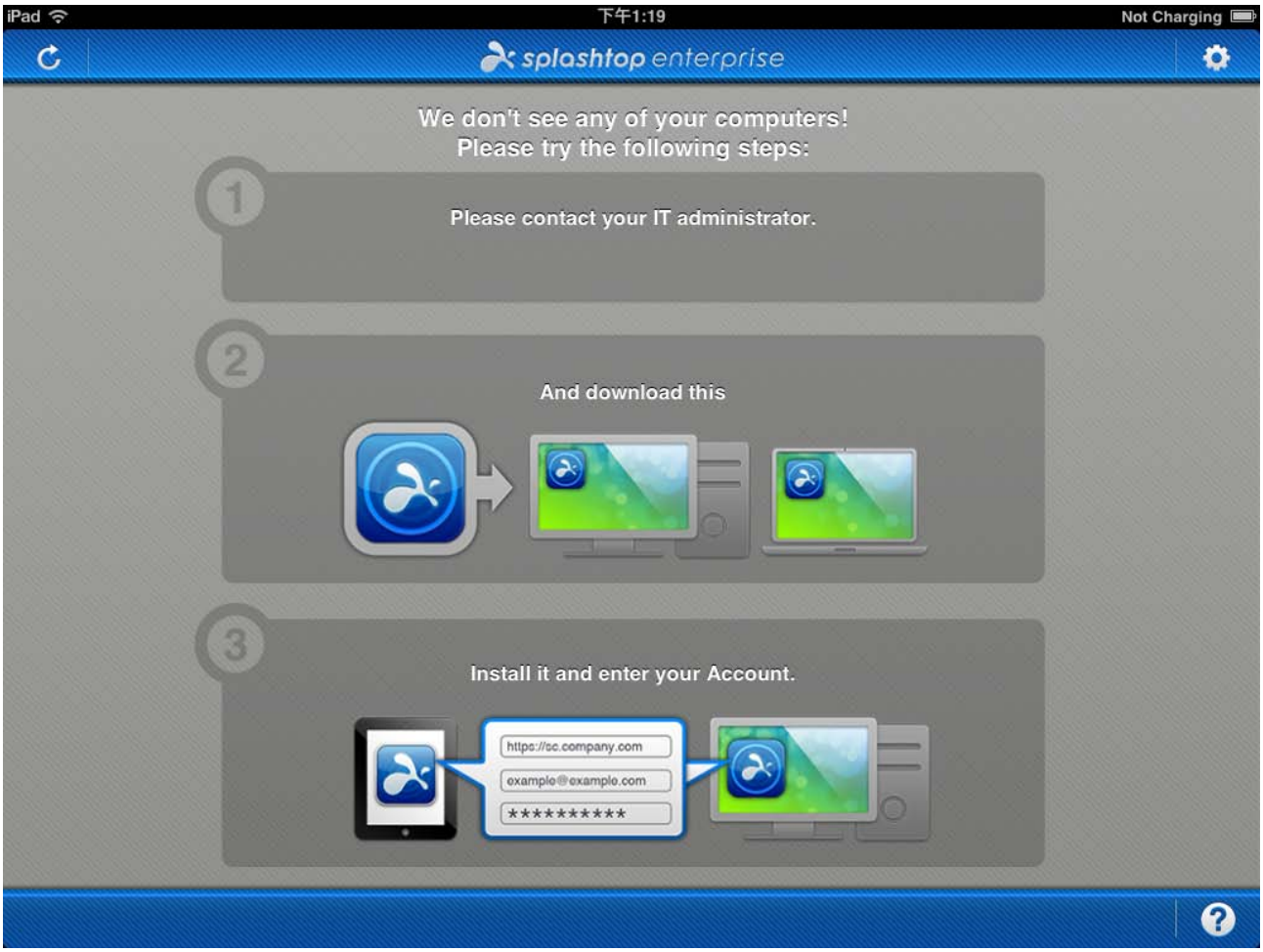
5. If you continue to get an error message stating "Account Login Failed; This product isn't activated," it means your IT department has enabled an option that requires users to activate Splashtop Enterprise on this client device before the **Splashtop Enterprise** App can be used.

So, in this case, users should contact the IT department to get the proper activation code, and input it into the following screen.

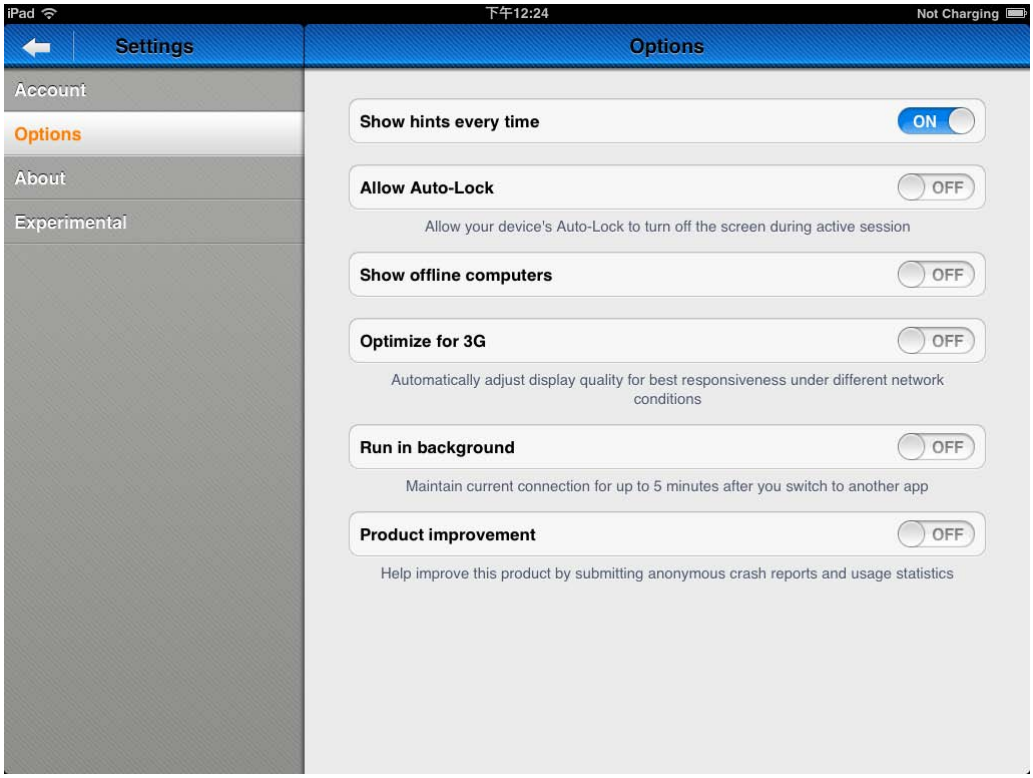


6. After successfully activating your mobile device, the "Set Your Password" screen will appear if you have not yet set up a password. Otherwise, you'll get the same "Enter Your Account" screen that was shown under Step 3. Enter your information and try to log in again.

7. After you log in successfully, the screen shown below will display. In this screen, 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 like the one pictured below, 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 for helpful tips.



NOTE: You can click the "gear" icon (shown in the upper right corner of the illustration above) to open the **Settings/Options** tab (pictured on the next page). These options are helpful in certain conditions. For example, **Optimize for 3G** could be switched ON if your available network bandwidth is not so good.



NOTE: The Client app for Windows supports silent installation and un-installation. Please append the appropriate parameter as follows:

- Install: "**/s**"
- Un-install: "**/s /removeonly**"

Silent install

For silent installation use a command following this formula:

Install path\execution file(.exe) setup/s

For example:

D:\SC_WinClient\V2.2.0.1\Splashtop_for_Business_Win_v2.2.0.1.exe setup/s

Silent un-install

For silent un-installation use a command following this formula:

Install path\execution file(.exe) setup/s/removeonly

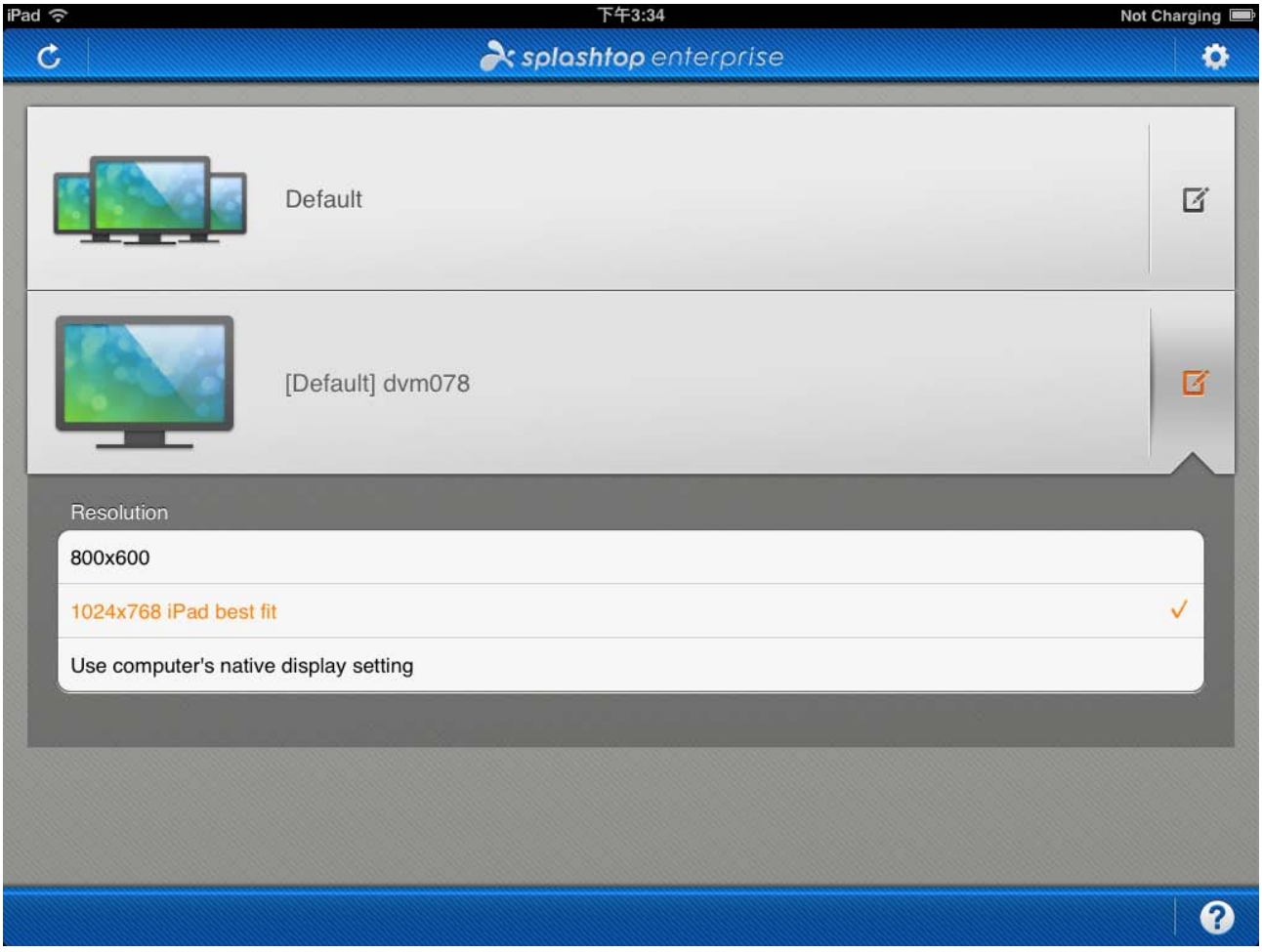
For example:

D:\SC_WinClient\V2.2.0.1\Splashtop_for_Business_Win_v2.2.0.1.exe setup/s/removeonly

2.4.1. Making a Remote Connection

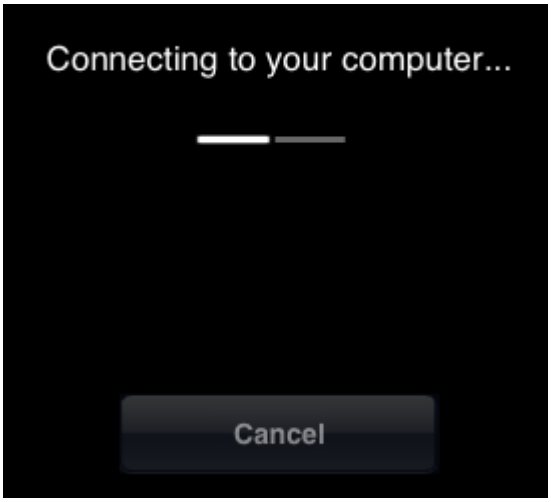
The computers you are allowed to remote-connect to, using this iPad, will be listed in your iPad's Computer List screen as in the example below.

Tap the computer icon representing the computer you want to connect to. (Don't forget, the Streamer must be running on that computer, in order for the Splashtop app on your mobile device to find it.)

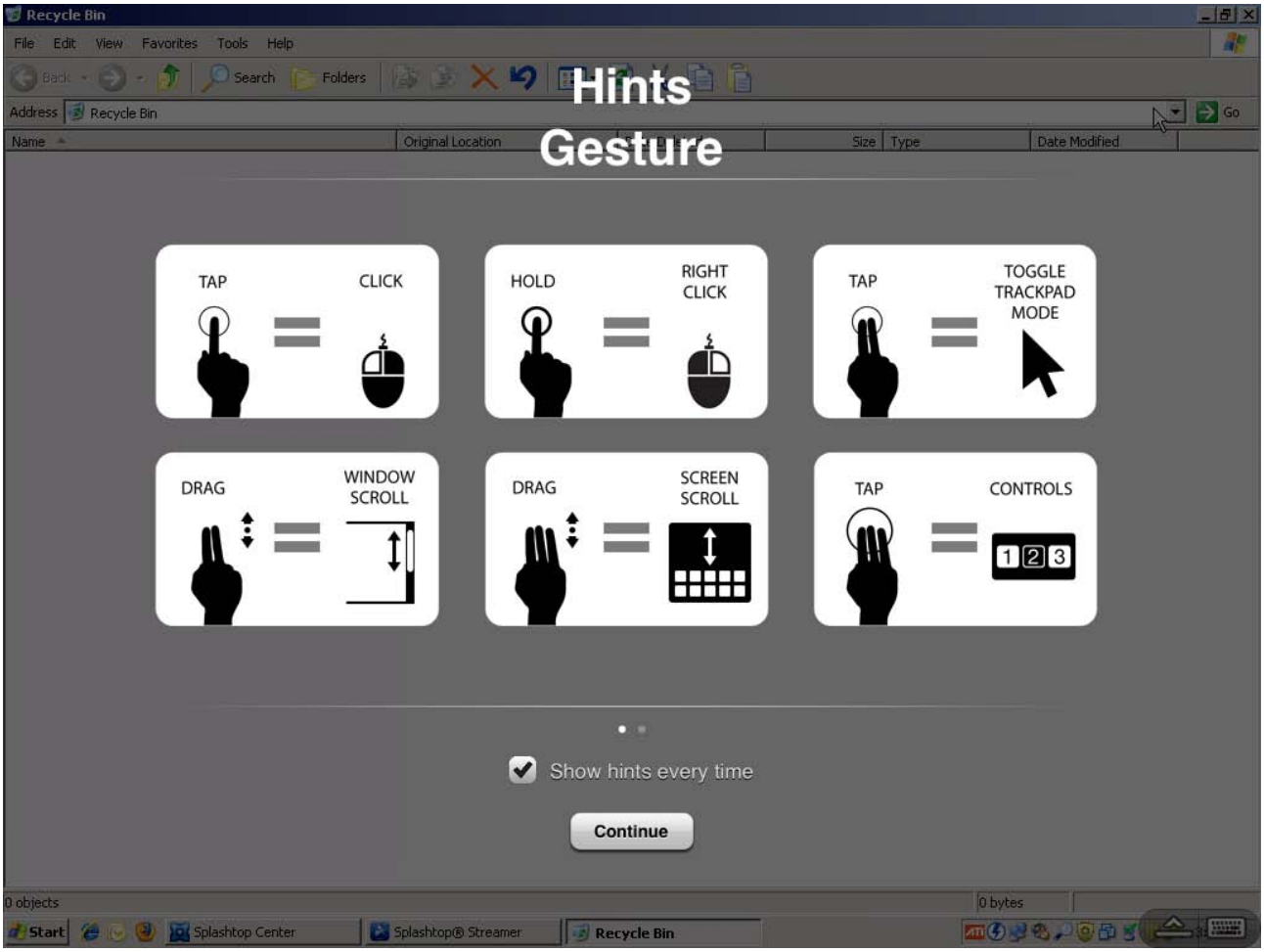


NOTE: Tapping the icon to the right of a computer name will open a drop-down menu as shown above, which allows you to select a Resolution.

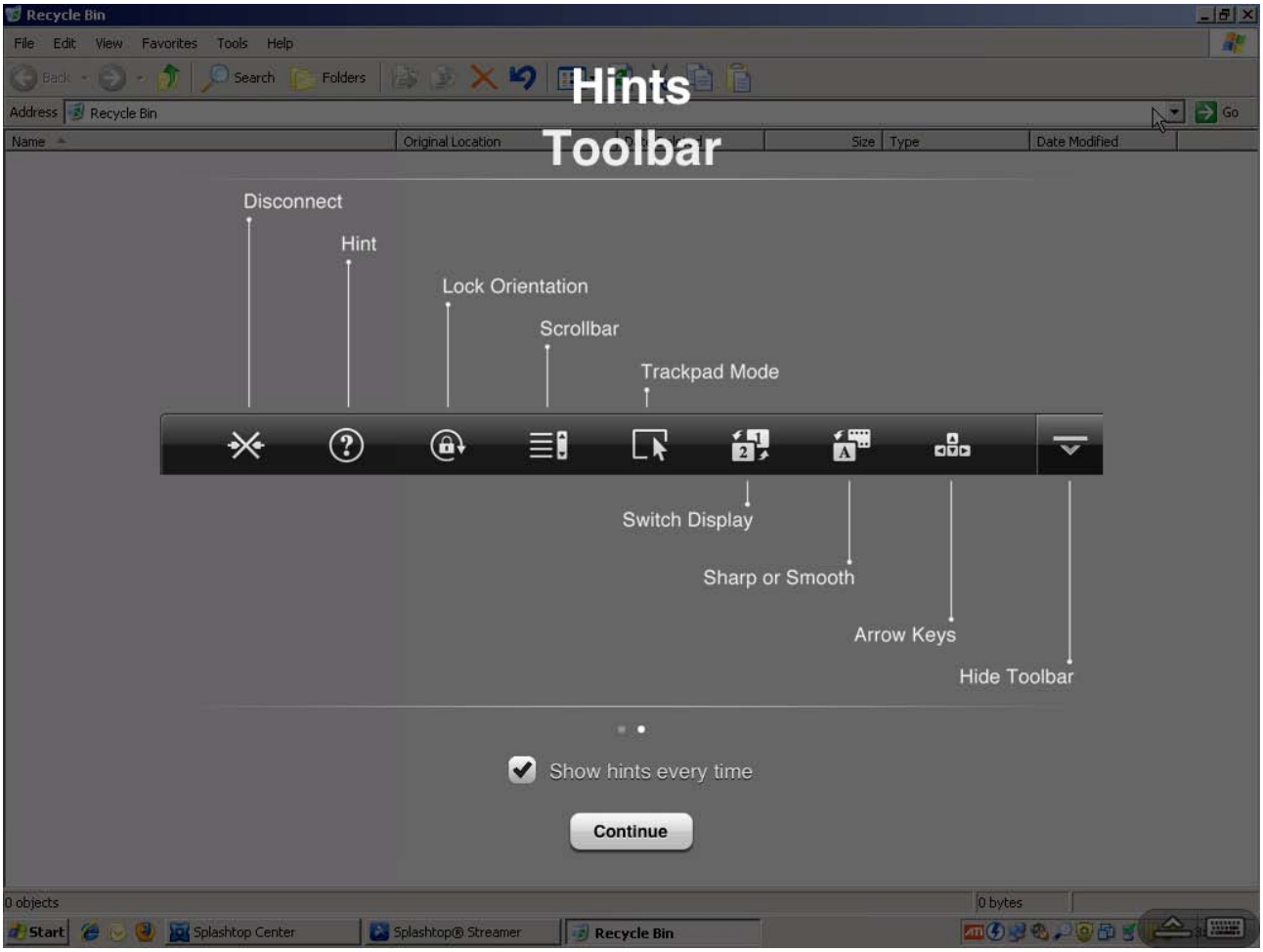
This message will display momentarily:



On your first connection, the next thing you will see should be the "*Hints*" screen, illustrating the gestures you can perform on your iPad during a remote connection. These will be super-imposed over the remote computer's screen, which is now shown on your iPad. If you do not want to see this *Hints* screen every time you make a connection, un-check the **Show Hints Every Time** checkbox shown below.



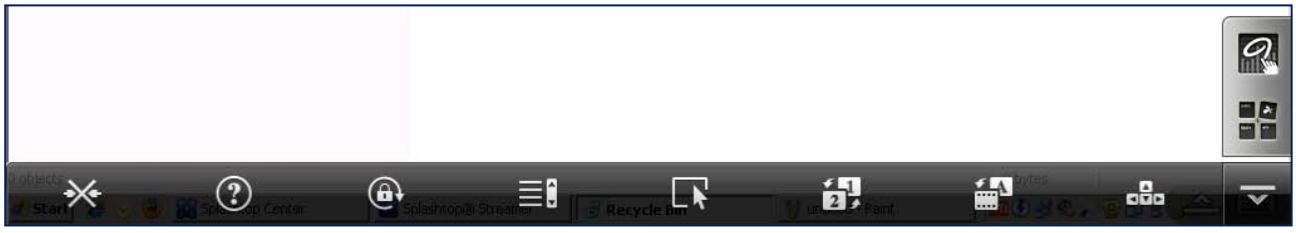
The other translucent "Hints" screen tells you what the icons on the Toolbar do:



There are two icons in the lower right corner of the screen during a remote connection (as shown above).

You can open the on-screen **Keyboard** by tapping  in the lower right corner (as shown above).

Or, display the **Toolbar** (shown below) by tapping the  icon.



New Freebies Available on the Toolbar !

We now offer two of our products free, with your purchase of Splashtop Enterprise — **Splashtop Whiteboard** and **Configurable Shortcuts and Gamepad**. You can access them from the Toolbar on the Client app during a remote connection (shown on the previous page).

Splashtop Whiteboard

Our popular **Splashtop Whiteboard** app is included free with your Splashtop Enterprise! To start it, just tap the  icon on the Toolbar, shown in the previous illustration.

For information about **Splashtop Whiteboard**, please see our web page at:
http://www.splashtop.com/whiteboard
For Frequently Asked Questions, please see the Splashtop Whiteboard Support page at:
http://splashtopwhiteboard.zendesk.com/home

Configurable Shortcuts and Gamepad (CSG)

Another app that you now get free with Splashtop Enterprise is our **Configurable Shortcuts and GamePad**.

To start **CSG**, tap the  icon on the Toolbar. For information about this product:

For a basic introduction, please see this Press Release:
http://www.splashtop.com/press/1-remote-desktop-leader-splashtop-introduces-configurable-shortcuts-gamepad-%E2%80%93-ability-to-create-keyboard-shortcuts-mouse

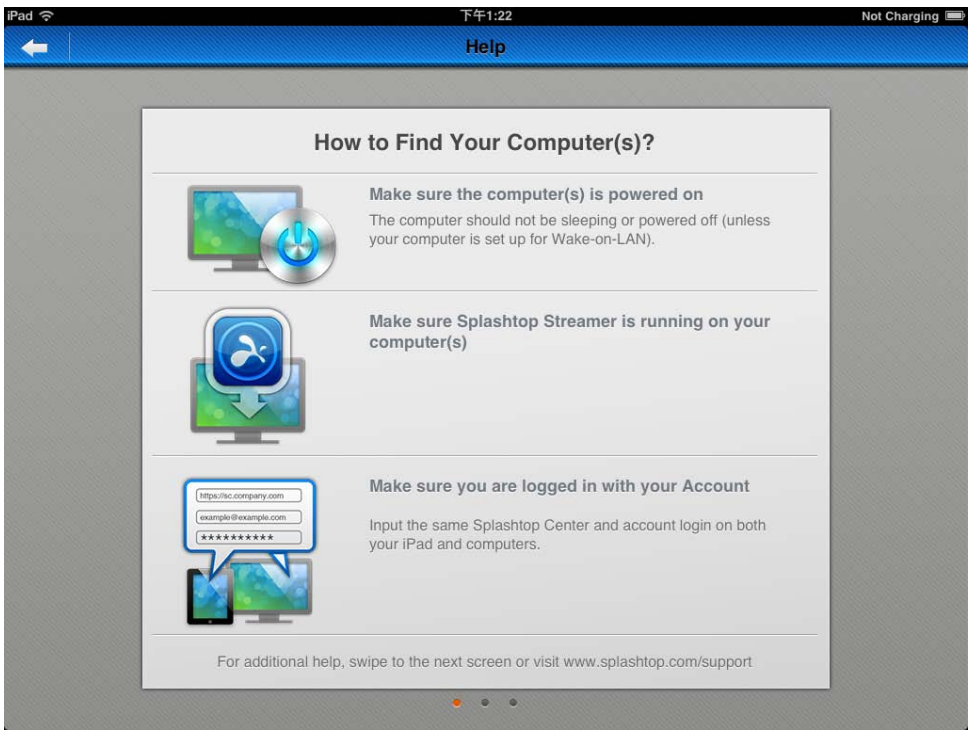
And this brochure:
http://d36wcsykcv5g5l.cloudfront.net/doc/CSG_brouchure.pdf

To watch a demo video and tutorial video, go to our web page at:
http://www.splashtop.com/resource

Meanwhile, on the screen of the desktop computer being remotely accessed, a message will display in the lower right corner, which states the name of the iPad which is accessing the computer. It displays for about five seconds and then disappears automatically.

On your iPad (or other client mobile device), after you tap the **Disconnect** icon on the Toolbar  to terminate the remote session, your regular iPad screen will re-appear, and you should be returned to the screen that contains the **Splashtop** icon shown below. Tap the **Splashtop** icon if you wish to begin a new remote-connection session.

NOTE: Tap the  icon to access screens of **Help** messages such as:



2.5. Installing Splashtop Streamer

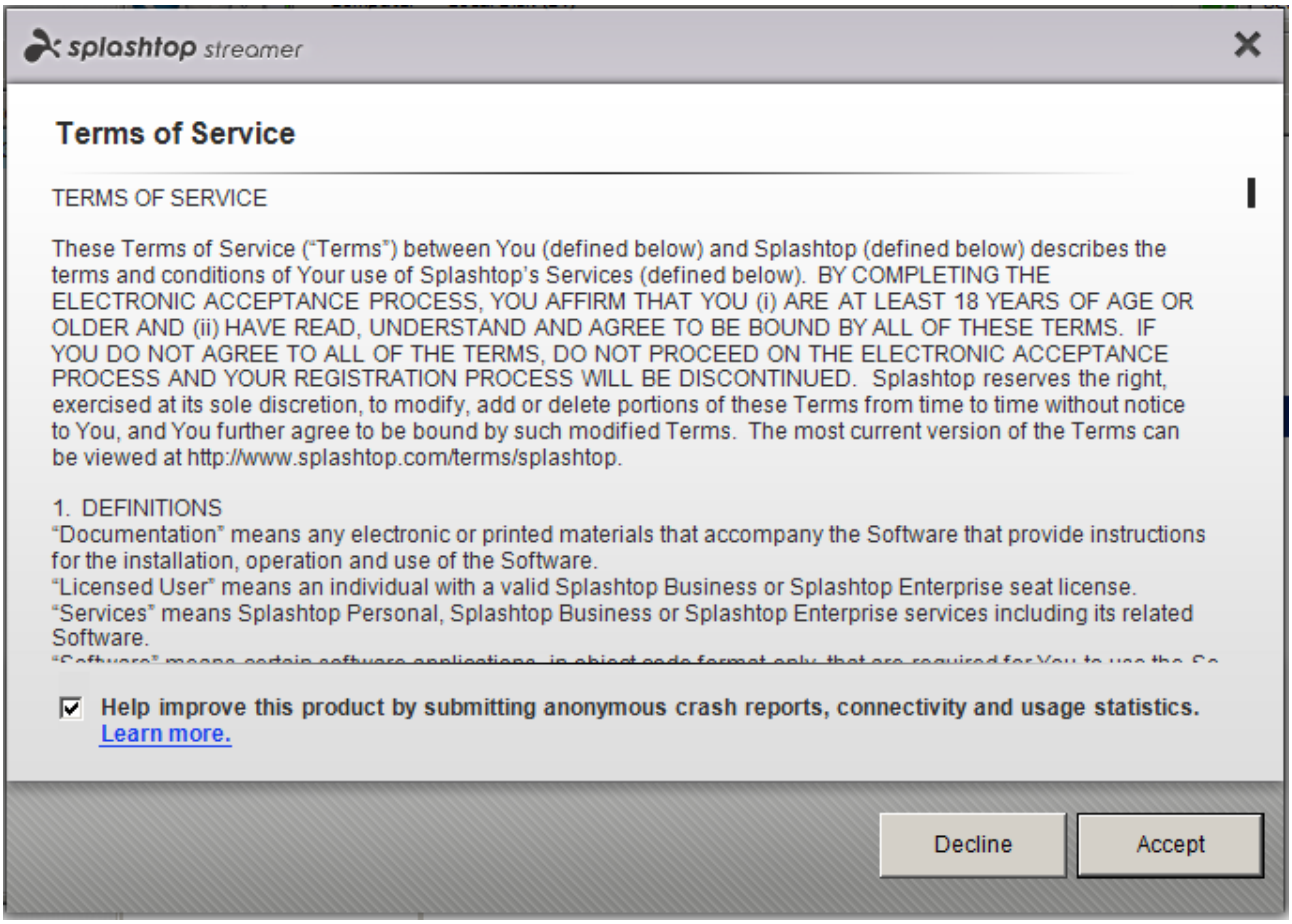
The Splashtop Streamer is the streaming source for remote access. Install the Streamer on any computer that you want to make capable of being accessed remotely. Then users (who are authorized within Splashtop Center) can access the content of the host computer using their mobile device (client) running 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**.

NOTES:

- **Mac Streamers:** 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. If you agree to uninstall the existing version, the InstallShield Wizard will first perform a complete Uninstall, including all backup files for that Streamer. After that is done, the InstallShield Wizard will automatically install Splashtop Streamer (for Mac).
- **Windows Streamers:** Please note that for the Windows version of the Streamer, we now provide a "**Co-existing Streamer**" feature. This feature allows both the **Splashtop Streamer** (for Windows) and the **Splashtop 2 Streamer** (for Windows) to exist on the same machine at the same time.
- The Streamer now supports both Basic and NTLM authentication when connecting to a Proxy server:
  - **Basic Authentication:** When authenticating with the Proxy server, the Streamer sends the User Name and Password as un-encrypted, base64-encoded text, but over the HTTPS secured protocol. After the User Name and Password have been authenticated, each request is treated as a new session, and these credentials will be verified every single time.
  - **NTLM Authentication:** When authenticating with the Proxy server, the Streamer uses a secure challenge/response mechanism over HTTPS, which does a better job of preventing password capture, replay attacks, and spoofing. This authentication only takes place per connection. (More information about NTLM can be found at the end of the Appendix.)

2. After you click **Finish** to close the InstallShield Wizard window, the Splashtop Terms of Service agreement will display. You will need to click **Accept** to continue.



3. The **Status** tab of the **Splashtop Streamer** window will then display.

4. 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 3 of the previous section, entitled "Installing the Splashtop Enterprise Client App").

NOTE: The illustration above shows the Streamer ready for login to Splashtop Center. Unless restricted, a user can click **Log in to Splashtop Personal or Business** in the lower right corner of the Streamer console (Status tab) to switch to Splashtop Personal/Business mode. As the IT Administrator, you can prevent your Splashtop Center users from doing this, if desired, by making sure the "**Stay in Splashtop Center Mode Only**" checkbox is checked in the Policy assigned to the user(s). This is illustrated and explained later in Mode Switching in the **Policies** section.

NOTE: The Splashtop Streamer installer for Windows supports silent installation and un-installation. Please append the appropriate parameter as follows:

- Install: "**/s**"
- Un-install: "**/s /removeonly**"

Silent install

For silent installation use a command following this formula:

Install path\execution file(.exe) setup/s

For example:

D:\S4B_SRS\V2.2.0.1\ST_SCRS00_v2.2.0.1.EXE setup/s

Silent un-install

For silent un-installation use a command following this formula:

Install path\execution file(.exe) setup/s/removeonly

For example:

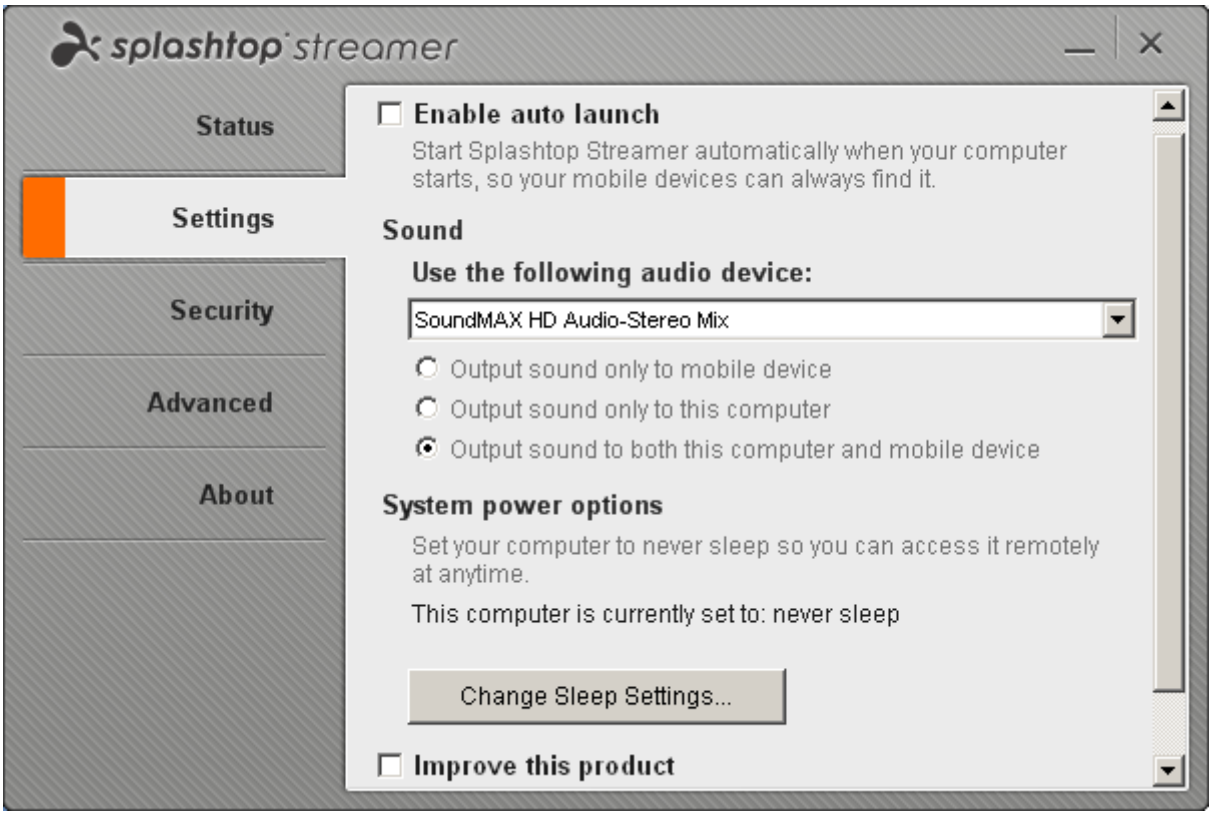
D:\S4B_SRS\V2.2.0.1\ST_SCRS00_v2.2.0.1.EXE setup/s/removeonly

For complete details and illustrations of the Streamer, please see our separate document entitled "*Getting Started with the Splashtop Streamer*."

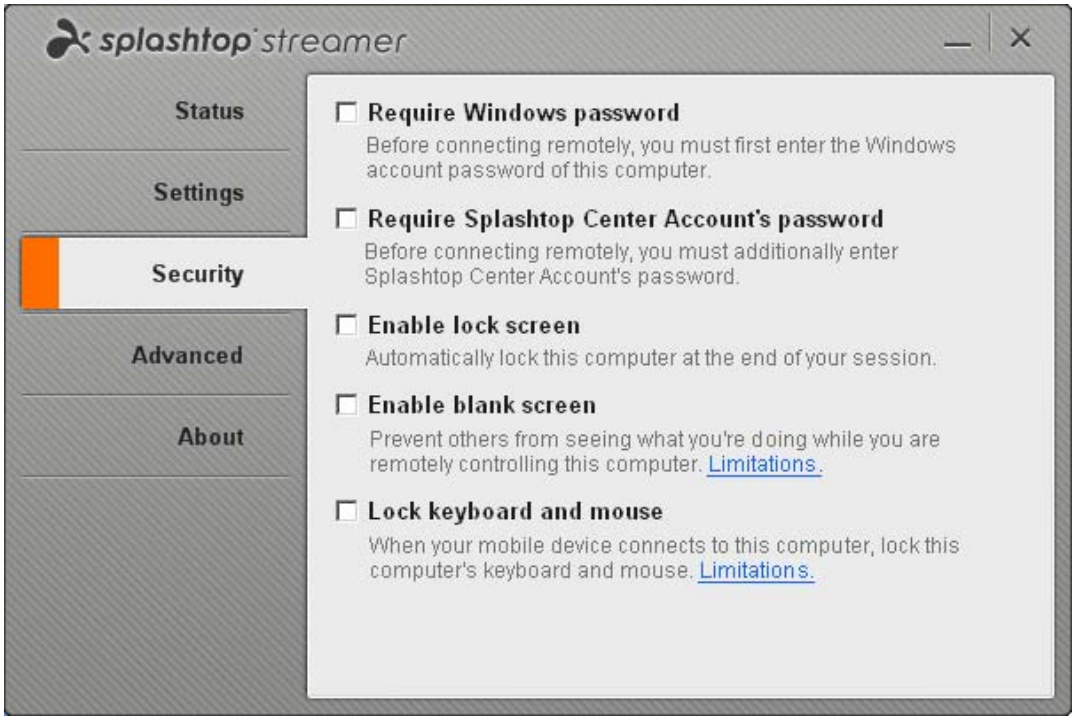
2.5.1. Illustrations of the other Splashtop Streamer tabs

The **Status** tab of the Splashtop Streamer window was illustrated above. For your reference, below are illustrations of the other four tabs. The options and settings are self-explanatory, but some of them are touched upon in Section 4.7.1 because they can also be controlled by the Policy Settings.

Settings tab

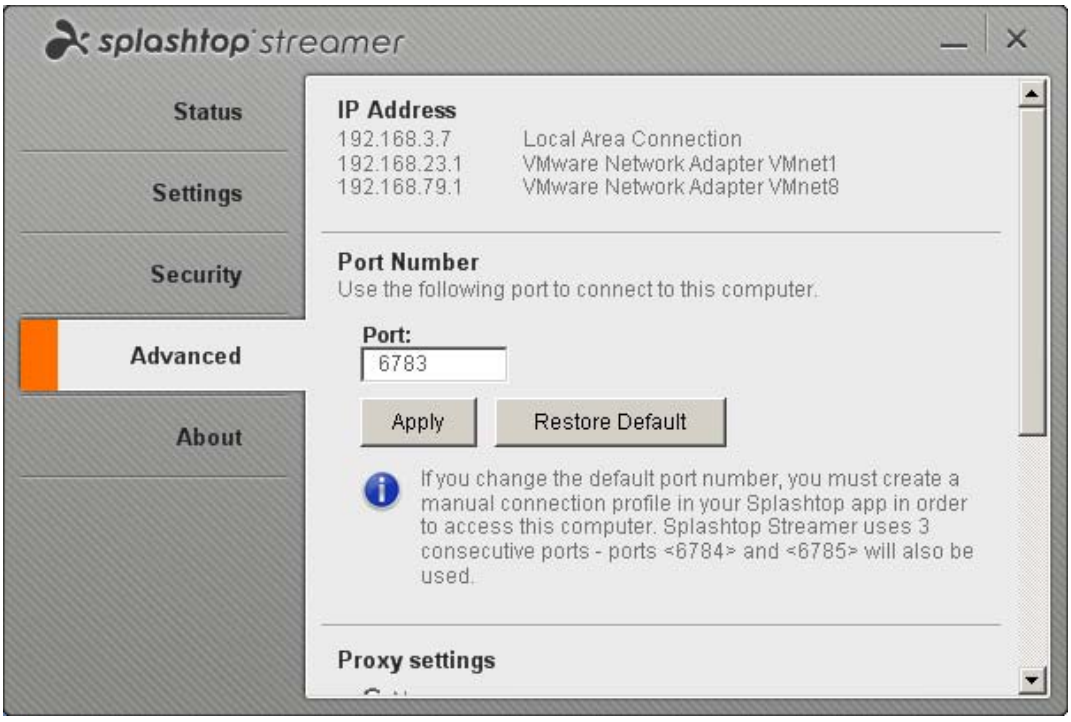


Security tab:

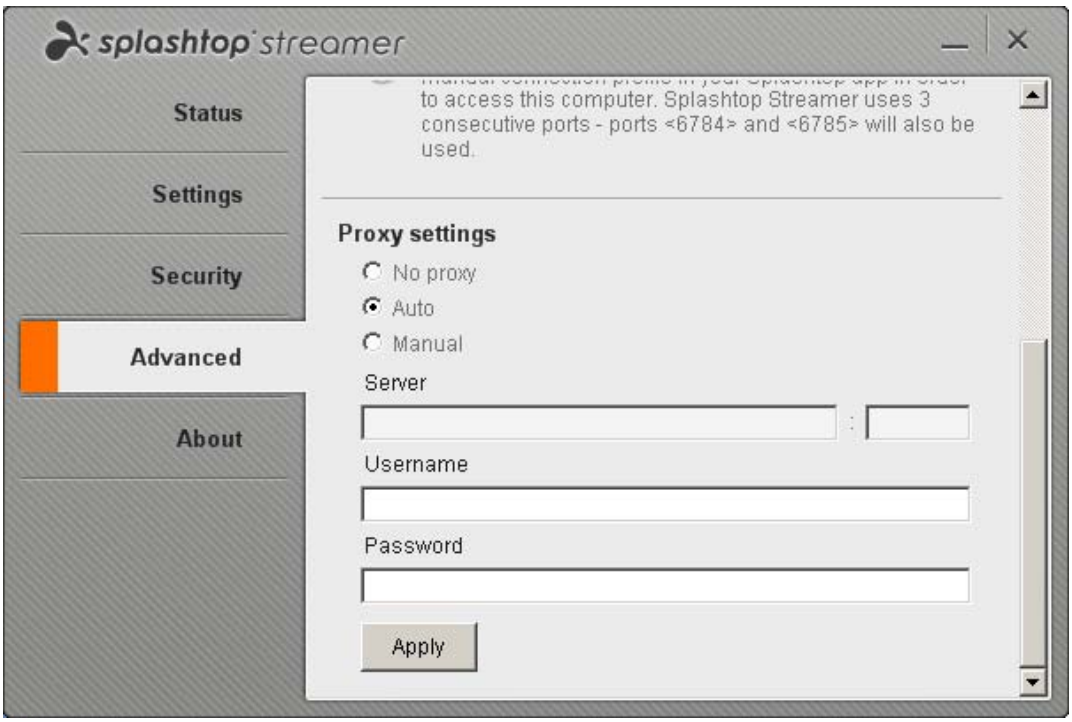


Advanced tab:

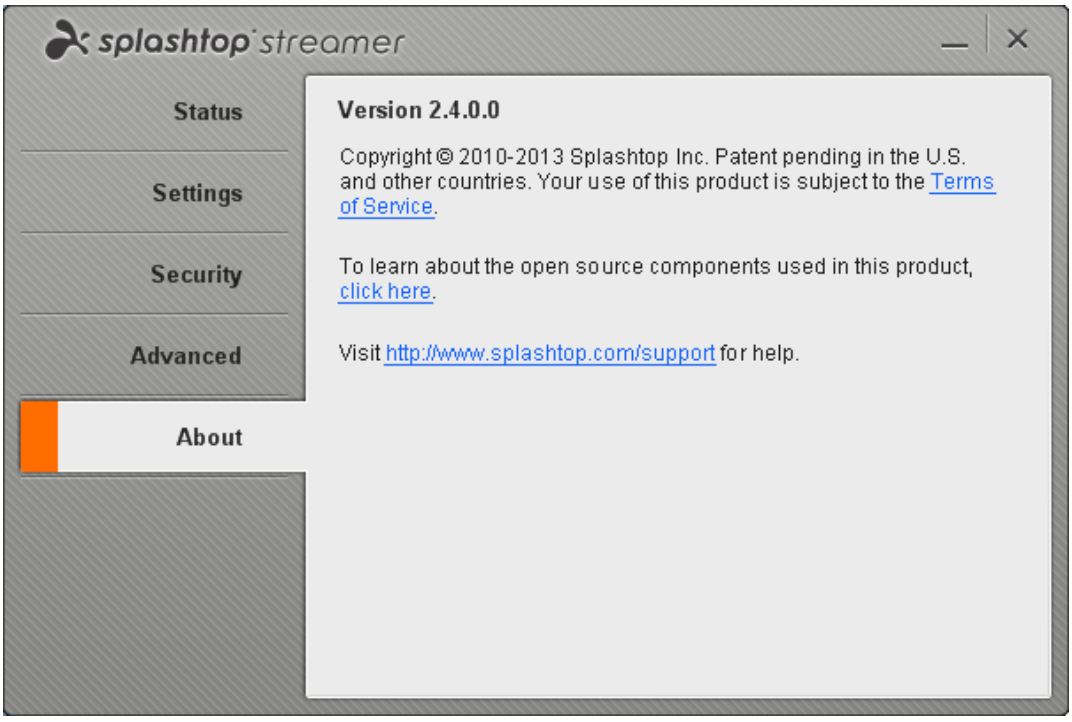
Upper half of the **Advanced** tab:



Lower half of the **Advanced** tab:



About tab:



2.5.2. Trouble-Shooting Splashtop Streamer Installation Issues

If you can't launch the Streamer *after* the Streamer installation is finished, please try the following suggestions:

- If you are using Windows XP, and Splashtop Streamer will not start after installation has completed, use *Task Manager* to stop the **SRServer.exe** process. Then manually launch again.

- We found that if a service process named **Terminal Services** is disabled, this would prevent the Splashtop Streamer from being launched. If it is disabled in your case, please enable it manually from Task Manager/Process. Note that the **Terminal Services** process exists only in XP Professional (*not* in XP Home). You can find **Terminal Services** as follows:

  1. Right-click on **My Computer** and select **Manage** from the menu.
  2. In the **Computer Management** window, open **Services And Applications** in the left pane and click **Services**.
  3. In the **Services** pane, there should be a **Terminal Services** item in the list in the right pane. If it is disabled, right-click on **Terminal Services**, select **Properties** from the menu, then select **Manual** and click **Apply**. The **Start** button will then be enabled.
  4. Click the **Start** button to start Terminal Services. The Splashtop Streamer should then start up automatically!

- Try un-installing the previous installation, restart the PC, then install again.

If an error occurs (or hang-up) *during* installation of the Windows Streamer, you can try the following suggestions:

- If you get an error message immediately when executing the Installer file, it may have been corrupted during the last downloading. Please re-download and try again.

- If you are using Windows XP, and get an error message like "Windows installer service could not be accessed," please follow the steps below to enable the **Windows Installer** service from the Control Panel:
    1. Click the **Start** button, click **Control Panel**, then click **Administrative Tools** in "classic view" — or, **Performance and Maintenance** and then **Administrative Tools** in "category view. "
    2. Click **Services**. Find the service name "**Windows Installer**" and click that line so it's highlighted. The *Status* column will be blank if the service is *not* currently running.
    3. If not running, there will be something like "**Start the Service**" on the left side of the screen — click it. That starts up the process on your system.
    4. Run the Splashtop Streamer installer again, and it should work!

- It has been reported that the **Kaspersky** software running on Windows XP will block Splashtop Streamer installation.
- If you have installed "**Airfoil**," the Splashtop Streamer installer will be blocked, and may hang while installing. The solution is to un-install Airfoil, then install Splashtop Streamer again. Or, add the Splashtop Streamer **install.exe** program to the "exclude" list under Airfoil's Automatic Hijack settings. (Some users have reported that Airfoil also interferes with DirectTV2PC's installer.)
- One of our users informed us that he solved the installation error-1719 (on Win7 64-bits) by exiting out of the **Comodo** anti-virus application. It has a built in "sandbox," which may be the cause.
- If you get error code 1618, please try these steps to solve it.
    a. Go to Task Manager.
    b. Go to the Process tab.
    c. Click on " Show all processes for all users."
    d. Find a SYSTEM process named **mciexec** and kill that process. This should solve the problem.

- If you get error code 1152, this might be due to one of the following situations:
  a. There is not enough disk space on the hard drive to which files are being extracted.
  b. You don't have sufficient privileges to write files to TEMP file.
  c. The downloaded files may be corrupted.

  Based on the possibilities listed above, here are some suggested solutions:

  1. Download the Streamer again.

  2. Free up some disk space wherever possible on the C drive (where the Splashtop Streamer is installed).

  3. Try to disable User Account Control (UAC) before installing. Click on the following hyperlink to view an article about how to do this in Windows: http://www.howtogeek.com/howto/windows-vista/disable-user-account-control-uac-the-easy-way-on-windows-vista/)

  4. Right-click on the installer file, select **Run As...** from the menu, and then in the dialog box, choose to run as Administrator in order to execute the installation.

3. Deployment Guidelines

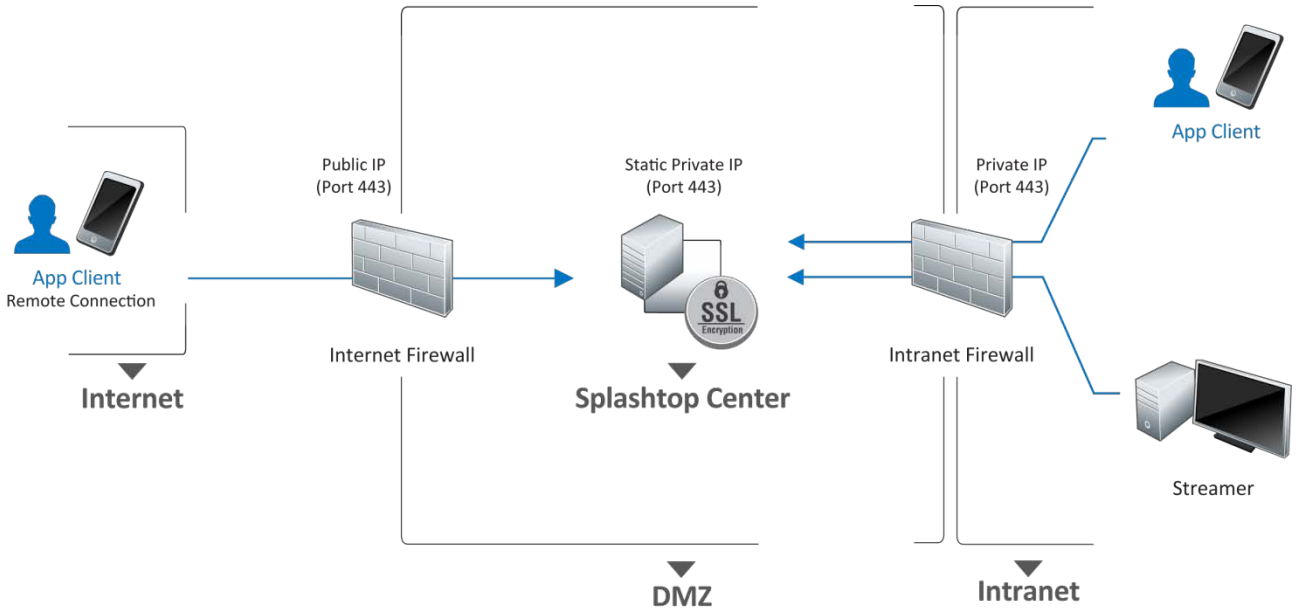
3.1. Installation Deployment Choices

Splashtop Center is designed to be hosted inside the enterprise firewall to protect sensitive user information. Without complicating the existing network setup for security, here are a few common deployment approaches for on-premise hosting.

3.1.1. Splashtop Center deployment in the DMZ

A "demilitarized zone" (DMZ) is used as a boundary between the Internet and the company's internal private network. The Splashtop Center Gateway provides a single secure access point for remote access traffic over the Internet from the mobile device (client) to any of the managed computers in a private network. This reduces the number of ports required to be opened in a firewall. Communication from both the mobile client device and Streamer to the Splashtop Center Gateway are encrypted using HTTP over SSL. The presence of the secure relay between Intranet and Internet extends the secure path between the mobile client device and Streamer.

It is recommended that Splashtop Center be installed on its own machine in your network DMZ.



As shown in the diagram above, deploying in the DMZ requires opening port 443 (by default it is 443, unless someone changes it) on the firewall to allow access to services via the Splashtop Center. The IT administrator needs to open port 443 and configure port forwarding for port 443 between public IP (Internet) and private IP (Intranet) in the firewall. All traffic between Internet client (mobile device) and Intranet Streamer communication and data transfer will be relayed by the on-premise Relay service of Splashtop Center.

3.1.1.1. Internet firewall (for DMZ)

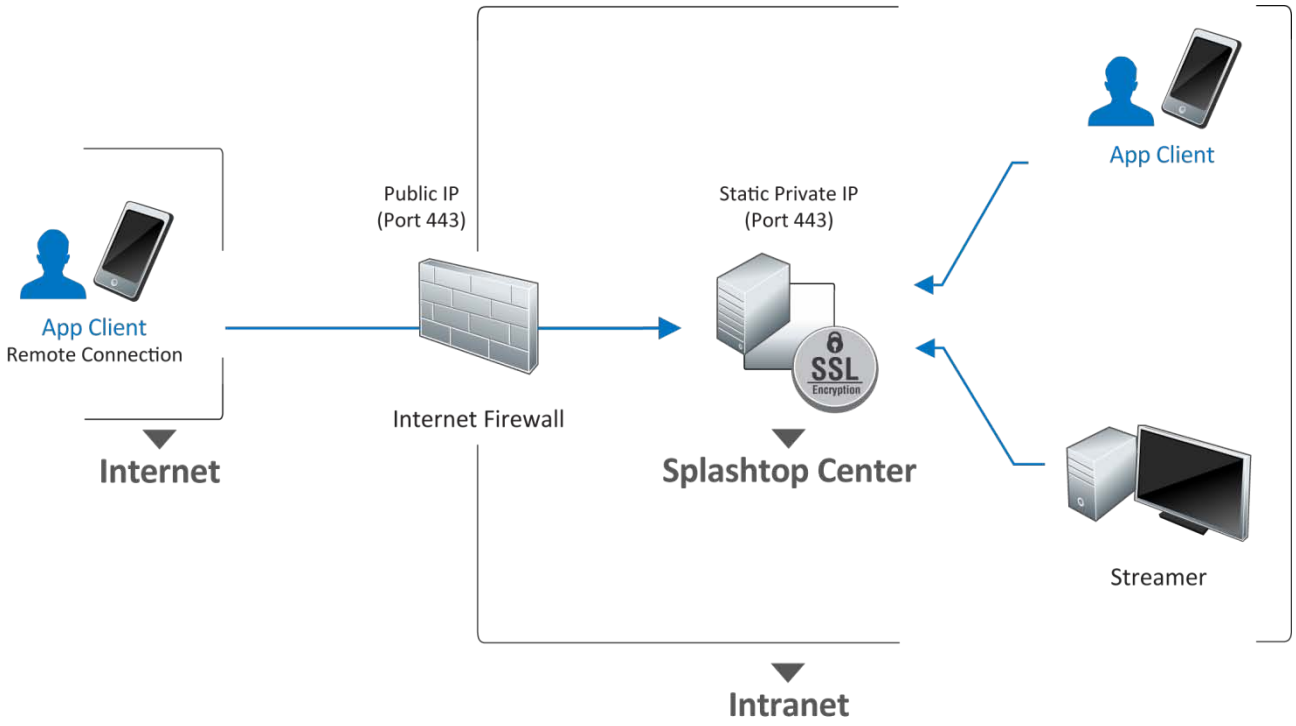
So, to summarize, open ports need to be available so that the client can communicate over the Internet with a Splashtop Center Gateway residing in the DMZ. We recommend opening port **TCP 443** in the Internet Firewall for DMZ, to facilitate HTTPS communication from the Splashtop Center mobile client device over the Internet to Spashtop Center Gateway.

3.1.1.2. Intranet firewall

Likewise, for HTTPS communication, open ports need to be available so that the Splashtop Center Gateway can communicate with Streamers in a private network, and port **TCP 443** is recommended.

3.1.2. Splashtop Center deployment in a private network

An alternative deployment option is placing Splashtop Center in the Intranet. This option is for companies who do not have DMZ. Splashtop Center can run in the Intranet and the IT administrator also needs to open port 443 and configure port forwarding for Splashtop Center in the firewall.



3.1.2.1. Internet firewall (for a private network)

So, similarly, for HTTPS communication from a Splashtop Center mobile client device over the Internet to Splashtop Center Gateway (residing in the same private network), open ports need to be available so that Splashtop Center Gateway can communicate with the computers running the Streamer in that private network, and again port **TCP 443** is recommended (by default it is 443 in Splashtop, unless someone changes it).

3.1.3. Physical vs. Virtual

Splashtop Center can run in a virtual machine. However, there may be additional virtual machine settings which need to be configured, such as using "Bridged" mode network - not "NaT".

4. Navigating 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**. The usage of each tab is explained in this section. By default, the **Users** tab is initially displayed as shown below.

Near the upper right corner of the Console screen, there is a **Get Help** button. Clicking this button will open the main Splashtop Enterprise web page.

At the bottom of the Console screen, there is a **Restart** button and a **Stop** button:

Restart

If you click the **Restart** button, the Splashtop Center service will stop and then start up again.

⚠ CAUTION: Please be aware that all currently active remote sessions will be disconnected if you restart!

Stop

Clicking **Stop** would terminate the Splashtop Center service and all active remote sessions.

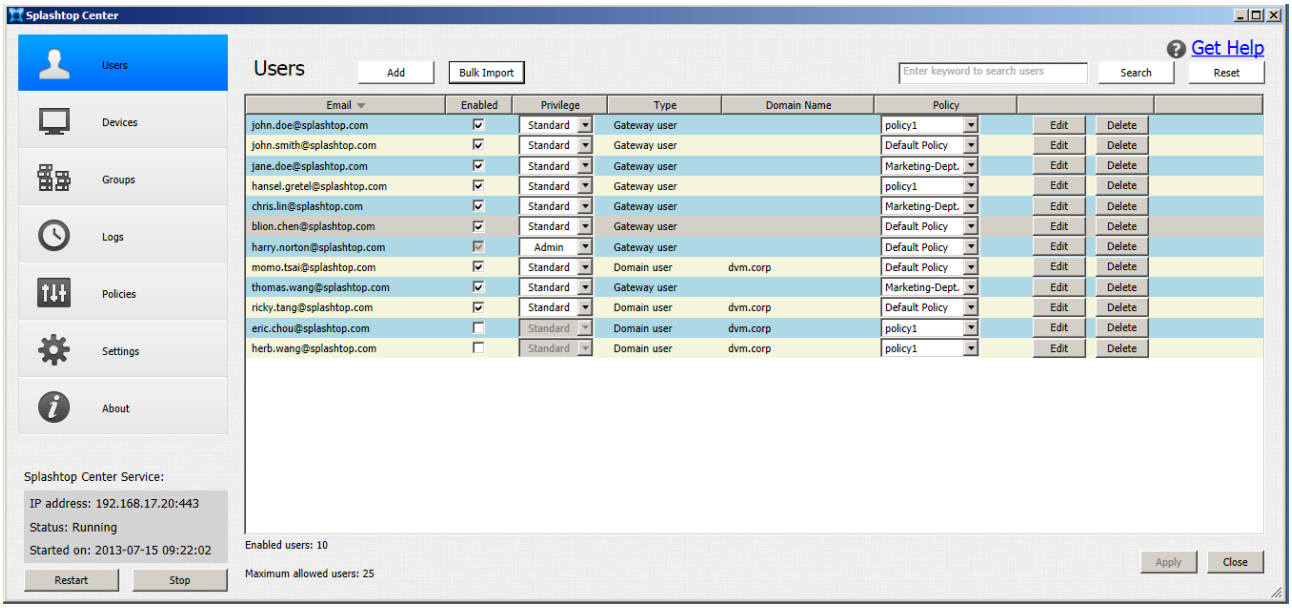
NOTE: You would then need to manually click the **Start** button when you want to start the Splashtop Center service again.

4.1. The User's Tab

The **Users** tab displays all the users who have already been added. From this list, you can quickly change the **Privilege** setting or **Delete** the user. 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, because one activation code can be used with only one mobile client device). A **Search** field in the upper right of the window lets you search for users; click **Reset** if you want to blank the **Search** field.

4.1.1. Enabling or Disabling Users

There may be times when you just want to prevent a user from using Splashtop Enterprise temporarily (as opposed to permanently deleting a user as mentioned above using the **Delete** button). By default, when an *individual* user is added, the checkbox in the **Enabled** column is checked. Simply un-check the **Enabled** checkbox at any time to conveniently disable the related user, and check the checkbox when ready to permit this user to use Splashtop Enterprise again.



If you want to add new users, you can click the **Add** button to add new users *individually*, or you can use the **Bulk Import** button to add *multiple* users all at once. However (unlike adding users individually), when you add users via **Bulk Import**, they will have a status of **Disabled** by default. After users are bulk-added, you can choose which users you want to Enable. (Note at the bottom of the **Users** tab, the number of currently **Enabled users** is shown, along with the **Maximum allowed users**.) Also, please be aware that in order to use the **Bulk Import** feature, you must first set up the Email/SMTP configuration, in the Settings tab (if not already done).

Email

Email is used to identify user in Splashtop Center. Each user shall have unique email address, and it is displayed in the **Email** column of the **Users** tab.

Enabled

By default, when a user is added, the checkbox in the **Enabled** column is checked. Simply un-check the **Enabled** checkbox at any time to conveniently disable the user, and check the checkbox when ready to permit this user to use Splashtop Enterprise again. Additionally, the **Enabled** status has a direct relationship to the number of users allowed, as defined in the License Key. If it is specified in the License Key to restrict the number of users, then the number of Enabled users can't exceed the maximum user count. For example, if your maximum number of users allowed is five, and you currently have four users in Enabled status and ten users in Disabled status, you still have one spot available to assign as Enabled status.

For convenient reference, the total number of currently **Enabled users** is shown at the bottom of the **Users** tab, along with the **Maximum allowed users** (illustrated on the previous page) according to your license agreement.

Privilege

Privilege can be set to either **Standard** or **Admin**. This is to offer IT admin the ability to assign the Admin role for Splashtop Center, and all the responsibilities granted as Admin. There can only be one user set to Admin privilege in Splashtop Center.

Type

This column provides "user type" information. There are 2 types of users: Gateway and Domain users. They are explained further on the next page.

Policy

Each user will be assigned a policy at the time of creation, which can be later modified, and conveniently switched to another existing policy. The drop-down list will contain all policy names available for selection. Please refer to Policy chapter on how Policy works and modifies.

Supported User Types

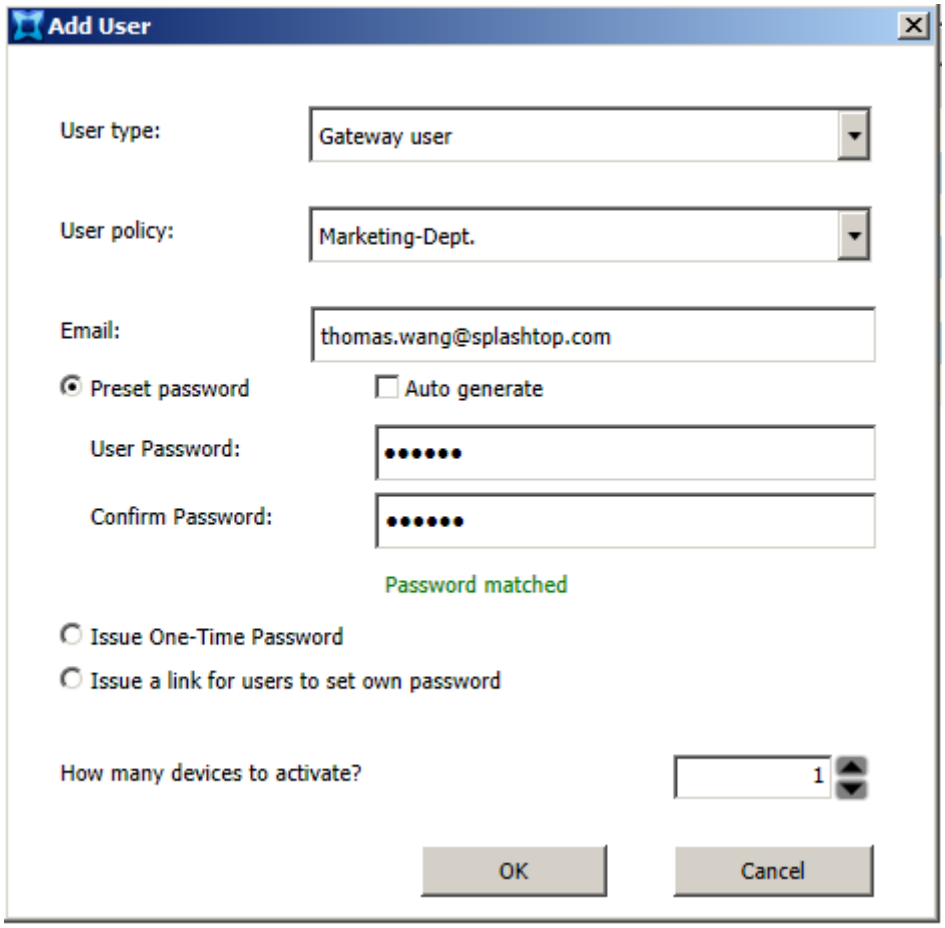
Splashtop Center supports two types of users: **Gateway** users and **Domain** (Active Directory) users.

1. 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.
2. 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.

4.1.2. Adding Gateway Users individually (using the Add button)

Creating Gateway users with an activation code:

1. Click the **Add** button in the **Users** tab. The *Add User* dialog box will appear.



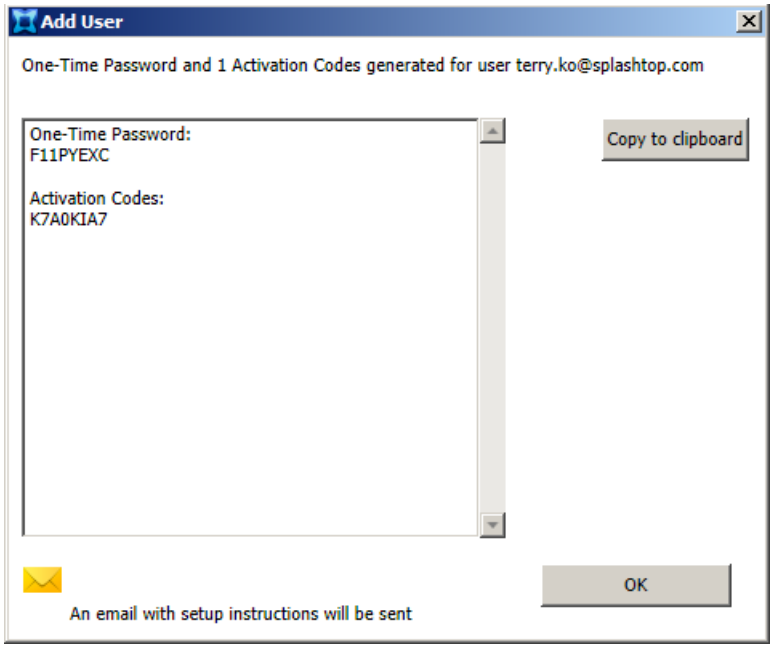
2. Make sure **Gateway user** is selected in the **User type** field (**Gateway user** is the default value).
3. From the drop-down list, select the **Policy** you want to apply to this user. A Default Policy is created during installation automatically, so this will be applied if you have not created any additional policies for selection. For information about policies in Splashtop Center, and how to create and edit new polices, please see section 4.7 (entitled **The Policies Tab**) for complete details.
4. Enter the user's **Email** address.
5. Choose the method you want to use for password creation. The three choices are as follows:

- **Preset Password**

  Select this button if you want to assign a specific password to this user, then type the desired password into the **User Password** and **Confirm Password** fields. (An example was illustrated on the previous page.) If you opt to check the **Auto Generate** checkbox, then the **User Password** and **Confirm Password** fields will be grayed out, and the password will automatically be generated by Splashtop Center. The Invitation Email sent to the user will contain the preset password, and will include a link which he/she can click, to change the password.

- **Issue One-Time Password**

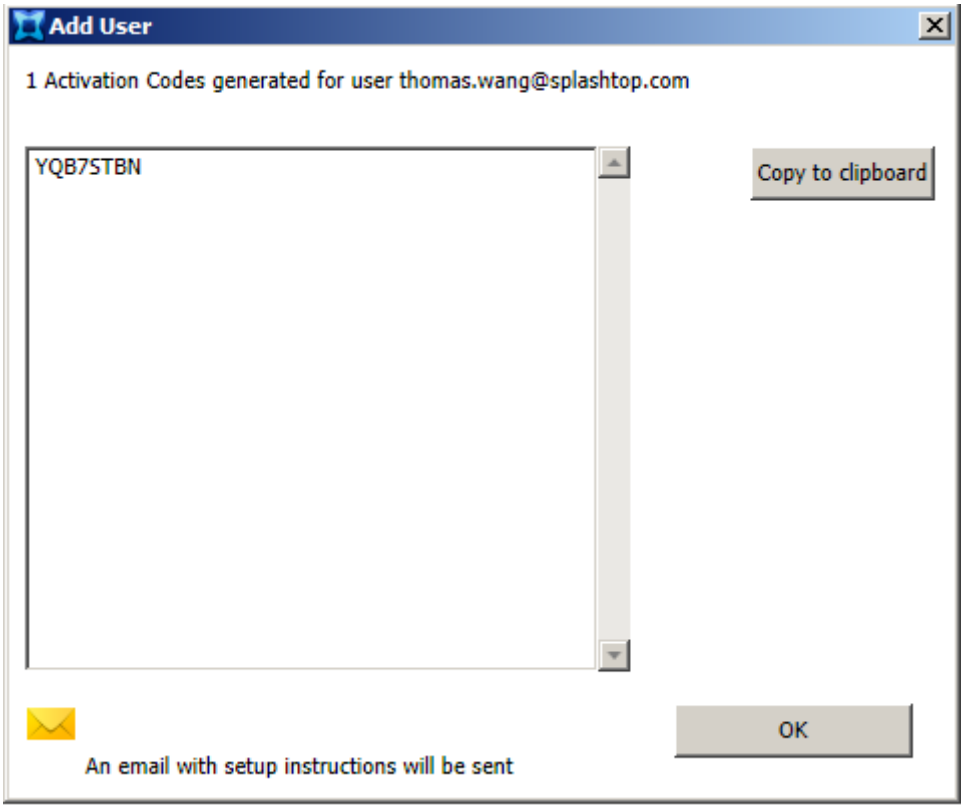
  Select this button if you want Splashtop Center to automatically create a password for the user. After you click **OK**, the dialog box shown below will appear. It shows the password that was generated, and Activation Code(s). This password can only be used one time to log in, and then after logging in, the user must change their password on the client side so he/she will have a valid password for future use.



- **Issue a Link for Users to Set Own Password**
  If this button is selected, no password will be preset, and the Invitation Email sent to the user will just include a link which he/she can click to create the password. This link goes to our Splashtop Center **Web portal** where passwords can be set/reset. In this case, no login credentials will be required to access the Web portal, because this user does not have a password yet. Please see section 5.3 for more details about the **Password** tab in the Web portal.

NOTE: Please be aware that if the **Enable Device Activation** checkbox is disabled (not checked) in the **Settings/General** tab (section 4.8.1) then when you add new users, the **How many devices to activate?** field will not be available in the *Add User* dialog box, and no Activation Codes will be automatically generated at the time when new users are added.

6. By default, the **How many devices to activate** field is set to a value of **1**. If the user you are adding just has one mobile device which you want to authorize for Splashtop Center use, you are ready to click **OK**. Or, if the user has more than one mobile device that you want to give an Activation Code to, specify the number in the **How many devices to activate?** field. In our example illustration shown under section 4.1.2 above, the user has one mobile device, so one Activation Code was generated (each Activation Code can be used to activate only one mobile device), as shown on the next page.
7. Click **OK** in the *Add User* dialog box. Another dialog box will appear, showing the generated activation code(s), shown in the example on the next page.

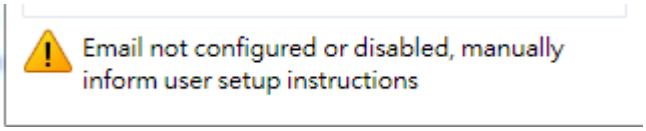


If the message "An Email with setup instructions will be sent" is displayed at the bottom of the dialog box as shown above, then you are done. "Invitation Email" has already been sent to this user automatically. The Email will contain a link for the user to conveniently click and download the Streamer. In the Streamer window, the Splashtop Center URL and the user's Email address (for use with Splashtop) will need to be entered, along with the password. (One Activation Code can be used for one mobile client device.)

NOTE: In order to set up the necessary information for "Invitation Email" to be automatically sent, use the **Email** tab in **Settings**, and make sure to check the **Automatically send email to users for account/password setup and device authentication** checkbox in that tab. For instructions and illustrations, please see section 4.8.3. (In addition, you would need to have the **Email** tab set up in order to use the **Bulk Import** feature, if desired.)

On the other hand, if the automatic "Invitation Email" feature is *not* enabled:

If the message displayed at the bottom of the dialog box is…



…then this tells you that the "Invitation Email" function is not enabled, and therefore you, the IT Administrator, should manually send Email to this new user to notify him that he/she has been added as an authorized Splashtop Enterprise User. In this case, you can conveniently click the **Copy to clipboard** button to copy the Activation Code, then paste it into the Email with your instructions and send it to the user.

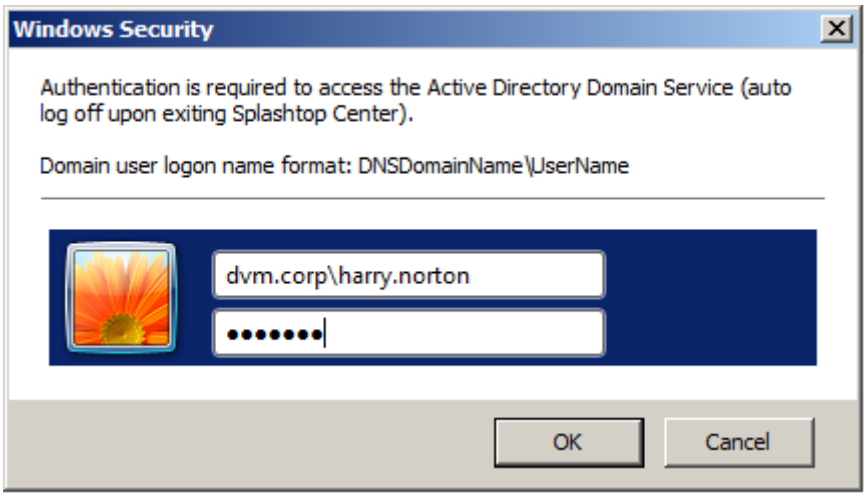
The user needs to activate from a mobile client device (iOS, Android, or Windows client) – not from the Streamer system, as follows:

- Launch the Splashtop Enterprise app on the client device, then click on the "Activate this product" link.
- Enter the account Email address and activation code, and tap the "**Activate**" button.
- Enter the password twice to set up.
- The user can then try to log in.

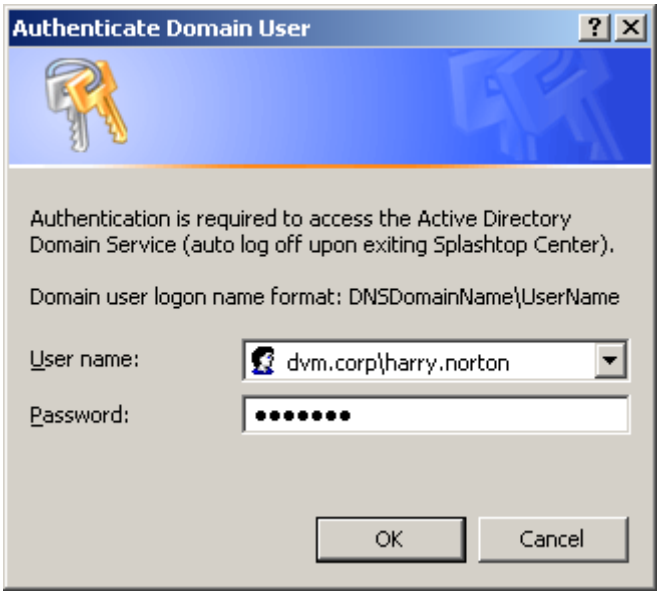
4.1.3. Adding Domain (Active Directory) users individually (Add button)

Click **Add**. In the *Add User* dialog box, select **Domain user** in the **User type** field. If the current computer is not yet logged in to the domain, then the domain user system verification dialog will pop up after you select **Domain User**. You will need to log in as a domain user on Splashtop Center to join the host server in to the Active Directory domain.

The dialog box may take various forms depending on the Windows operating system you are using. For example, if you are using Windows 7, it may look as shown below.

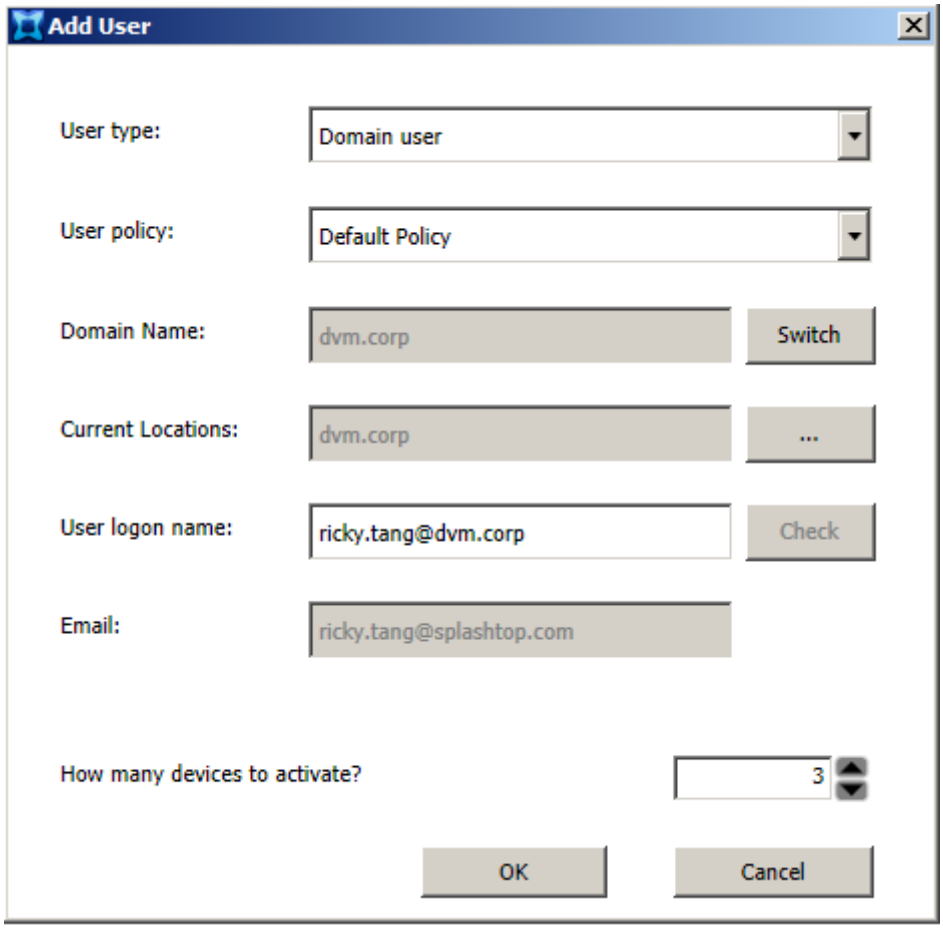


Or, if you are using Windows XP, it might look like this:



Enter the **domain_name\user_name** in the **User name** field and its related **Password** into the dialog box.

After successfully logging in as a domain user, the **User Type** field will display **Domain user**, as shown below. Then select the **User Policy** you want to apply to the user you will be adding.



The **Domain Name** field will display the domain you logged in to. If you wish to add a user from a different domain, click the **Switch** button. The "Domain Login" dialog box (illustrated on the previous page), will open again, and let you change to a different domain.

The **User logon name** can be any valid domain account. Then you must click the **Check** button to verify the domain account. If no problem, the Email address associated with that domain account will automatically display in the **Email** field. The **OK** button will then be enabled, and you can click **OK** to add the AD domain user into Splashtop Center. Splashtop Center will use the value shown in the **Email** field as the user account.

For example, if you add a user named "john" from the "abc.com" domain, the user account for Streamer and Client would be "john@abc.com". If the **Email** field is empty, the **User logon name** would be the user account.

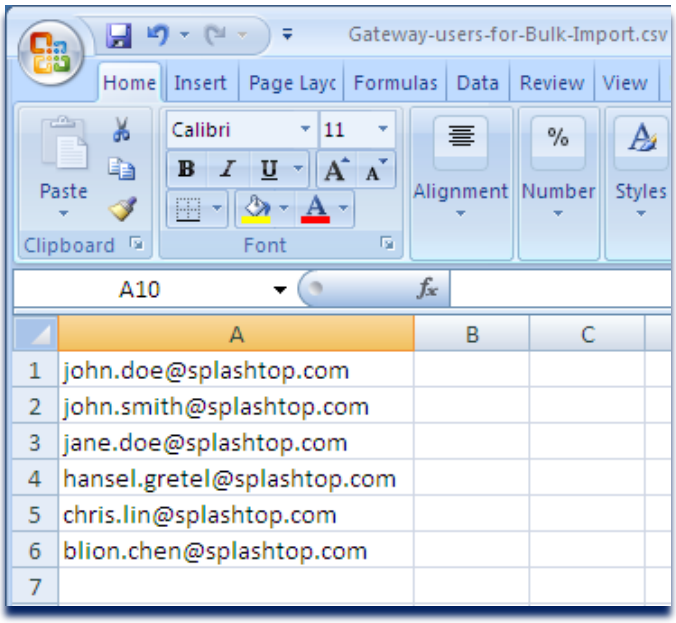
If a user is removed from AD directly, that user will still be present in Splashtop Center. However, the account will be disabled, because the credential check will fail when querying against AD.

NOTE: If you cannot add Domain users from Active Directory, see section 2.3.2.1 for further info.

4.1.4. Bulk Import – Adding Gateway Users

The handy **Bulk Import** feature lets you add multiple users all at once, limited only by the number of Seats defined in your License Key (purchased Seats). Initially, users you add via Bulk Import will have a status of Disabled after being added. That is, the checkbox in the **Enabled** column of the **Users** tab for each of the users will *not* be checked. This allows you to import a file containing more users than Seats you may have remaining and available. If the file you want to import contains 10 users, but you only have 5 Seats available, you can import the file of 10 users and then just select 5 of them to be enabled in the **Enabled** column.

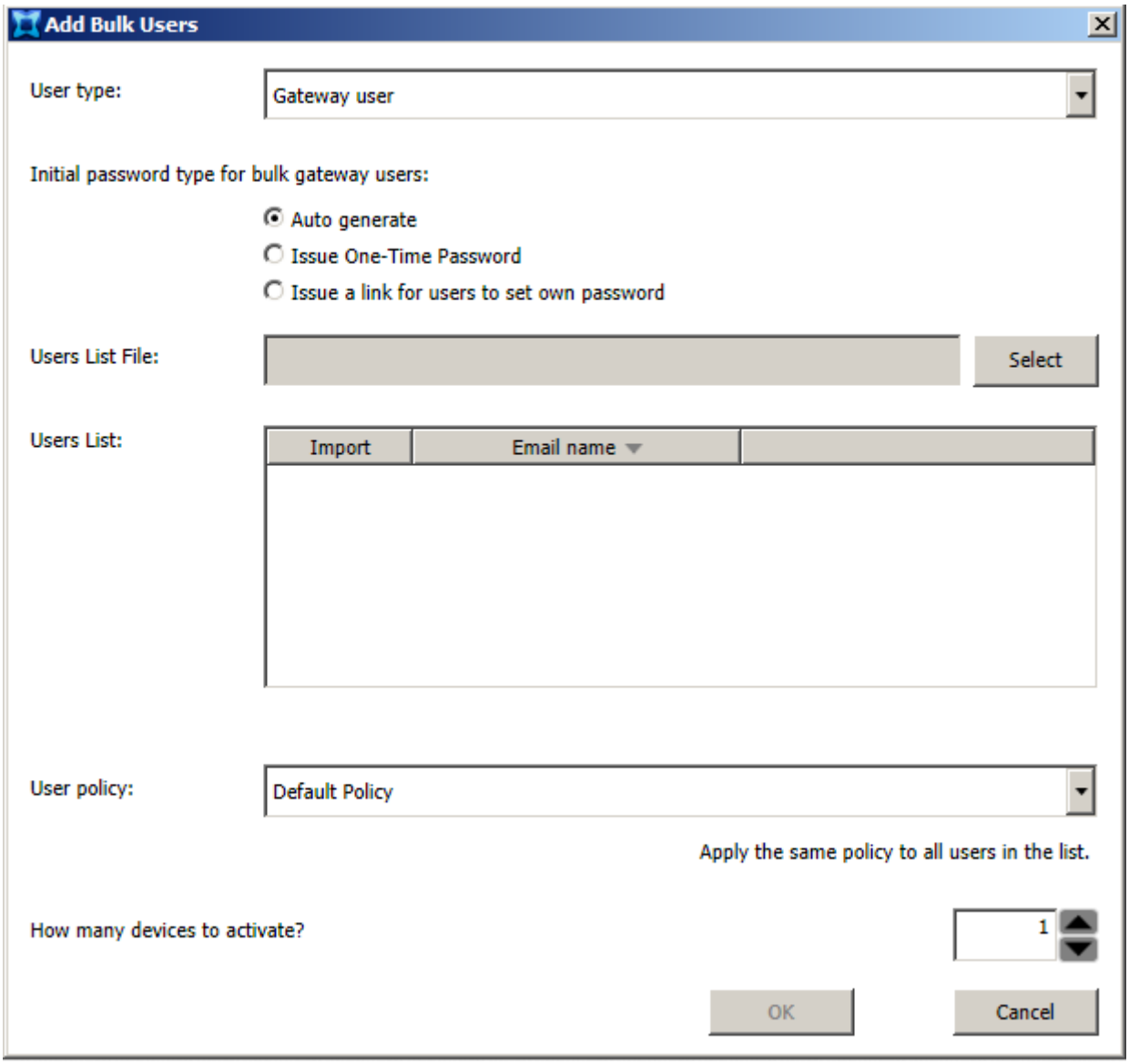
First, you as the IT Administrator need to have created a file for import (such as a .CSV file using Excel or a plain text file using NotePad for example), which lists the Email addresses of the Gateway users you want to add. Each Email address must be on a line by itself, as shown in the example below. Keep in mind that you cannot add more users than licenses you have purchased.



NOTE: Please be reminded that in order to use the **Bulk Import** feature, you must first set up the Email/SMTP configuration, in the Settings tab.

1. Click the **Bulk Import** button in the **Users** tab.

2. The *Add Bulk Users* dialog box will appear. Make sure **Gateway user** is selected in the **User type** field (**Gateway user** is the default value).

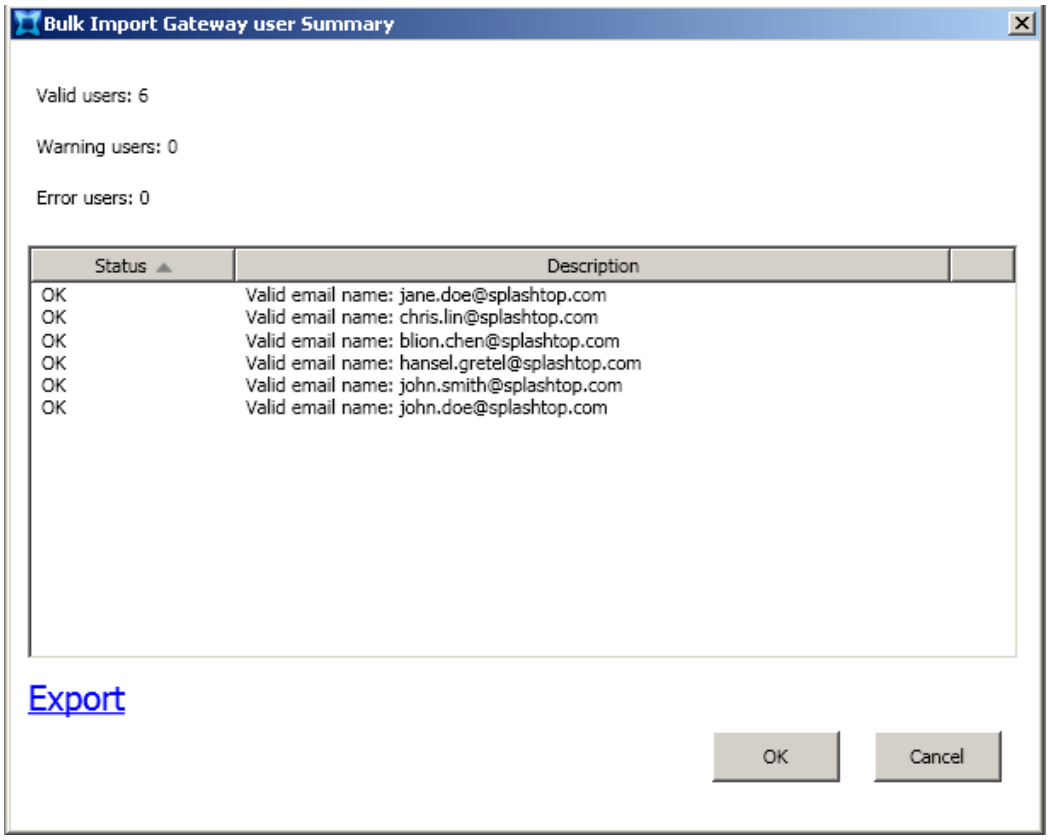


3. Select the initial password type for bulk gateway users. There are three buttons available: **Auto generate**, **Issue One-Time Password**, and **Issue a link for users to set own password**. Each of these options was explained earlier in section 4.1.2 (step 5).

NOTE: The "Preset Password" option is not supported for bulk user import, but is available when adding users individually.

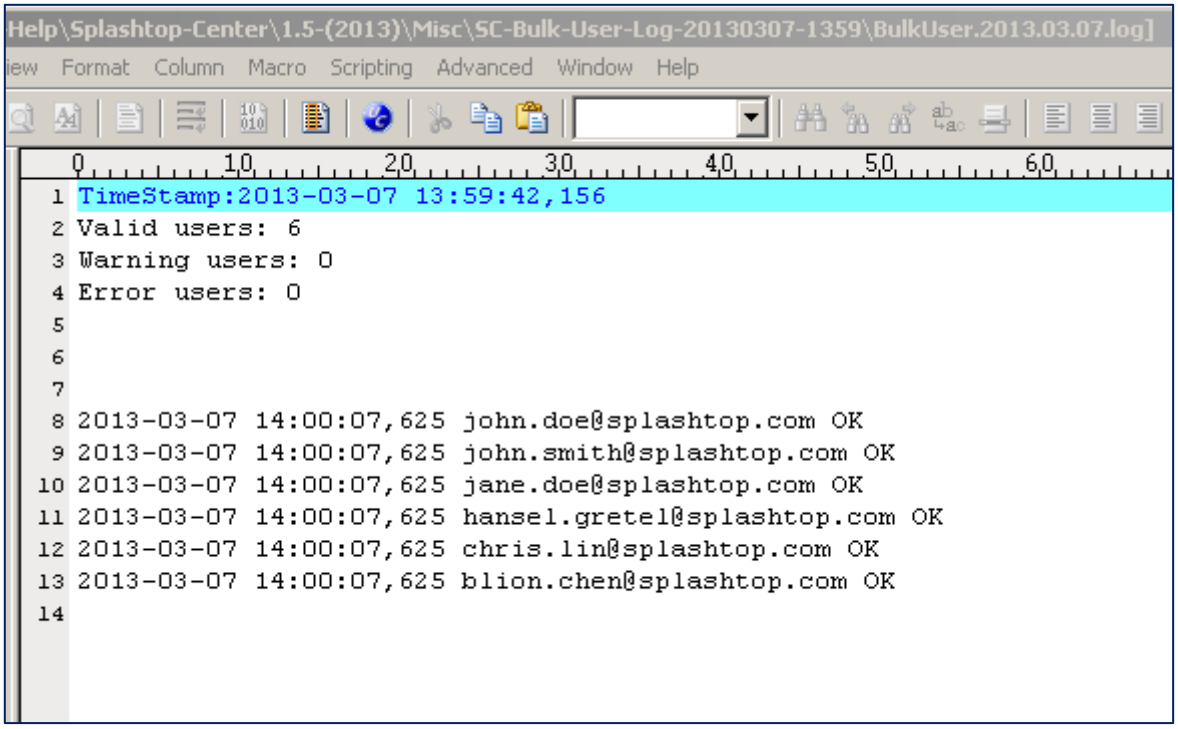
4. In the **Users List File** field, enter the path and name of the file which lists the Email addresses of the users you want to add. You can manually type the path and name of the file, or click **Select** and browse to the desired file. If you choose to click **Select**, an *Open* dialog box will allow you to navigate to the file you want to import.

After you do this, Splashtop Center will automatically analyze the Email addresses in the file and will inform you of the status of each one. For example, if an Email address is found to be identical to an already-existing Splashtop Center Email address, or if it is an invalid address, you will be notified. A status of "OK" will be displayed for each Email address that is found to be valid, as shown below.



Export

If you wish to save all the messages displayed in the log window for future reference, click the **Export** button. A Browse box will open so you can choose the folder where you want to save the generated text file. By default, a folder will be created whose name will contain the date and time, such as "SC-Bulk-User-Log-20130307-1357." In addition, a default filename is created which contains the date, such as "BulkUser.2013.03.07.log." The log file for our example above would look like the sample illustration below.



Cancel

If you click **Cancel** in the *Bulk Import Gateway user Summary* dialog box (shown on the previous page), the Import process will be aborted and you will be able to select a different file if desired.

OK

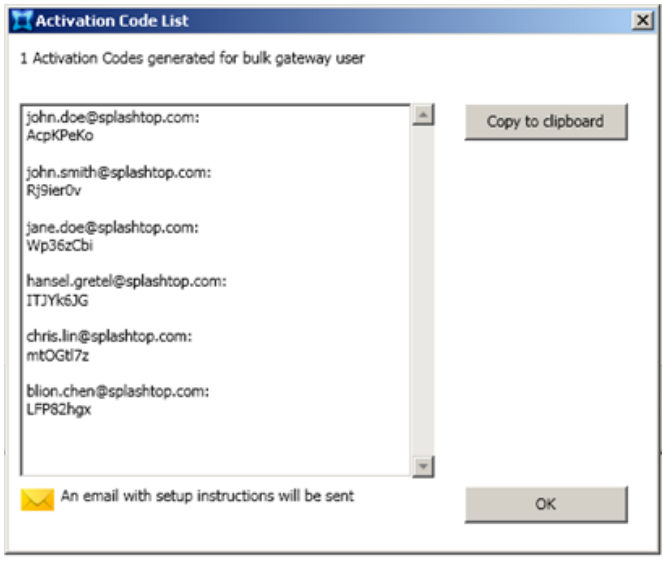
If you click **OK**, it will return to the *Add Bulk Users* dialog box, and the valid e-mail addresses in the selected file will be displayed in the **Users List** field.

5. There will be a checkbox to the left of each Email address in the **Import** column. At this time, you can choose to exclude certain users, if desired, by making sure the related checkbox under **Import** is *not* checked (they are all checked by default).

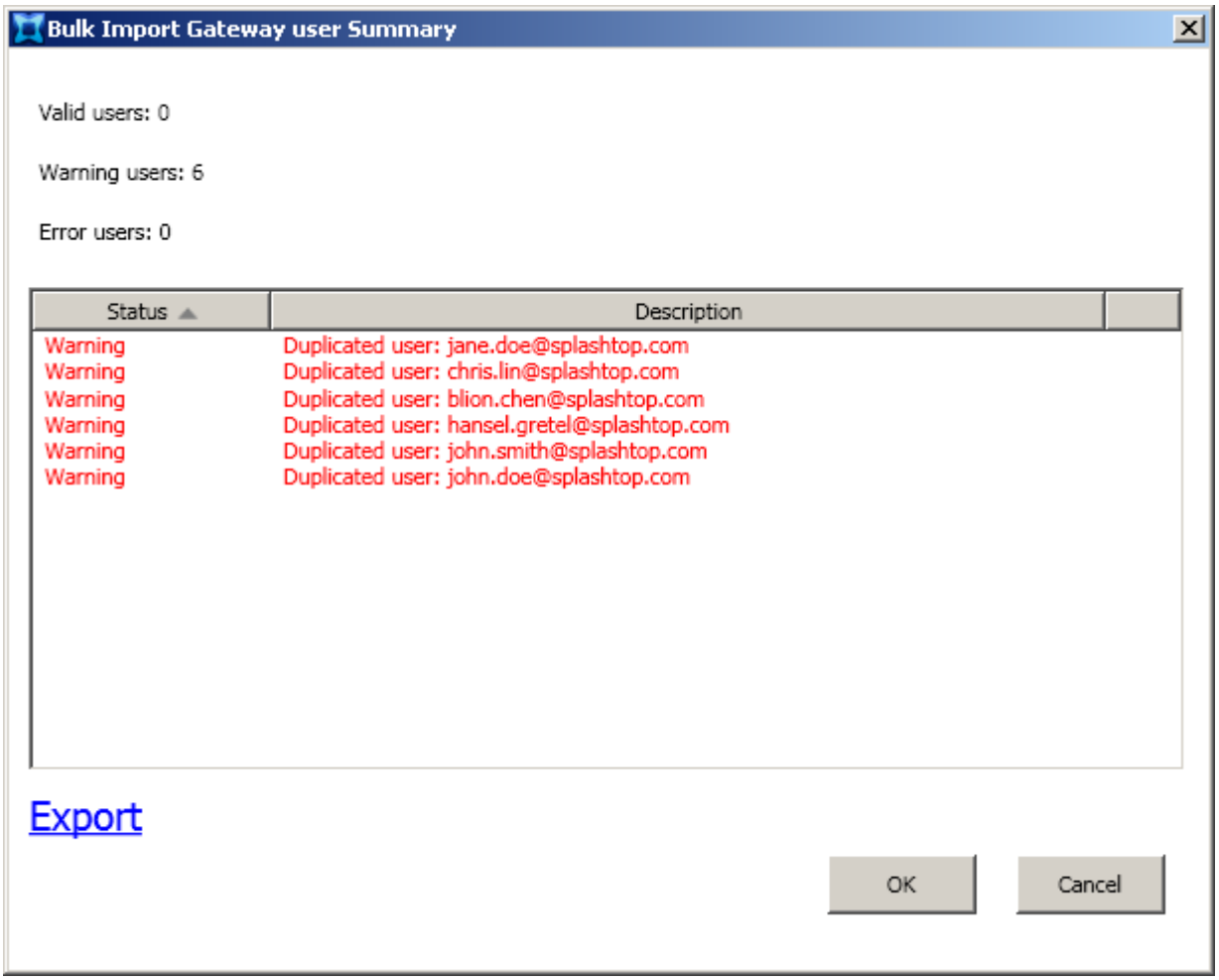
6. In the **User Policy** field, select the name of the policy you want to assign to *all* users in the list. A *Default Policy* is created during installation automatically, and will be used if no other policies have been created. If you have created additional policies, they will be available for selection from the drop-down list. (For information about policies in Splashtop Center, and how to create new policies or modify existing polices, please see section4.7, entitled **The Policies Tab**, for complete details.

7. The number you specify in the **How many devices to activate?** field (if available) will be applied to *all* users when they are added via Bulk Import. By default, this value is set to **1**. Each Activation Code can be used to activate only one mobile device. Since it will be applied to all users being imported, you may want to leave this value at **1** and then add more activation codes for users individually at a later time as needed.

8. Click **OK** in the *Add Bulk Users* dialog box to perform the actual Bulk Import User operation. The *Activation Code List* dialog box pops up as shown below, displaying the generated Activation Code(s). Invitation Email will automatically be sent to these newly-added Splashtop Center users, with instructions and the Activation Code they will need for their mobile device. The new users will now be listed in the **Users** tab.



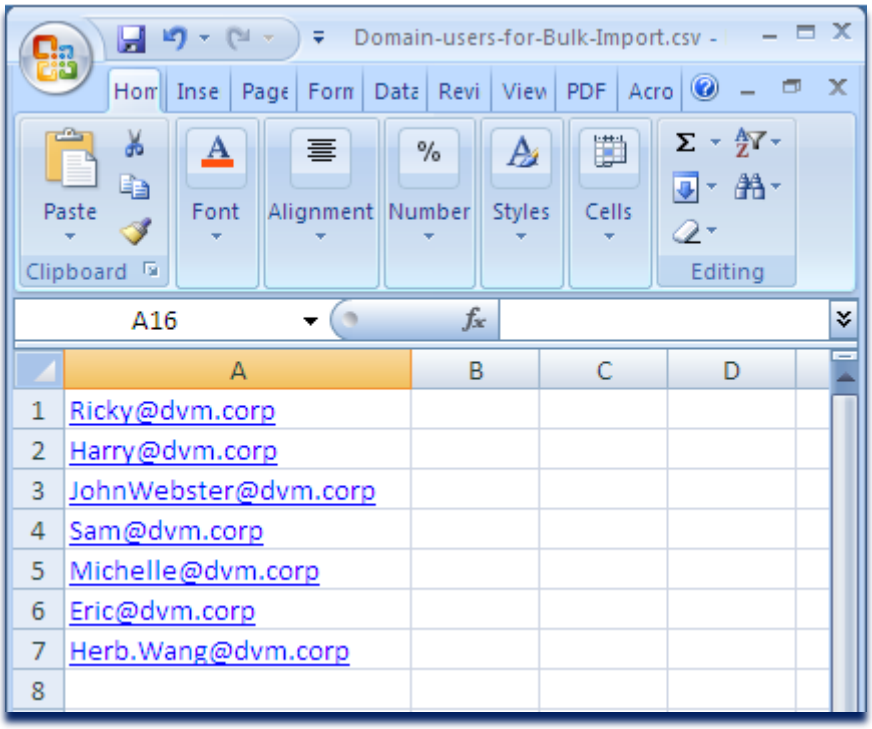
NOTE: Just to illustrate what would happen if you accidentally tried to import the same file again, the *Bulk Import Gateway user Summary* dialog box would display as shown below, with six "Duplication" warnings, in red.



4.1.5. Bulk Import – Adding Domain (Active Directory) users

Unlike the Bulk Import of **Gateway** users described above (wherein you can import a .CSV or .TXT file of *Email addresses* of the users you want to add), if you want to use Bulk Import for **Domain** users then the file must list the *Active Directory domain user names* (not the Email addresses). For example, if the Active Directory user name in the imported .CSV or .TXT file is John.Doe@acme.corp, Splashtop Center will automatically get the user's Email address and the user will be able to log in using the associated Email address such as John.Doe@acme.com.

Shown below is a sample .CSV file for import, which lists the Active Directory (domain) names of the users to be added. Each entry must be on a line by itself, as shown in the example below.



In addition, all the names listed in a file to be imported must be in the same domain. For example, John.Doe@acme.com cannot be added to the sample file illustrated above. The imported file cannot be comprised of users from different domains, but you can create separate files by Domain, and import them individually.

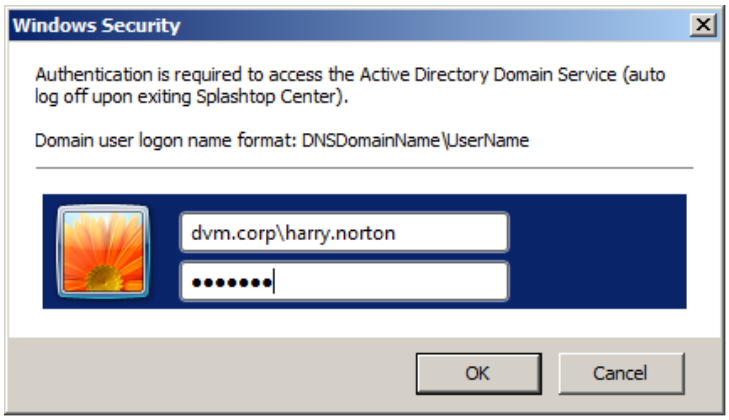
If the number of users in the file exceeds your licensed-seat limit, you can still select the file for import, and then exclude some of the Email addresses from import, in exactly the same way described in the previous section (importing Gateway users).

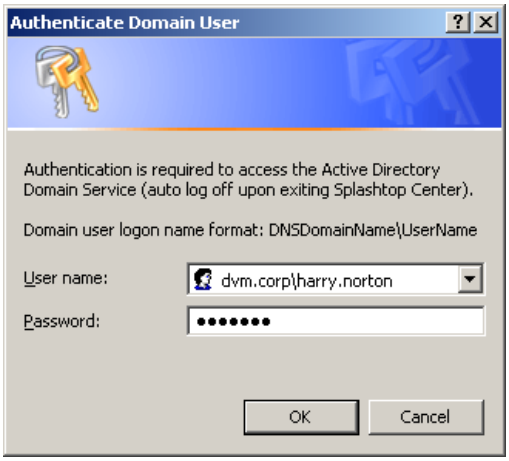
NOTE: Please be reminded that in order to use the **Bulk Import** feature, you must first set up the Email/SMTP configuration, in the Settings tab.

1. Click the **Bulk Import** button in the **Users** tab.

2. The *Bulk Import Users* dialog box will appear. Select **Domain user** in the **User type** field. If the current computer is not yet logged in to the domain, then the domain user system verification dialog will pop up after you select **Domain User**. You will need to log in as a domain user on Splashtop Center to join the host server in to the Active Directory domain.

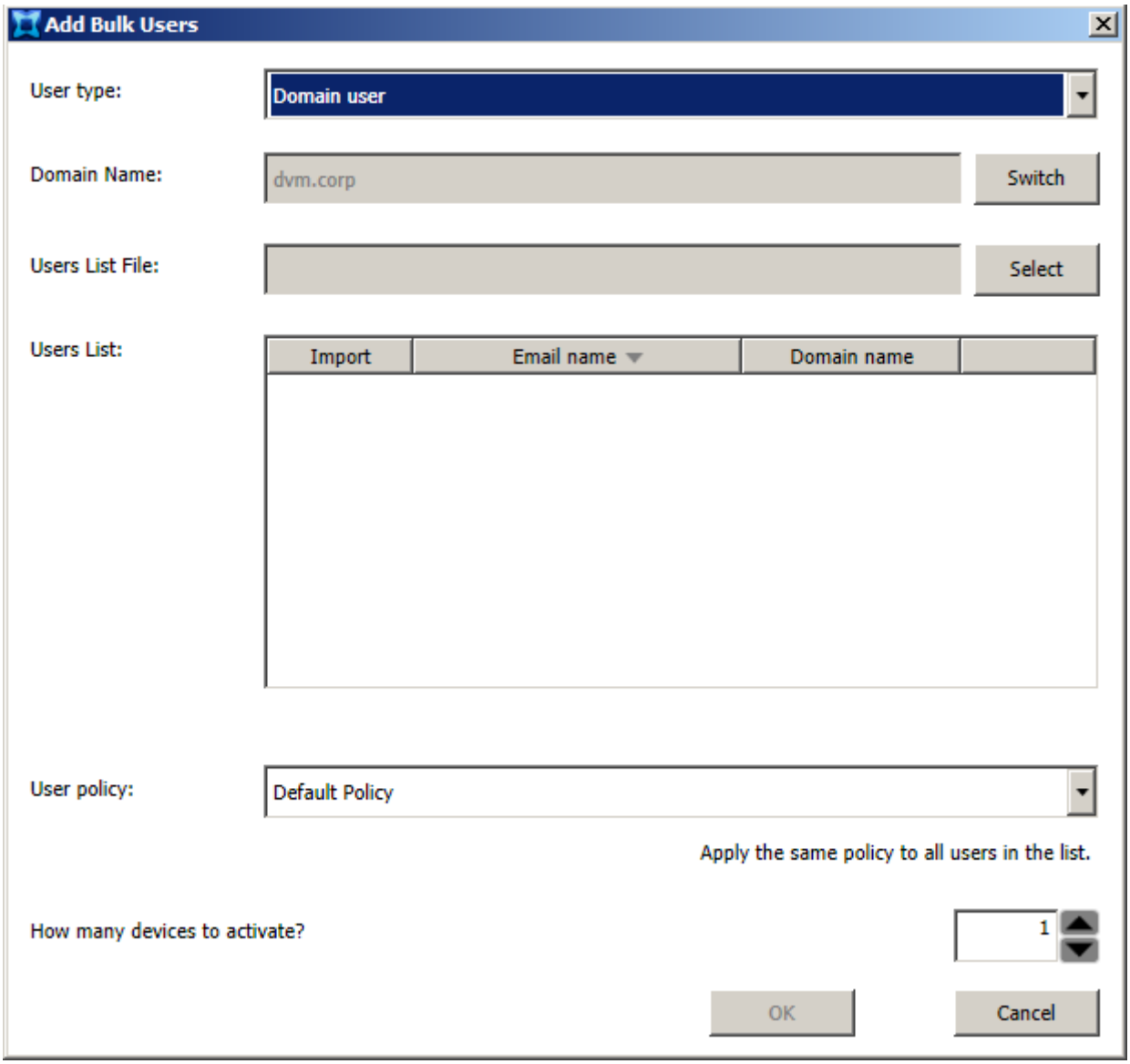
NOTE: The dialog box may take various forms depending on the Windows operating system you are using. For example, if you are using Windows 7, it might look as shown on the left below. If you are using Windows XP, it might look as shown on the right below.





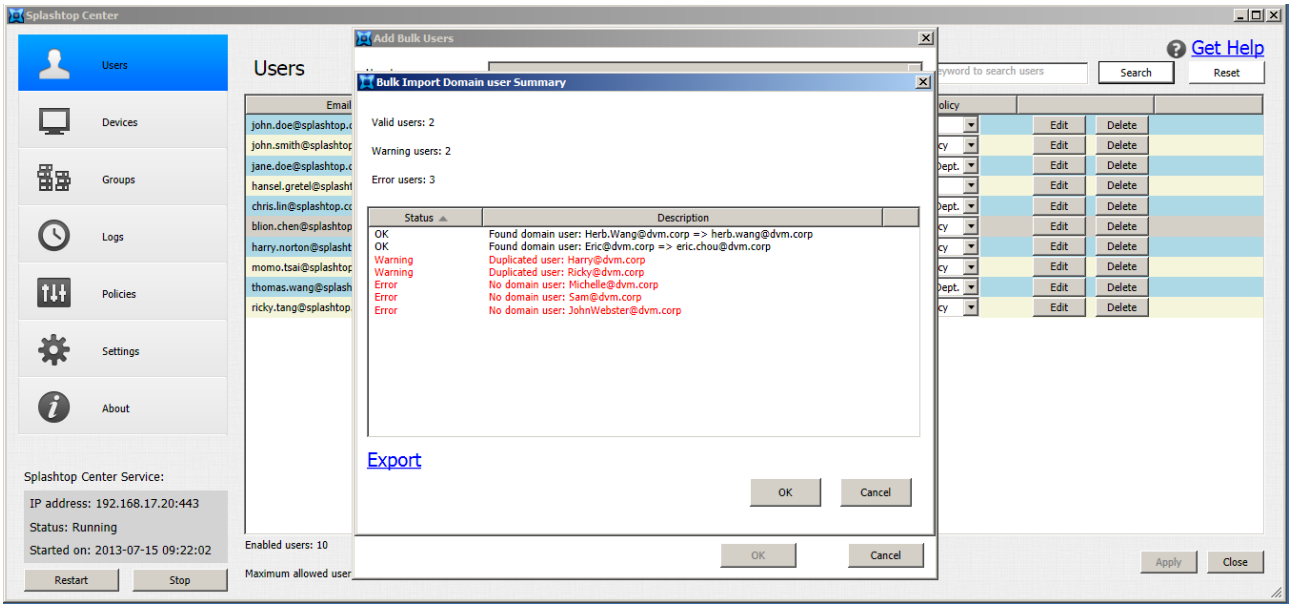
Enter the **domain_name\user_name** in the **User name** field and its related **Password** into the dialog box.

After successfully logging in as a domain user, the **User Type** field will display **Domain user**, as shown below.



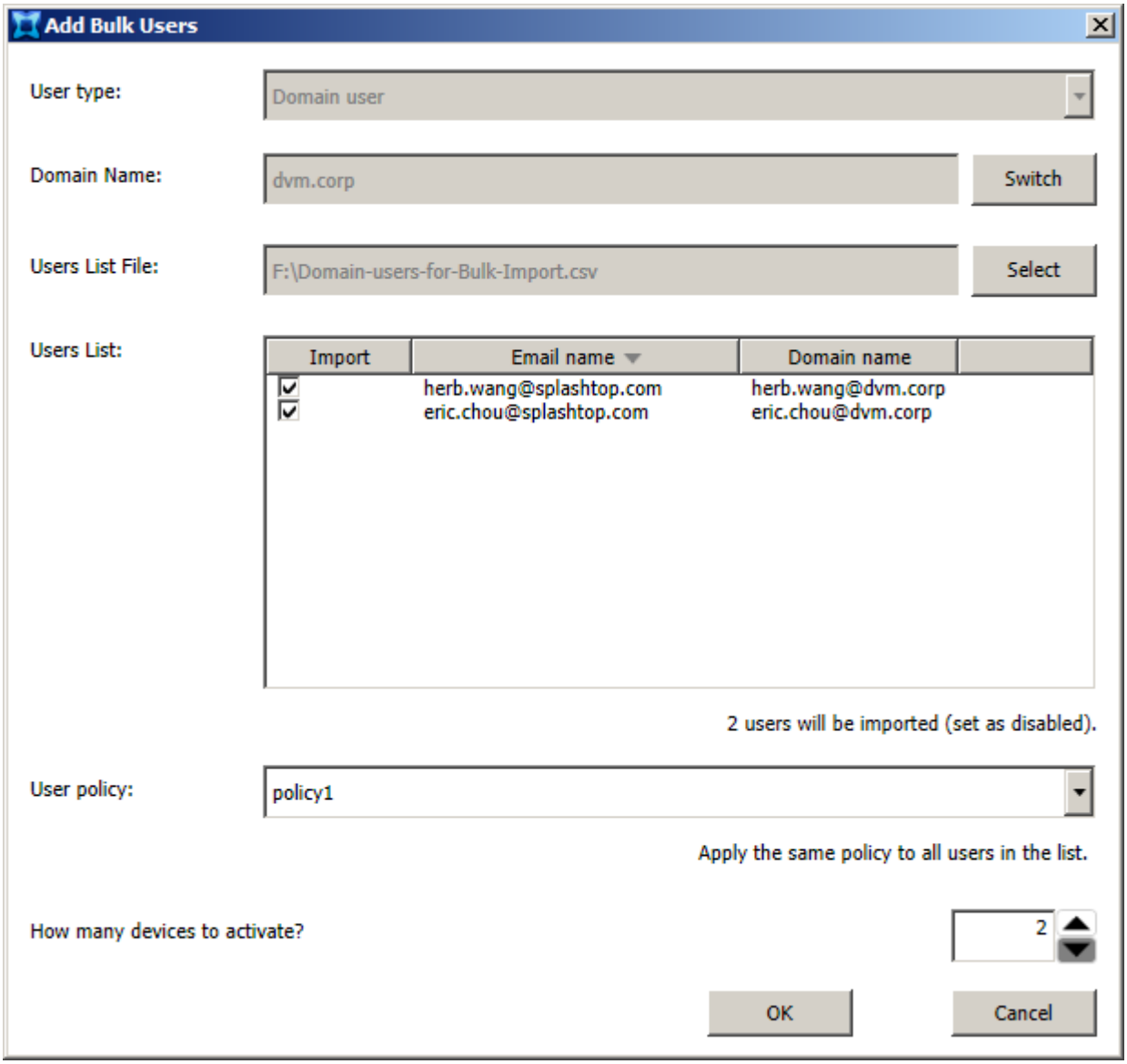
The **Domain Name** field will display the domain you logged in to. Splashtop Center supports multiple domains, so if you wish to add users from a different domain, you can click the **Switch** button. The "Domain Login" dialog box (illustrated on the previous page) will open again, and let you change to a different domain.

3. In the **Users List File** field, enter the name of the file which lists the Active Directory domain user names you want to add to Splashtop Center. You can type the name of the file, or click **Select** and browse to the desired file. After you do this, Splashtop Center will automatically analyze the AD domain names in the file and will inform you of the status of each one in the *Bulk Import Domain user Summary* dialog. For example, if a domain name is found to be identical to an already-existing name, or if it is an invalid name, you will be notified as shown in the example illustration below. A status of "OK" will be displayed for each AD domain name that is found to be valid, similar to the behavior of adding Gateway users via Bulk Import.



4. Click the **OK** button to continue.

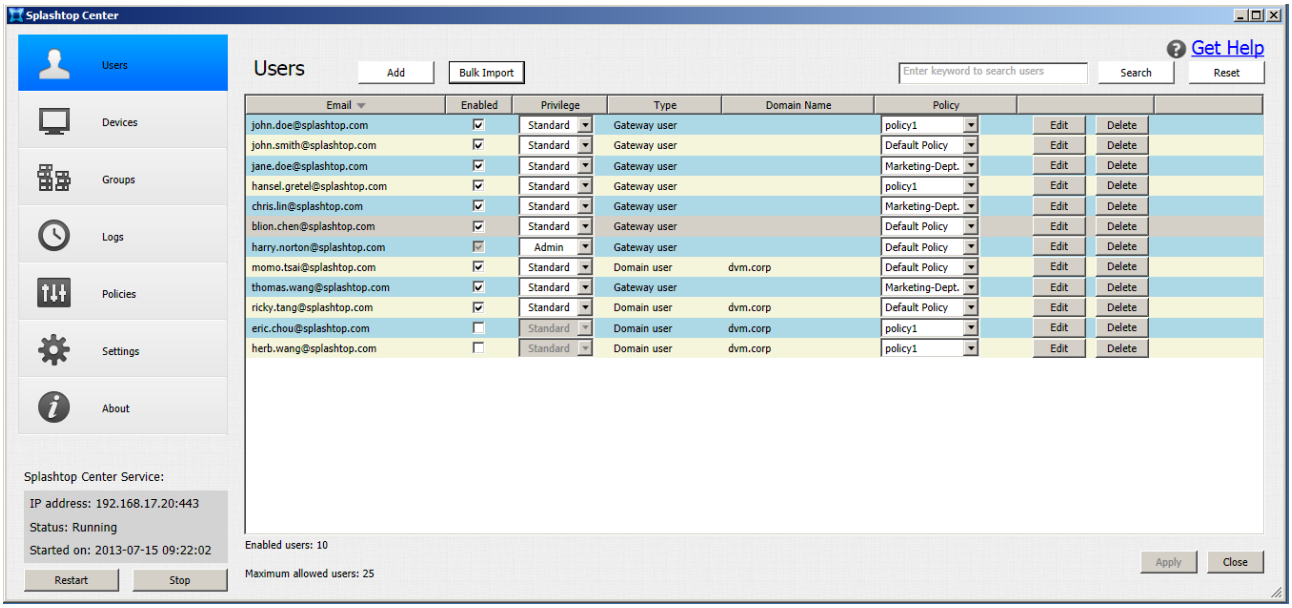
5. After you click **OK** in Step 4, you will be returned to the *Add Bulk Users* dialog. The users in the imported file who are found to be valid will automatically be listed in the **Users List** area. The Email address associated with each valid domain account will display in the **Email Name** column, and Splashtop Center will use the value shown in the **Email** field as the user account. This is shown in the example below. (According to the report shown in the illustration on the previous page, only two of the six users listed in the imported file were valid to be added to Splashtop Center.)



6. In the **User Policy** field, select the policy you want to apply to the users you will be adding. This same policy will apply to *all* users being imported from the file.

7. The number you specify in the **How many devices to activate?** field (if available) will be applied to *all* users when they are added via Bulk Import.

8. Click **OK** to add these AD domain users into Splashtop Center. The **Users** tab will show the newly-added users. Recall that users added via Bulk Import are initially in a Disabled status by default. Therefore, the two new users at the end of this list have an un-checked checkbox in the **Enabled** column.

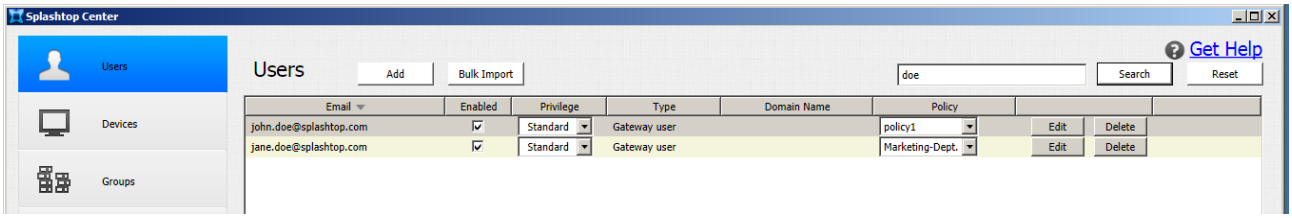


NOTES:

- If you cannot add Domain users from AD (Active Directory), see section 2.3.2.1 for further information.
- If a user is removed from Active Directory directly,that user will still be present in Splashtop Center. However, the account will be disabled, because the credential check will fail when querying against AD.

4.2. Searching Users

In the **Search** field near the upper right of the **Users** tab, enter the characters you want to search for. When you click the **Search** button, Email addresses of all users in Splashtop Center are searched for that string. The matches, if any, will be listed in the **Users** tab. In the example below, we searched for "doe" and two matches were found.



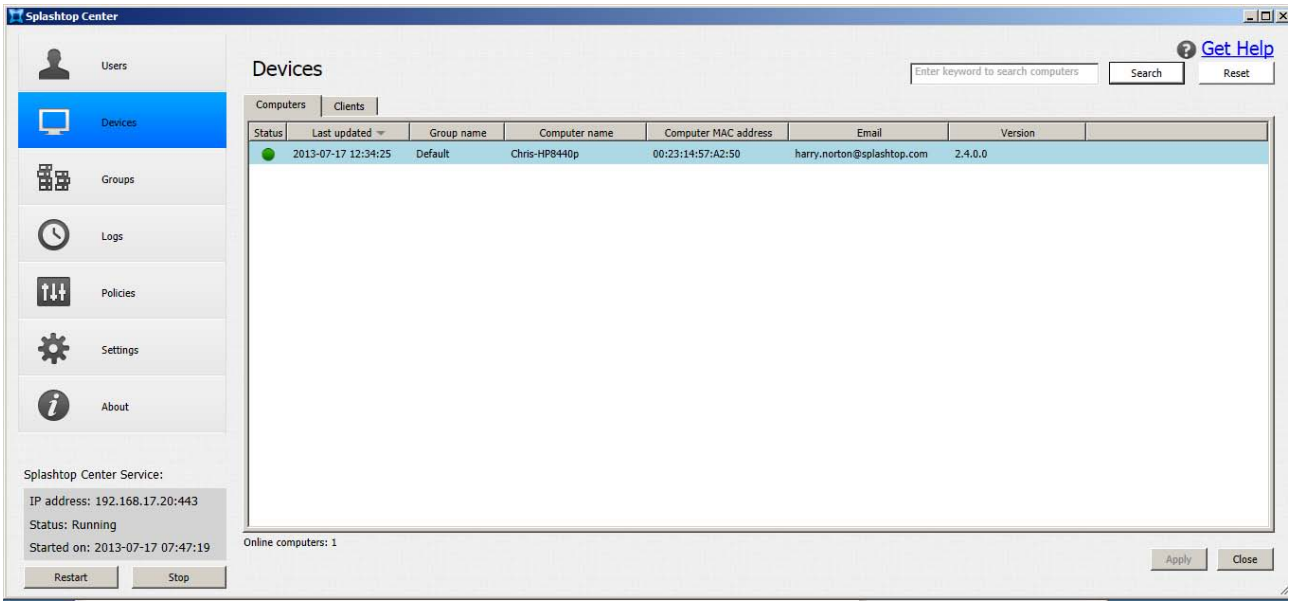
Clicking the **Reset** button will blank the **Search** field and will return the **Users** tab to the normal display which lists all users.

4.3. The Devices Tab

Clicking **Devices** in the Splashtop Center screen allows you to access the following two tabs:

4.3.1. Computers

The **Computers** tab displays current computers (Streamers) Status, the Last Updated time, the Group Name, the Computer Name, the Computer MAC Address, the User ID/Email, and the Streamer Version. A **blue** dot in the **Status** column indicates that this computer's Streamer is ready and available for connection. A green dot (as shown below) means the computer is currently connected in a remote session. Accordingly, the message "**Online computers: 1**" displays near the bottom of the **Devices** tab in this example.



The columns are further explained on the next page.

Status

A blue dot in the **Status** column of the Devices/Computers tab indicates that this computer's Streamer is ready and available for connection.

A green dot indicates that this computer's Streamer is currently in an active "connected session."

A gray dot indicates that this computer's Streamer is offline either due to Streamer logoff, or the system is in a Sleep or Powered Off state.

Last updated

It shows the time stamp of when the Streamer information was last updated. If the Streamer is online, the information will be updated automatically every 5 minutes.

Group Name

Each computer will be assigned to a group. The Group Name column shows the specific group the computer belongs to. Each computer will only be assigned to one group.

Computer Name

Typically, this is the same as the computer name defined for the host machine. But, this can also be a different name, and can be modified in the Streamer console for Splashtop display purposes (in the Computer Name field of the Status tab in the Streamer console).

Computer MAC Address

This column will provide MAC address information of the host machine. Please note that a host machine may have multiple NIC devices; in that case multiple MAC addresses will be shown.

Email

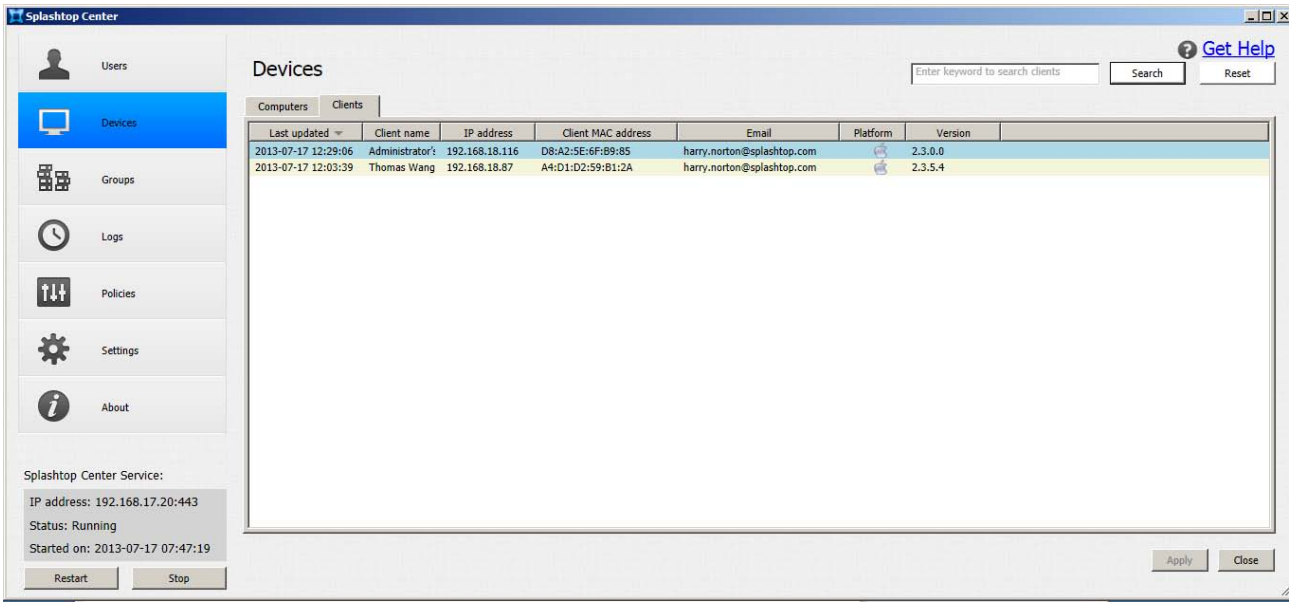
This column indicates the user who is currently login to the Computer's Streamer.

Version

This column displays the Streamer version information.

4.3.2. Clients

The **Clients** tab displays the current mobile client device's Last Updated time, Client Name, IP Address, Client MAC Address, User ID (Email), Platform, and Version of the Splashtop Enterprise app installed on that mobile device. These columns are explained below.



Last Updated

The **Last Updated** column in the Devices/Clients tab shows the time stamp of when the client information was last updated. If a client is running and logged in, the information will be updated automatically every five minutes.

Client Name

This is the same name defined for the client device. Changing the client name may require going through the system settings of the respective client OS.

IP address

This column shows the IP address that was used to log in to Splashtop Center.

Client MAC Address

This column provides MAC address information of the client device. Please note that a client device may have multiple NIC devices; in that case multiple MAC addresses will be shown.

Email

This column indicates the user who is currently logged in to the Computer's Streamer.

Platform

This column indicates the OS platform for the related client device. The OS platform can be one of the following :

- **iOS**
- **Mac** (shares the same *Apple* icon as **iOS**)
- **Windows**
- **Android**

Version

This provides the Streamer version information.

Deactivate

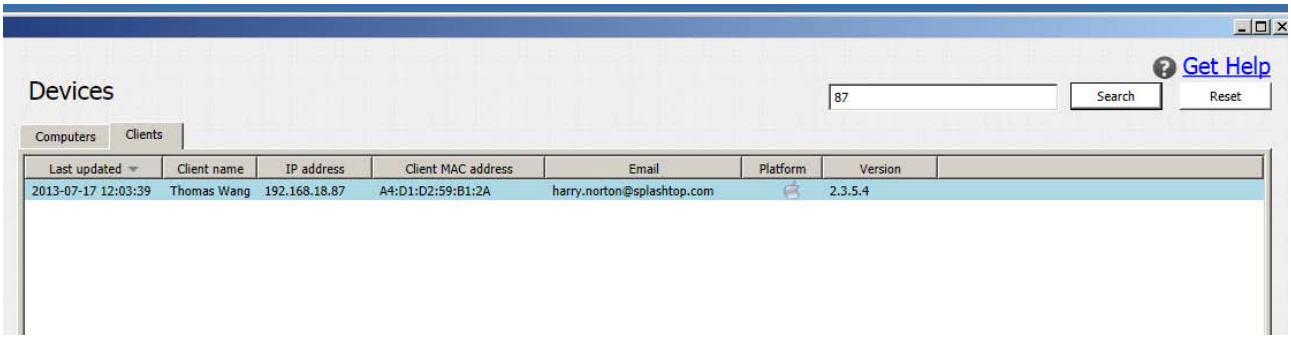
There is a **Deactivate** button to the right of each item. If a device has already been activated for use, but for any reason you want to deactivate it, click **Deactivate** to immediately block the related device for use with Splashtop Enterprise. (A warning message will pop up and require you to confirm the deactivation.) You can deactivate permanently (such as due to an employee being terminated), or temporarily (such as when a device is lost/stolen and then recovered.

4.4. Searching Computers or Clients

In the **Search** field near the upper right of the **Devices** tab, enter the characters you want to search for.

Whether you are in the **Computers** sub-tab or the **Clients** sub-tab of **Devices** when you click the **Search** button, Splashtop Center searches the data for that character or string of characters. The items that contain matches to the Search criteria will be listed.

In the example below, we searched for "87" in the **Clients** tab, and one match was listed. The string "87" was found to exist in the IP Address:

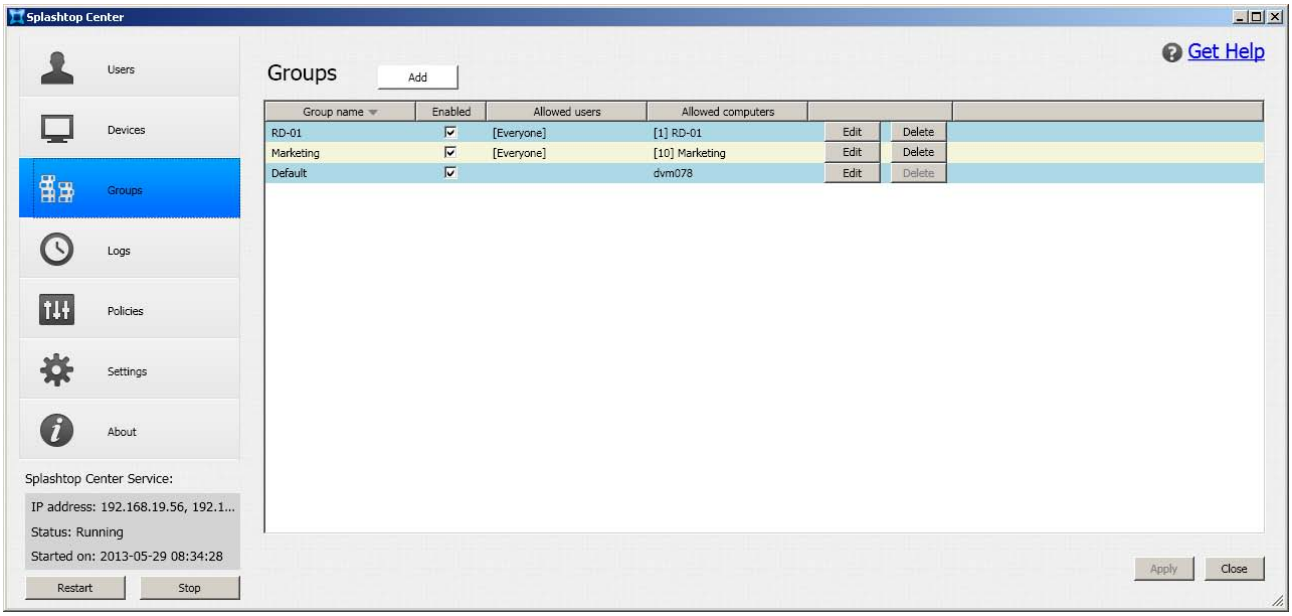


Clicking the **Reset** button will blank the **Search** field, and will return the Computers tab or Clients tab to the normal display which lists all items.

4.5. The Groups Tab

The **Groups** tab lets you create groups, and displays a list of existing group names; the users who have been added to those groups; and the computers they are allowed to use (if the **Enabled** checkbox is checked).

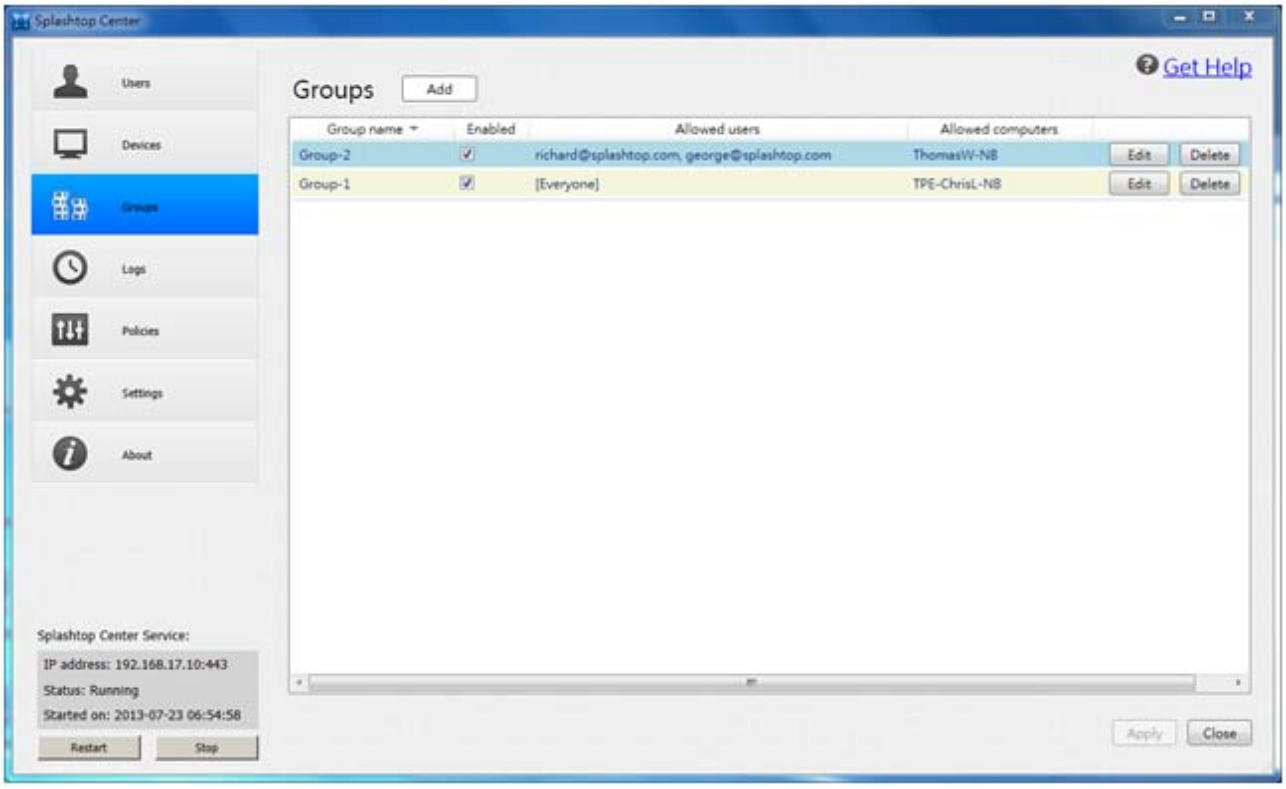
A group named "**Default**" is created for you during the Splashtop Center installation (shown in the illustration below). If you have not yet created any other groups, then the new users you add will automatically be added to that group by default. You can create as many groups as you want, for different purposes. This is one of the many advantages of Splashtop Center.



The first two items shown in the example above were added when using our optional **RDS** (Remote Desktop Services) feature. Please see Chapter 5 and Section 6.8 for details about RDP Connector.

The purpose of using groups is to facilitate shared access. Grouping gives the IT Administrator the ability to manage and grant access permissions of the groups to a selection of users.

Group Streamer allocation to users is provided randomly by Splashtop Center. If you add several computers to a group, then when multiple users attempt to connect remotely with their mobile devices, the connection will automatically be made randomly to a computer in the group which is not currently being remote-accessed. So if you have five users in the field, and five office computers (Streamers) in the group, then each person will be able to successfully connect to a computer in the office with his/her mobile device, even if they all want to connect at the same time.

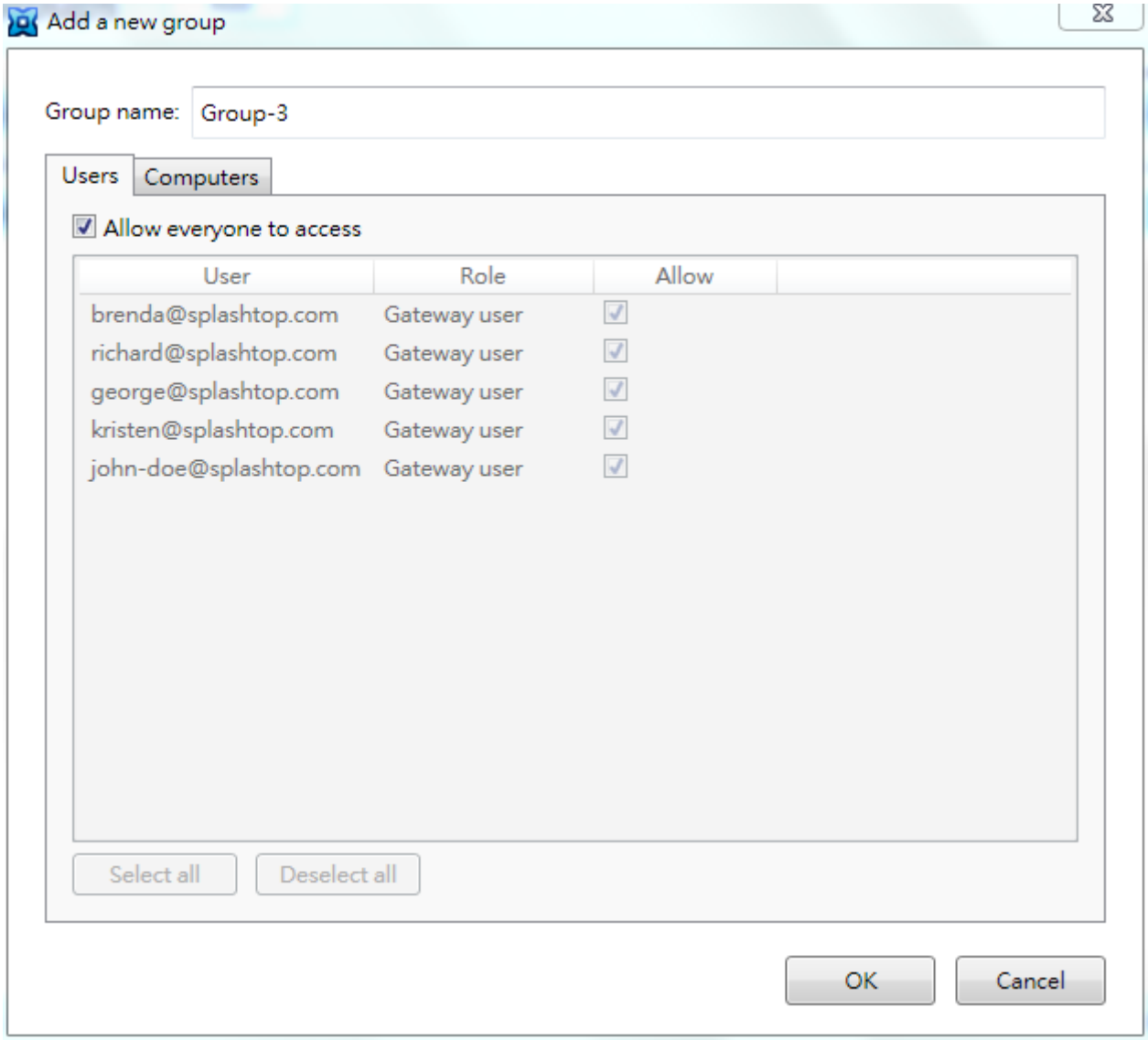


Please note that Users cannot use their mobile devices to "connect to Splashtop Center." Splashtop Center is not a Streamer. It is focused to be the gateway and relay of the mobile device clients and Streamers. However, if an IT Administrator needs to connect to the server, he or she can install a Streamer on that server, and log in to the Splashtop Center.

4.5.1. Adding Groups

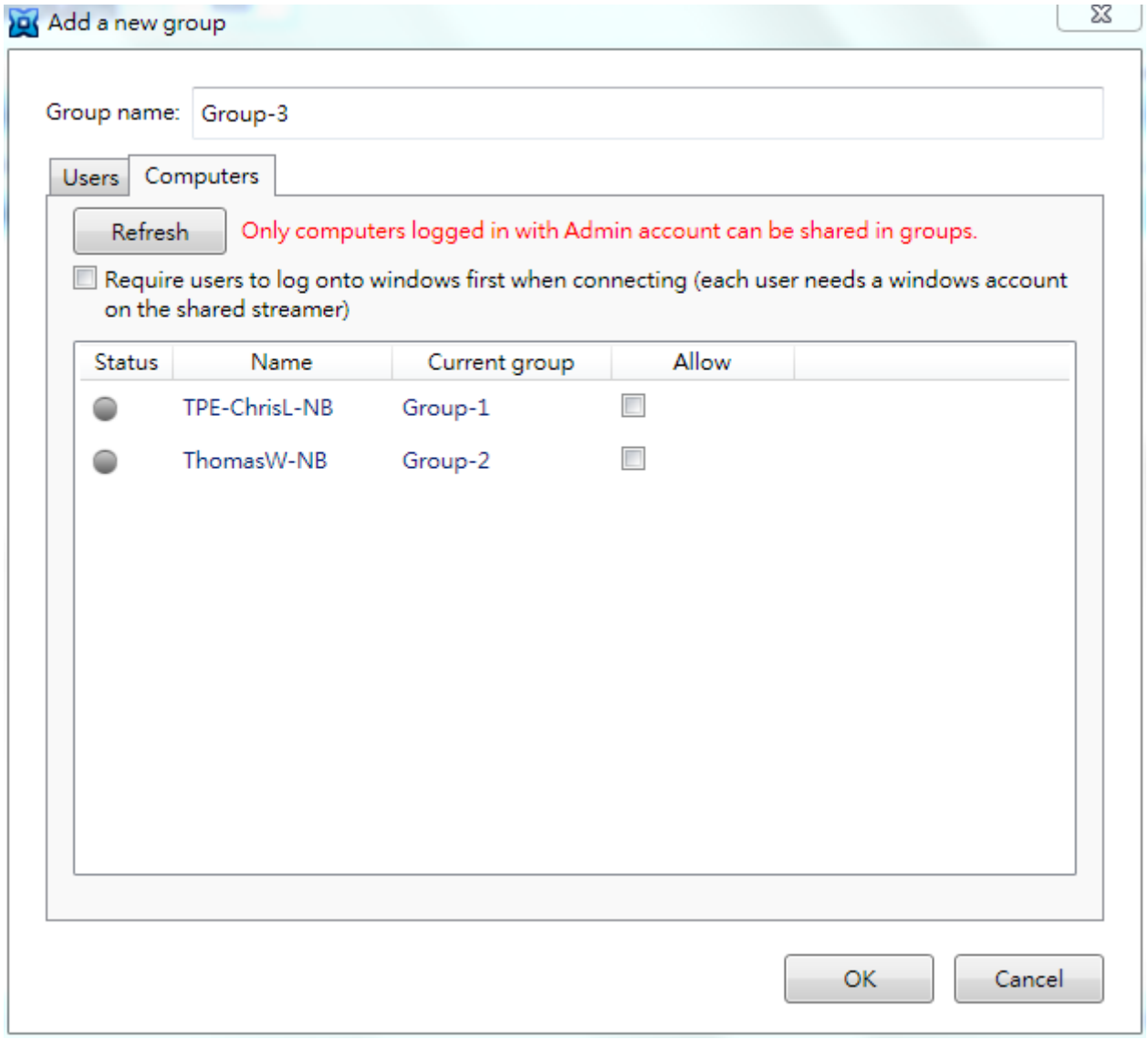
1. Click the **Add** button of the **Groups** tab. The *Add a New Group* dialog box will open as shown below.
2. In the **Users** tab, enter a name for the new group, and select the users that you want to have access to it, by checking the corresponding checkboxes.

   NOTE: The **Allow everyone to access** option allows *all* users in the list to access the computers available in this group.



Next, click **Computers** to open the tab shown below. In this tab, you will need to select the computer(s) that you want to be part of this group by selecting the appropriate **Allow** checkbox(es). The selected computer(s) will be available to allowed members of the group for remote access.

NOTE: As indicated in the red message in the dialog box shown below, in order for a computer to be available to be shared by a group, its Streamer needs to be logged in to by the IT Administrator (Admin account).



Please note that it is not necessary to have one Streamer available for each user. For example, you might have five users in the field authorized to use Splashtop Center, but only two desktop computers in the office with the Streamer installed (to enable remote access). However, be aware that only one computer can be accessed remotely at a time. Therefore, if both of those available computers are currently being accessed remotely by two of the five users, then the other three users will have to wait until one of the two Streamer computers becomes available — "first come, first served."

Click the **Edit** button if you want to allow more (or disallow) computers and/or users.

For more details:

To see a step-by-step example of adding a new group with more details, please refer to **section 6.5** entitled **Creating and Administrating Groups**.

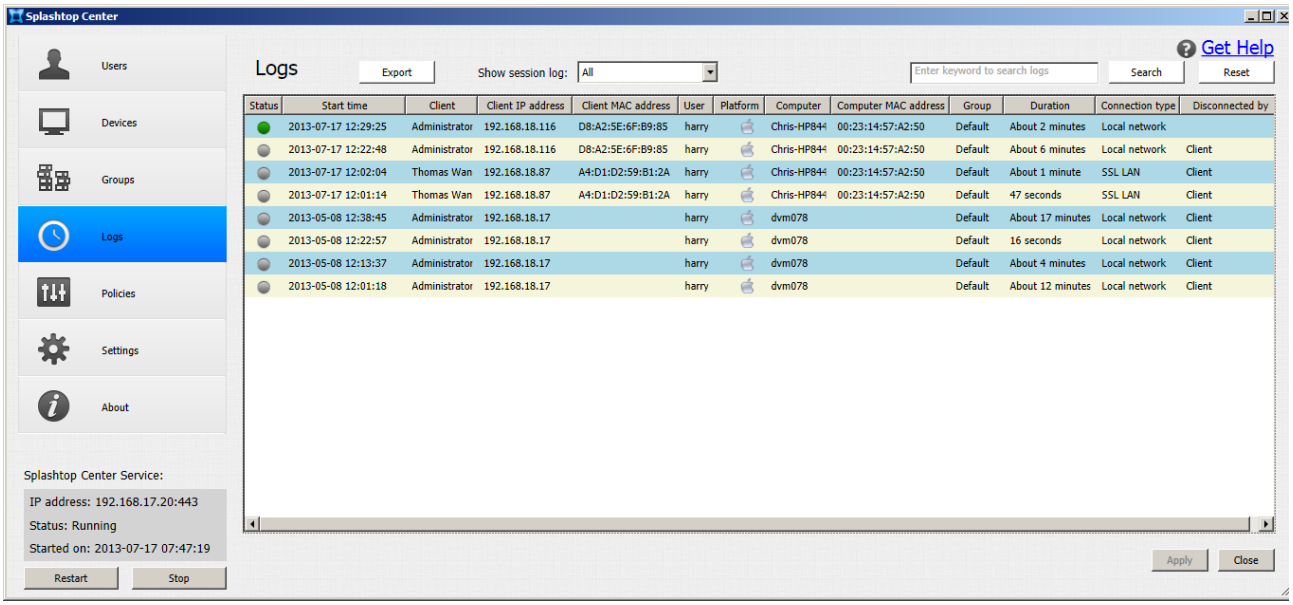
4.6. The Logs Tab

The **Logs** tab displays online and offline sessions and shows the Start time, Client name, Client IP address, User account, Client MAC address, Computer MAC address, Client Platform, Computer (Streamer) name, Group this computer belongs to, Duration of the session, Connection Type of the session, and which side initiated the Disconnection. These are explained on the next page.

In the **Status** column at the leftmost side:

- A **green** dot indicates the current online sessions (Streamer occupied/currently connected to by other clients). This is shown in the first item below in the sample illustration.
- A **gray** dot indicates past/disconnected sessions.

Logs are recorded from the very first day of running Splashtop Center, so dates can be tracked back to "day one." Log files are archived on a per-day basis, and can be manually exported or backed up. There are no size limits for log files.

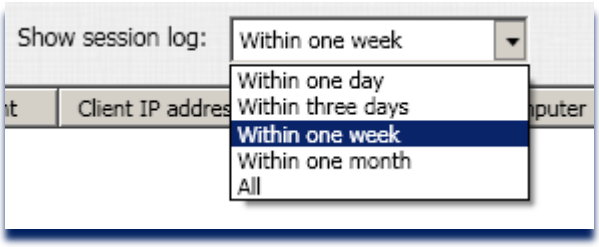


Search field

In the **Search** field near the upper right of the **Logs** tab, enter the characters you want to search for. When you click the **Search** button, each log entry in Splashtop Center is searched for that string. The matches, if any, will be listed in the **Logs** tab. Clicking the **Reset** button will blank the **Search** field and will return the **Logs** tab to the normal display which lists all log entries (according to the current filter setting in **Show Session Log**, explained below.)

Show Session Log

In the **Show Session Log** field near the top center of the **Logs** tab, you can specify which logs to display, according to various periods of time. By default, the log entries for the past seven days will be listed, starting with the most recent. If desired, you can instead select other display options from the drop-down list: **Within one day**, **Within three days**, **Within one week**, **Within one month**, or **All** (regardless of timestamp).



Export

This handy feature lets you save log files. If you click the **Export** button, a dialog box will open in which you can select a folder where you would like Splashtop Center to export all session log files, in CSV format.

⚠ CAUTION: Please be aware that un-installing Splashtop Center from the host OS will remove all log data.

Status

As mentioned earlier, a green dot in the **Status** column of the **Logs** tab indicates that a remote connection is actively in session. A gray dot indicates that this remote session is already over and disconnected.

Start time

This column shows the time when the remote session was initiated.

Client

This is the same name defined for the client device. (Changing the client name may require going through system settings of the respective client OS.)

Client IP address

This shows the IP address that was used to log in to Splashtop Center.

Client MAC Address

This will provide MAC address information of the client device. Please note that a client device may have multiple NIC devices; in that case multiple MAC addresses will be shown.

User

This indicates the user who created the remote connection. This is the same as the Email column in the Devices/Computers and Devices/Client tabs.

Platform

This shows the OS platform for the related client device. The OS platform can be one of the following :

- **iOS**
- **Mac** (shares the same *Apple* icon as **iOS**)
- **Windows**
- **Android**

Computer

This is the name to identify the Streamer. In the typical case, this is the same as the computer name defined for the host machine. But, this can also be different name, and can be modified in the Streamer console's Status tab.

Group

Each computer will be assigned to a group. The **Group** column shows the name of the group which the computer belongs to. Each computer will only be assigned to one group.

Computer MAC Address

This is to provide MAC address information of the host machine. Please note that a host machine may have multiple NIC devices; in that case multiple MAC addresses will be shown.

Duration

This column displays the the total time of ths connection from start to end. For on-going sessions, the duration will continue to expand until the session is terminated.

Connection type

This shows the type of remote connection between Streamer and client. The **Connection type** can be one of the following :

- Local network (both Streamer and client in the same network segment)
- SSL LAN (local network with SSL)
- SSL Relay (Streamer and client are on different network segments, and one of them is likely behind the firewall).
- RDP connection (Connection to host machine is via RDP protocol)

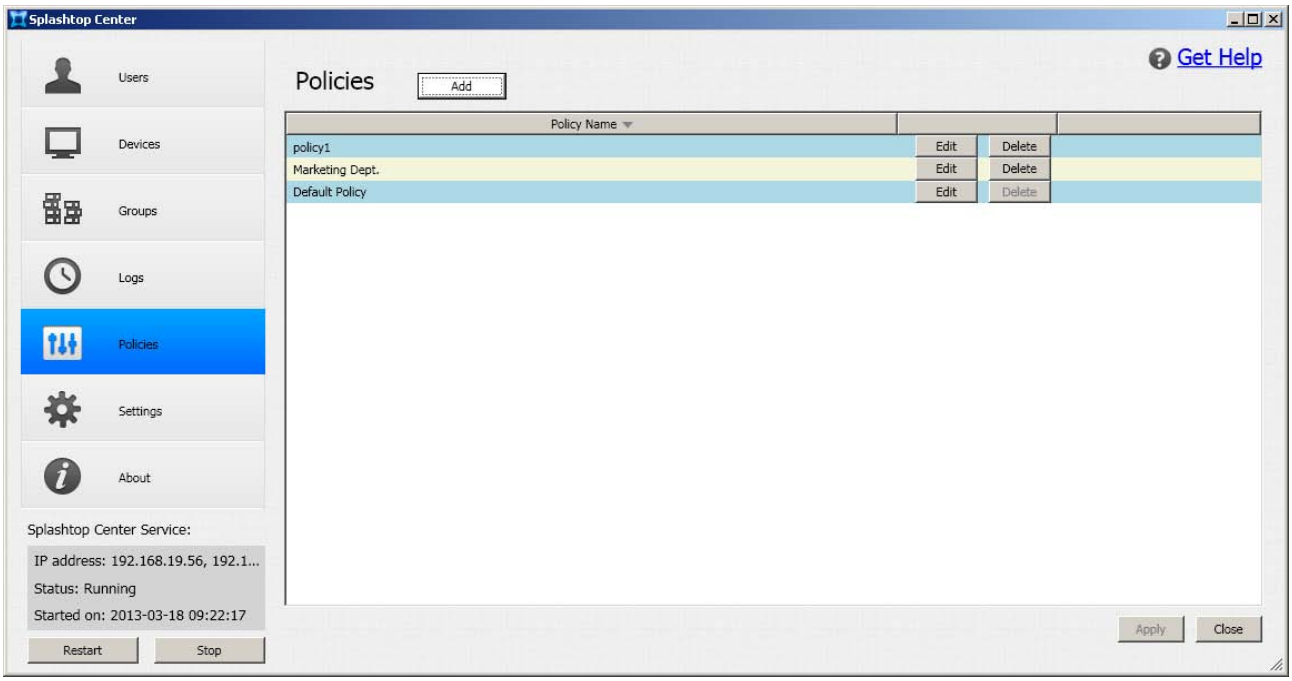
Disconnected by

This column reports what caused the remote session disconnection. Disconnection could be initiated by one of the following:

- Computer (if disconnection is triggered from the Streamer)
- Client (if disconnection is triggered from the client)
- Splashtop Center (if disconnection is triggered from Splashtop Center)
- Network issue (if disconnection is due to network quality)

4.7. 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).



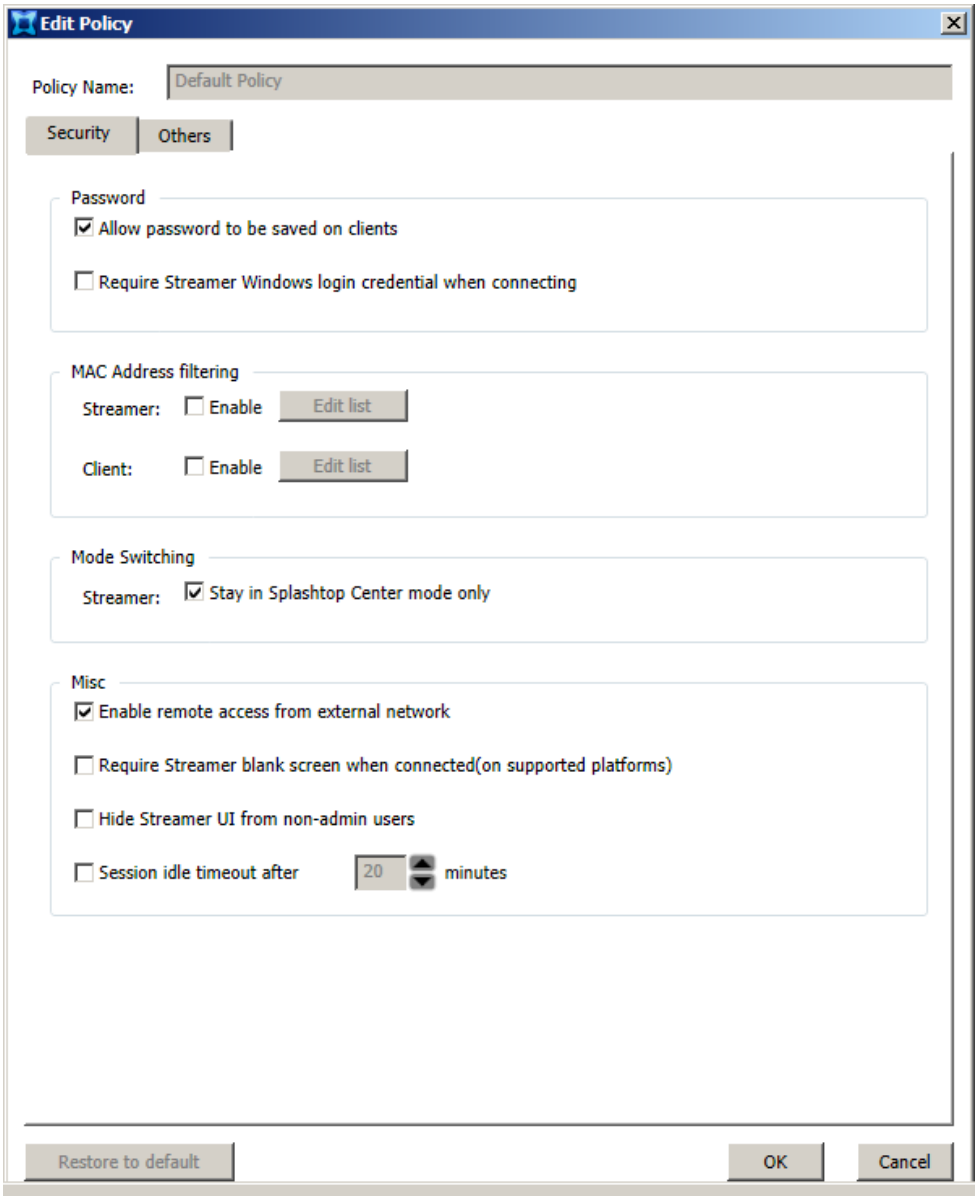
4.7.1. Default Policy

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 the Default Policy will be applied to all new users you add, by default. If you click the **Edit** button (shown above) for **Default Policy**, the dialog box shown on the next page will open. (If the policy has been assigned to any users, a message will notify you of such and require you to confirm that you want to continue.)

4.7.1.1. Security tab

Policy Name field

The name of the default policy is "**Default Policy**" and this name cannot be changed (thus, the **Policy Name** field is grayed out below). Of course, if you create new policies, you can subsequently change the name of those additional policies at any time.



NOTE: At the bottom of the **Edit Policy** dialog box for the *Default Policy*, there is a **Restore to Default** button. If the **Restore to Default** button is disabled as shown in the example above, then this indicates to you that the settings are already currently the "factory default" settings; therefore, there is nothing to reset. Conversely, if the button is enabled, then clicking it will re-set all the settings to their original values.

The **Restore to Default** button is only available when you are editing the *Default Policy*. In the **Edit Policy** dialog box for any other policies except the *Default Policy*, this button will not exist.

4.7.1.1.1. Password

Allow password to be saved on clients

The password for each user's client device is retained by Splashtop Center. If the **Allow password to be saved on clients** option is enabled, it means you are allowing all users to use their "Stay Logged In" option on their mobile devices, which in turn allows them to automatically get into their Splashtop Enterprise account without entering a password. This option is enabled by default.

Require Streamer Windows login credential when connecting

If this option is enabled, users who want to remotely connect to a Windows computer running the Streamer will need to enter their Windows Username and Password to log in to that computer first, before they can establish a connection to the Streamer.

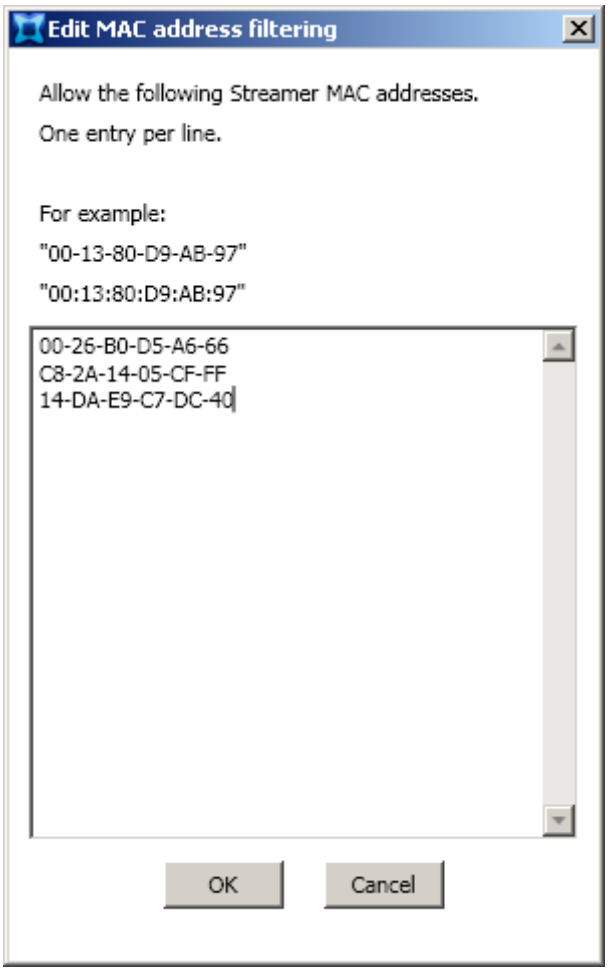
4.7.1.1.2. MAC Address filtering

The **MAC Address filtering** feature behaves as a "whitelist," allowing only the listed devices to establish a remote-login session in Splashtop Enterprise. You can now allow or disallow connection to **Streamer** MAC addresses and **Client** MAC addresses separately.

To enable connection to all of the Streamer MAC addresses currently in the list, check the **Enable** checkbox for **Streamer**. To prevent connection to all of them, un-check it. Likewise, to allow connection to all the Client MAC addresses currently in the list, make sure the **Enable** checkbox for **Client** is checked.

If a checkbox is checked, the corresponding **Edit List** button will be enabled. To add MAC addresses, click **Edit List** for either **Streamer** or **Client**, then enter the addresses you want to allow, with each one on a new line. (By default, there is nothing entered.)

In the example below, the **Edit List** window for **Streamers** is illustrated, with three sample MAC addresses entered. If the MAC address of a Streamer or Client is not listed, it will be blocked when trying to log in (if the **Streamer** checkbox is checked, as shown later in "Adding a New Policy."

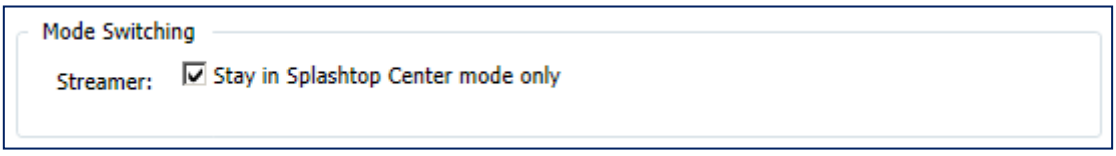


The IT Administrator can then choose which ones should be allowed to use Splashtop Enterprise, and export a list of MAC addresses. When the Client/Streamer has multiple NIC, all of the MAC addresses are uploaded to Splashtop Center. As long as just one of the Client/Streamer MAC addresses is listed in the "Whitelist," it is regarded as accepted. On the other hand, if none of them is listed, it will fail to log in to Splashtop Enterprise, and a message will notify the user of such.

4.7.1.1.3. Mode Switching

Background information: Unless restricted, our universal Streamer can be toggled for use with either Splashtop Personal/Business, or Splashtop Enterprise. The option that allows this "mode switching" is located in the lower right corner of the **Status** tab of the Streamer console. For example, if your Streamer's **Status** tab is currently ready for login to Splashtop Enterprise, then in the lower right corner you will see "Log in to Splashtop Personal or Business" as shown below.

New option in Policies to restrict mode-switching: If the **Stay in Splashtop Center mode only** checkbox is checked (as shown below) in the *Edit Policy* or *Add Policy* window, then the user(s) to whom this policy is applied will be prevented from switching the Streamer to the Login screen for Splashtop Personal or Splashtop Business. The Streamer **Status** tab will always stay in the Login mode shown above, for logging in to Splashtop Center. This option is selected (checked) by default.



4.7.1.1.4. Misc

The following options are available in the **Misc** section of the *New Policy* and *Edit Policy* dialog box.

Enable remote access from external network

If you want this user to be able to use a mobile device to remote-access computers on Splashtop Center from *any* network, make sure the **Enable remote access from external network** checkbox is checked. This will enable access from an external network. If you want to limit the user to only be able to access the computers that are on the *same* network with the mobile device client, un-check this checkbox. Please note that this option is enabled (checked) by default.

Require Streamer blank screen when connected (or supported platforms)

If this option is enabled, the screen of the computer running this Streamer will be blank when the user is remote-accessing it, to prevent others from seeing what he/she is doing. It will also lock this computer upon disconnecting from the remote session.

Hide Streamer UI from non-admin users

If this option is enabled, the computer running the Streamer will still display the "Streamer tray icon" to let the user know that the Streamer is running, but the user will not be able to open the Streamer dialog box. It will be hidden. Therefore, he/she will not be able to make any changes to the settings of the Streamer, or terminate it. However, anyone logged in with the Administrator credentials will be able to open the Streamer, close it, modify the settings, etc.

Session idle timeout

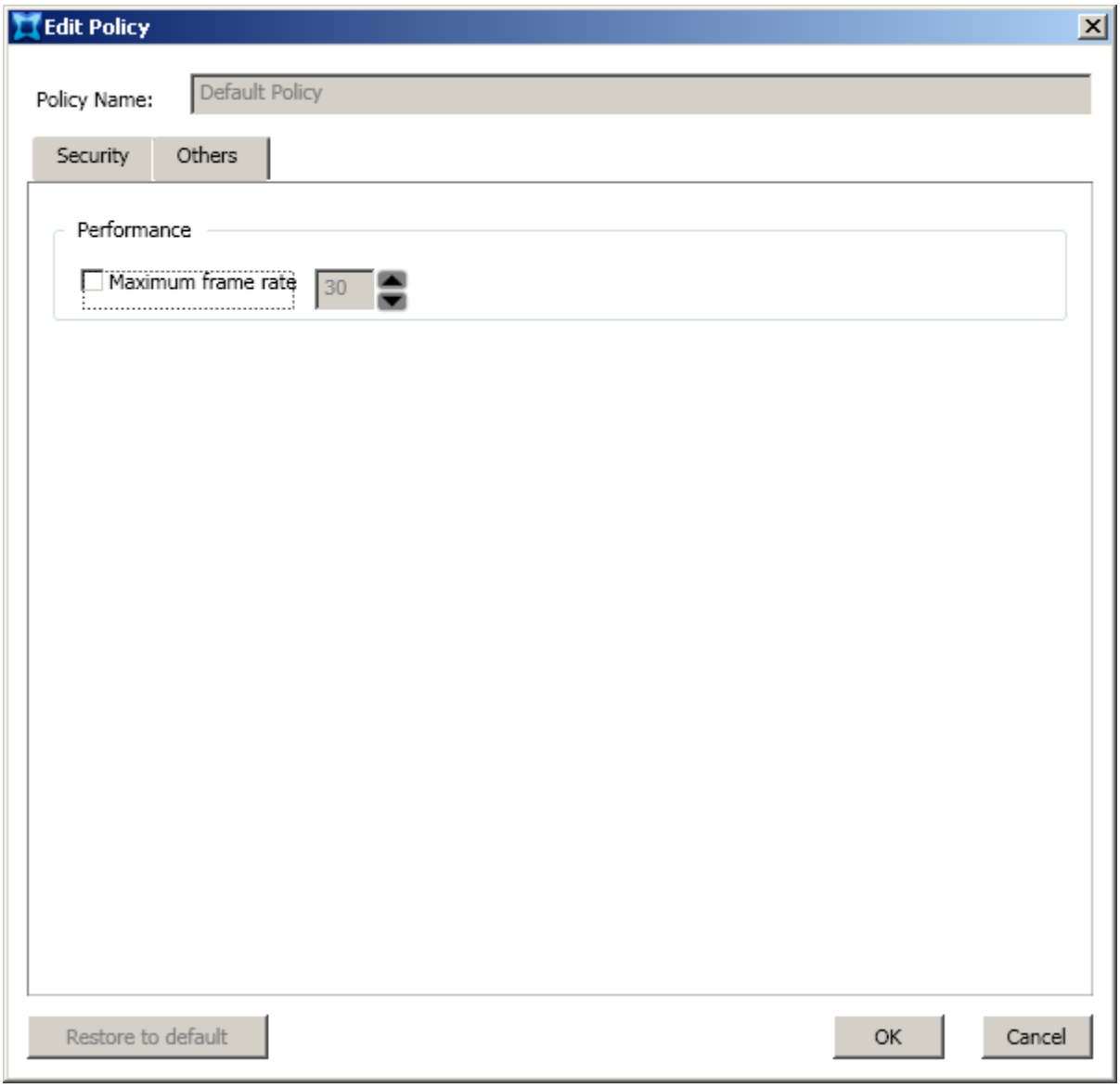
This option is disabled by default. If enabled, "idle time" will start to be counted from the time of last touch, during the connected session. After any touch event has occured, the idle time will be reset to zero and start counting again. By default, this value is set to 20 minutes, so after 20 minutes of no activity, the connection would be terminated, allowing more efficient resource usage. When there are 10 seconds left on the counter (before idle session timeout), a message will alert the user that he or she will need to respond within 10 seconds in order to keep the connection alive.

4.7.1.2. Others tab

Currently, there is only one option available in the **Others** tab of the Edit Policy or Add Policy dialog box. This option can help improve performance.

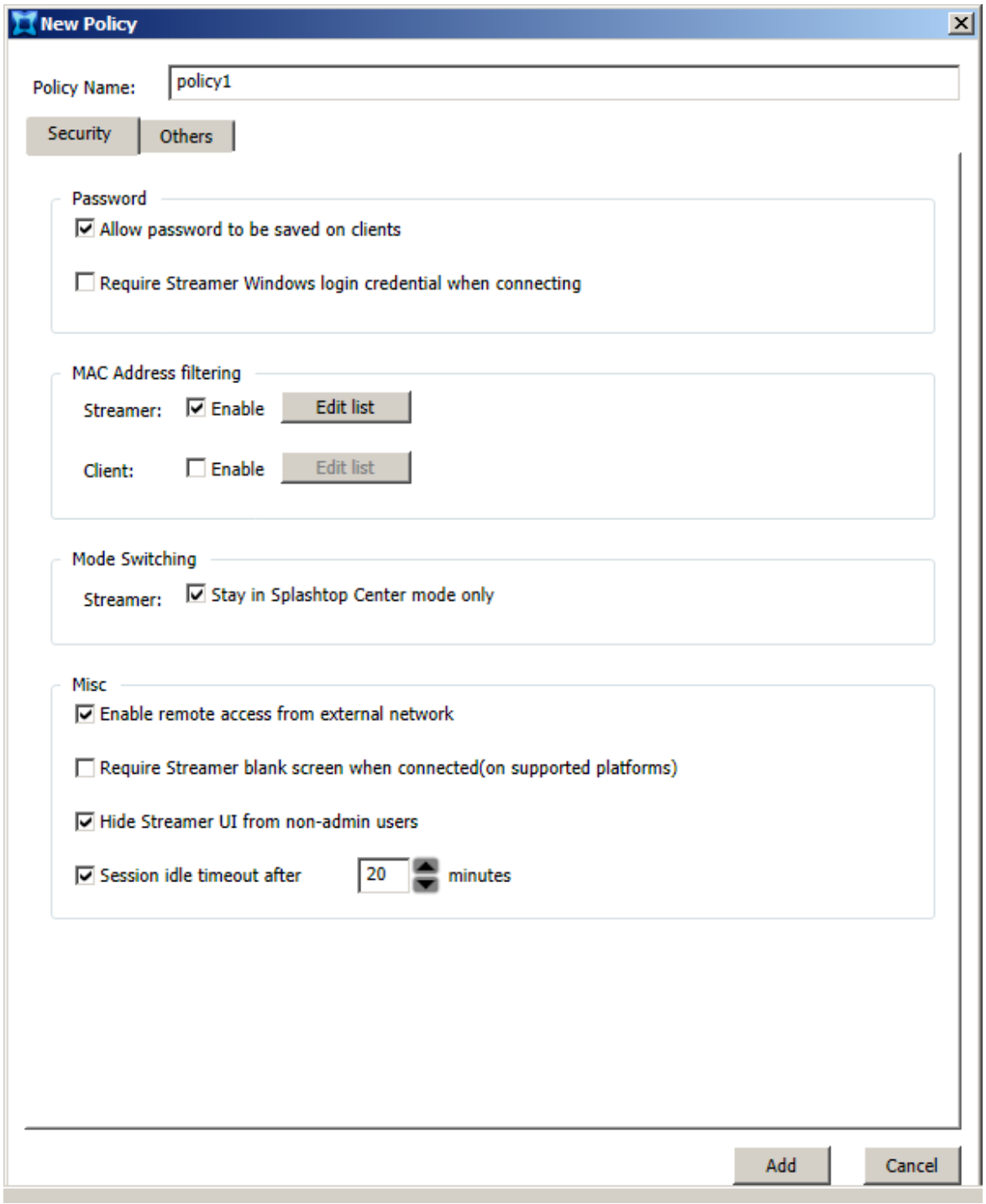
Maximum frame rate

This is disabled by default. If you check (enable) this checkbox, you can manually set the frames-per-second rate. This can help balance your network traffic. By default the value is set to **30** frames per second.



4.7.2. Adding a new policy

To create a new policy, click the **Add** button near the top of the **Policies** tab. The **New Policy** dialog box will open, with the **Security** tab displayed. By default, the Policy Name of your first newly-created policy will be **policy1**, but you can change this to a more descriptive name if desired, such as "Marketing Department," "Managers," etc.

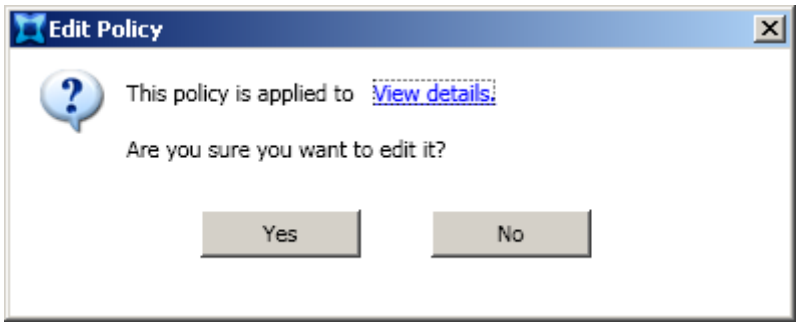


NOTE: For security concerns, you might want to consider disabling **Allow password to be saved on client**, meaning that the users to whom this policy is applied will not be allowed to enable the "Stay Logged In" option on their mobile devices. In this case, users would need to enter their password every time, to log in to Splashtop Enterprise.

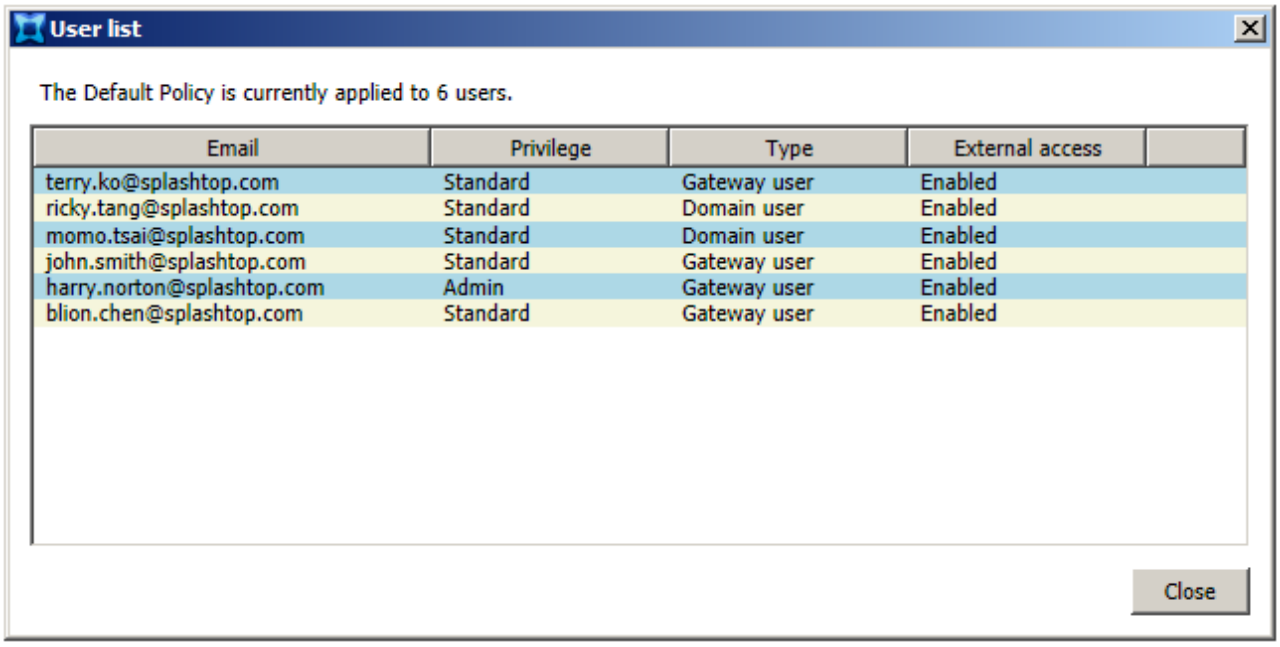
After you have configured all options in the **Security** tab and **Others** tab, make sure you have entered the name you want to use for this new policy in the **Policy Name** field, then click the **Add** button.

4.7.3. Editing an existing policy

To edit an existing policy, click the **Edit** button to the right of the corresponding policy name in the **Policies** tab. If the selected policy has been assigned to any users, a message will appear and require you to confirm that you still want to modify this policy. The message box will contain a "View Details" link or button, as shown in the example below.



Clicking **View Details** will display a list of the users to whom this policy is currently applied. An example is shown on the next page. In this example, the *User List* dialog box shows six users to whom the policy is currently applied.



4.7.4. Deleting a policy

To delete an existing policy, click the **Delete** button to the right of the desired policy name. If the selected policy has been assigned to any users, a message will appear and require you to confirm the deletion. In addition, the message box will tell you how many users this policy has been assigned to, and will contain a "View Details" button or link. Clicking **View Details** will display a list showing the users to whom this policy is currently applied (illustrated above).

NOTE: The **Default Policy** cannot be deleted.

4.8. The Settings Tab

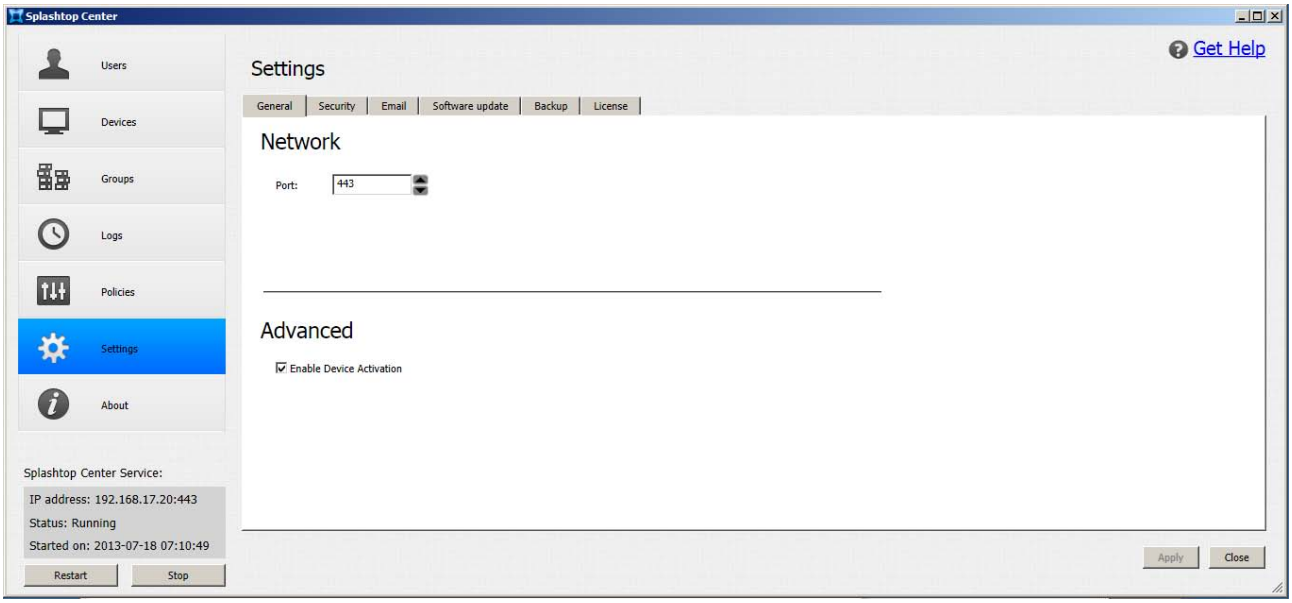
The **Settings** tab contains six sub-tabs (**General**, **Security**, **Email**, **Software update**, **Backup**, and **License**). The first time you launch Splashtop Center, the Settings/General tab (below) will display first by default.

4.8.1. General

In the **General** sub-tab, the port number in the **Port** field will be the point of entry for Splashtop Center, which performs the user/device management, as well as connecting client and Streamer, when users log in to Splashtop Center. Splashtop Center uses the TCP port only. The default gateway and relay port is **443** as shown in the illustration below.

⚠ CAUTION: Please make sure the port is not occupied by other services.

- If there is an existing public DNS name, the user can enter it on both the Streamer and the Client in the **Splashtop Center** field. For example, if the server domain name is **test.company.com**, the **Splashtop Center** field on both the Streamer and Client should be **test.splashtop.com**.
- If the user does not have a public DNS name, then he or she can input the IP Address in the **Splashtop Center** field of the Client and Streamer.

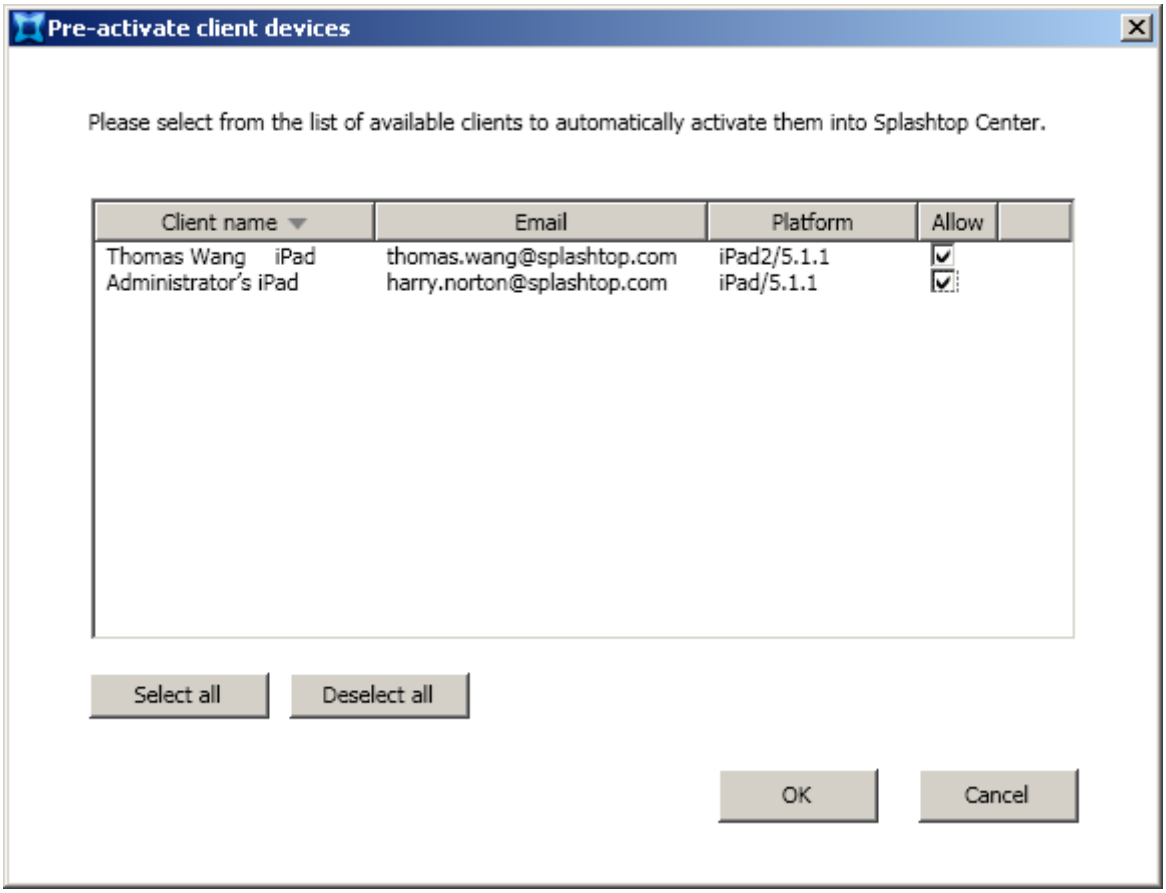


The **Enable Device Activation** option in the **General** tab of Settings is explained on the next page.

NOTE: To provide external access service, please set up port forwarding/mapping on your firewall or router. For example, if your Splashtop Center IP address is a private IP, you need to set up port forwarding on your firewall to redirect the port from the public IP to the private IP.

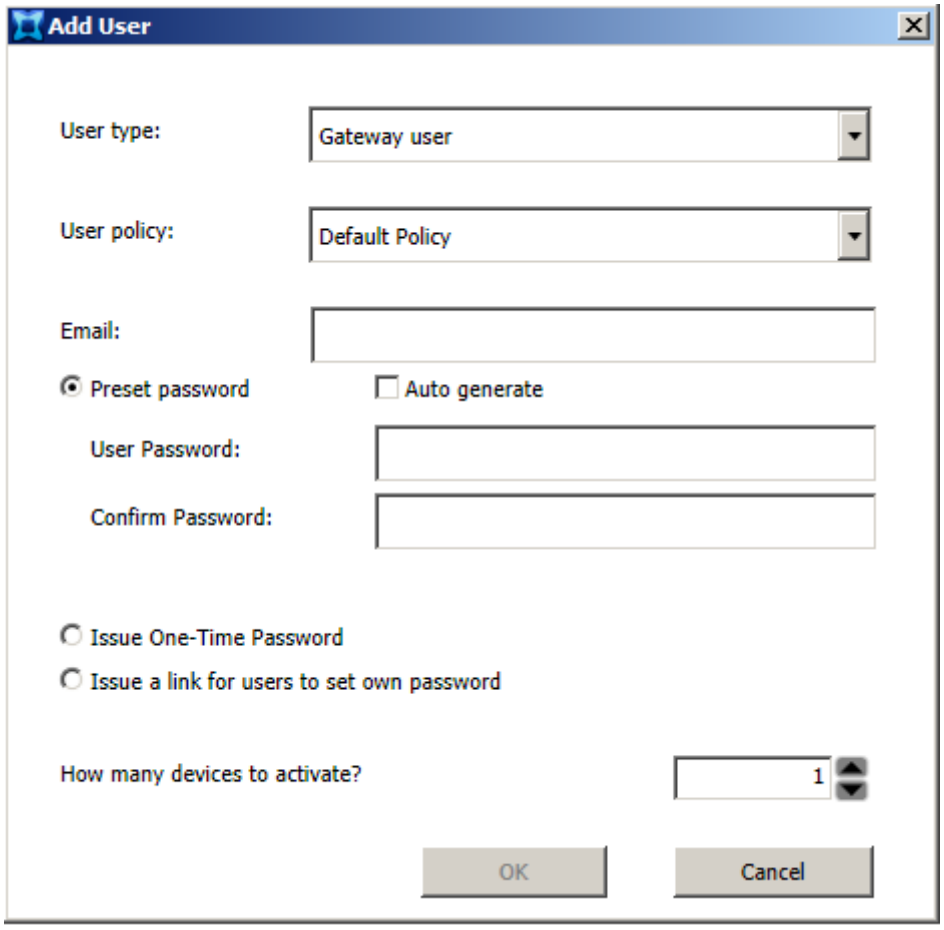
4.8.1.1. Device Activation Codes

The **Enable Device Activation** option in the **General** tab of Settings requires all client devices to be activated. Only the activated devices can connect with Splashtop Center. By default, this option is not enabled.

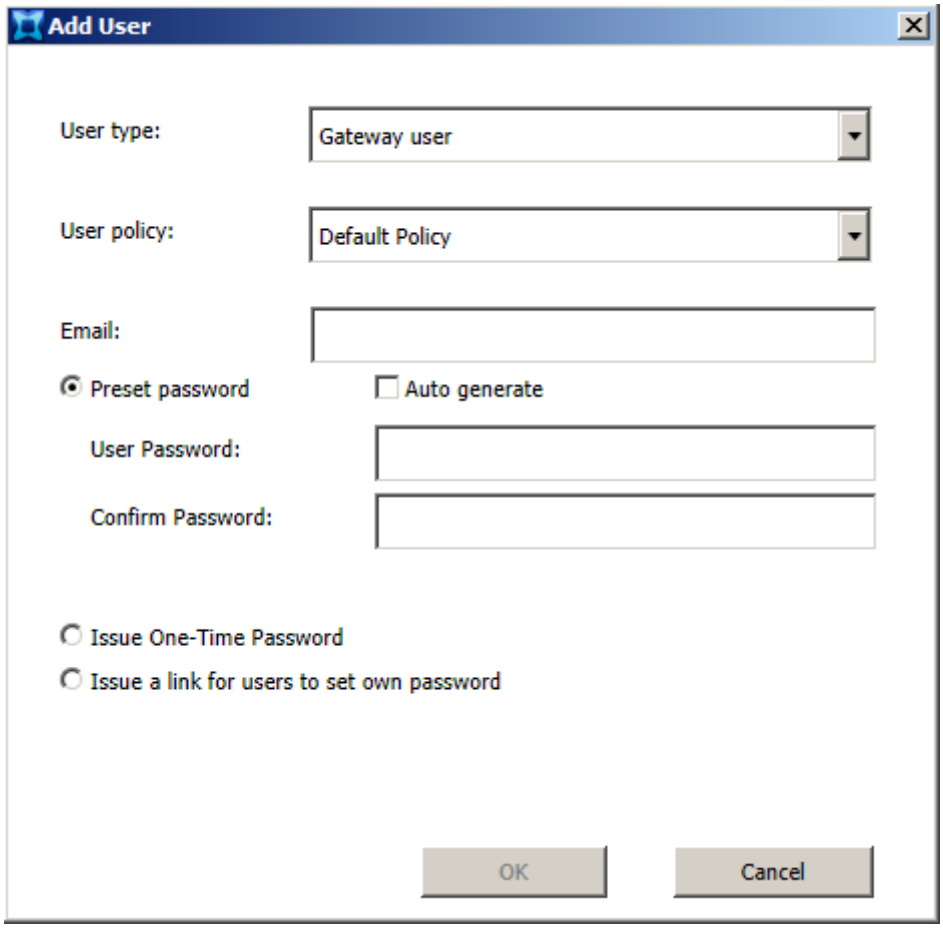


Enabling the **Enable Device Activation** option ("checking" the checkbox) will pop up the **Pre-activate client devices** dialog box shown in the example above. This dialog box allows an IT manager to qualify pre-connected devices.

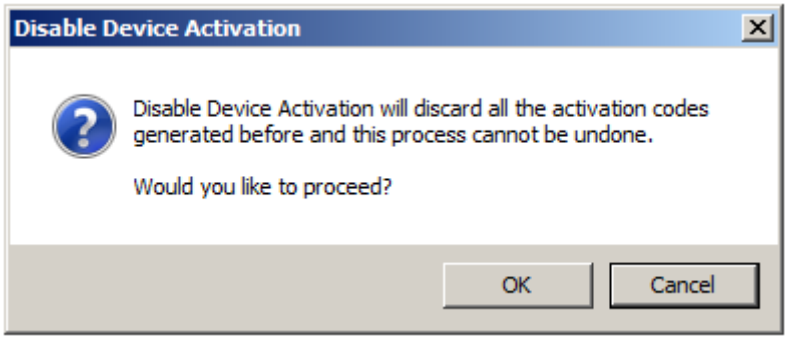
If **Enable Device Activation** is enabled (if you check the checkbox in the **General** tab of Settings) then when adding a new user, you *will* have the **How many devices to activate?** option available at the bottom of the *Add User* dialog box, as shown below. The Activation Code(s) will be given to the user in the Invitation Email.



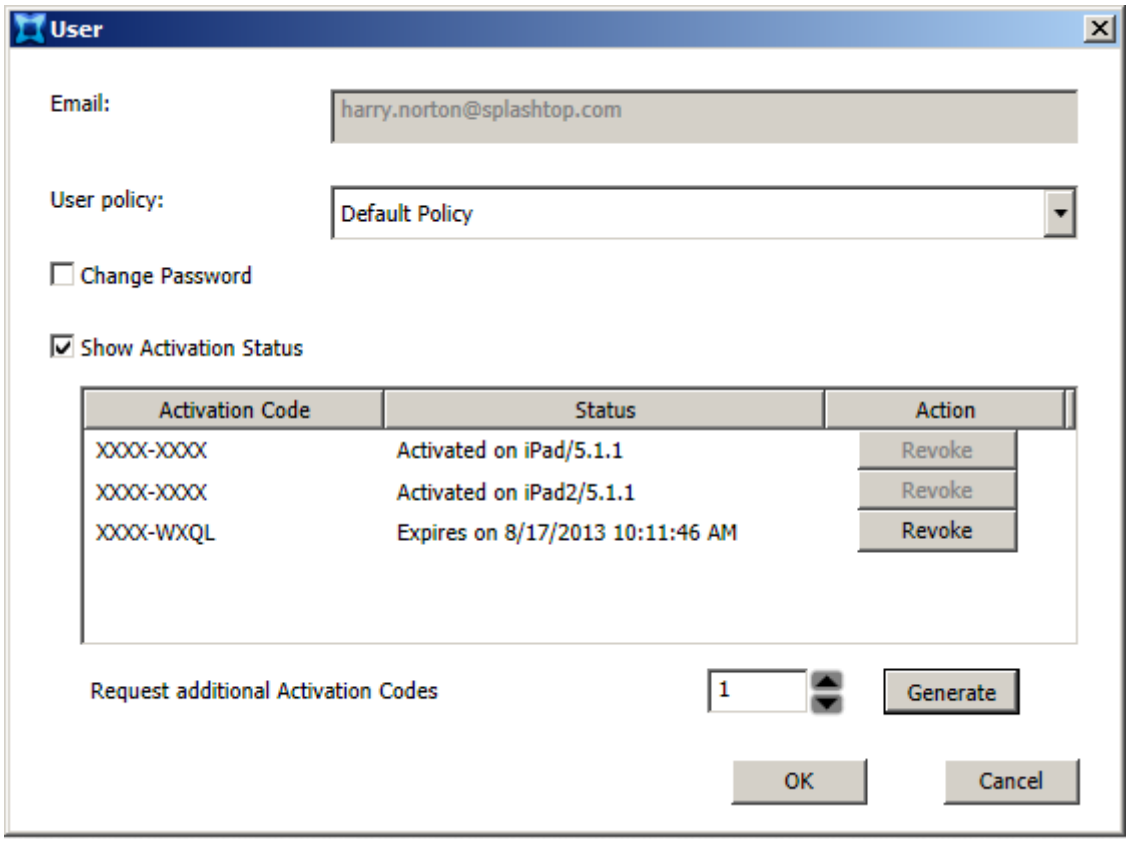
Conversely, if **Enable Device Activation** is disabled, then when adding a new user, you will *not* have the **How many devices to activate?** option at the bottom of the *Add User* dialog box, as shown below.



⚠ CAUTION: If you disable the **Enable Device Activation** option after enabling it, this would invalidate all activation codes that have been issued to users:



If you need to generate additional Activation Code(s) for a particular user, open the **Users** tab of the Splashtop Center Console window (shown and explained in Section 4.1). Then click the **Edit** button for the desired user. The dialog box shown below will open.

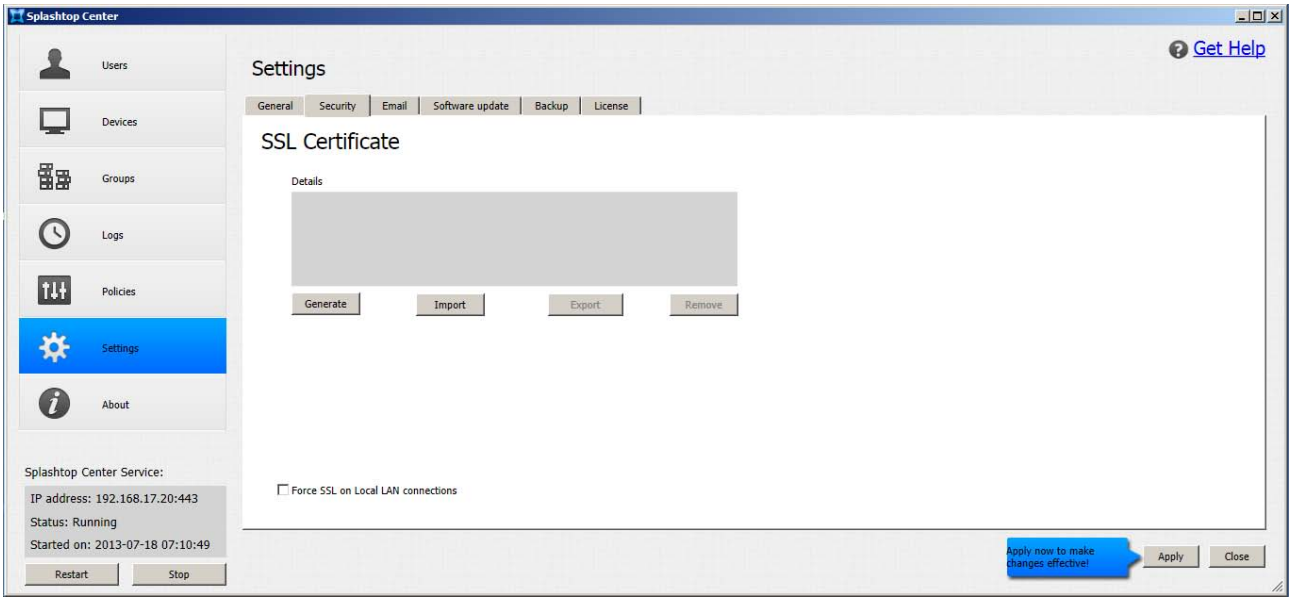


The **Show Activation Status** option allows the IT Administrator to review the status of the Activation Codes for each user. By default, this checkbox is not checked. When you "check" (enable) it, the dialog box expands and the related status information automatically displays as shown in the example illustration above.

The **Request additional Activation Codes** function creates more Activation Codes for the user. You would need to do this if the user has obtained more mobile devices, and now needs Activation Codes for them in order to use Splashtop Enterprise.

4.8.2. 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. (Please see the next sub-section, entitled "Converting a Certificate to PFX File Format," if your certificate is *not* currently in PFX file format.) You can also use the **Security** tab to generate a certificate if you don't have one. When you first open this tab, there is no certificate as shown below.

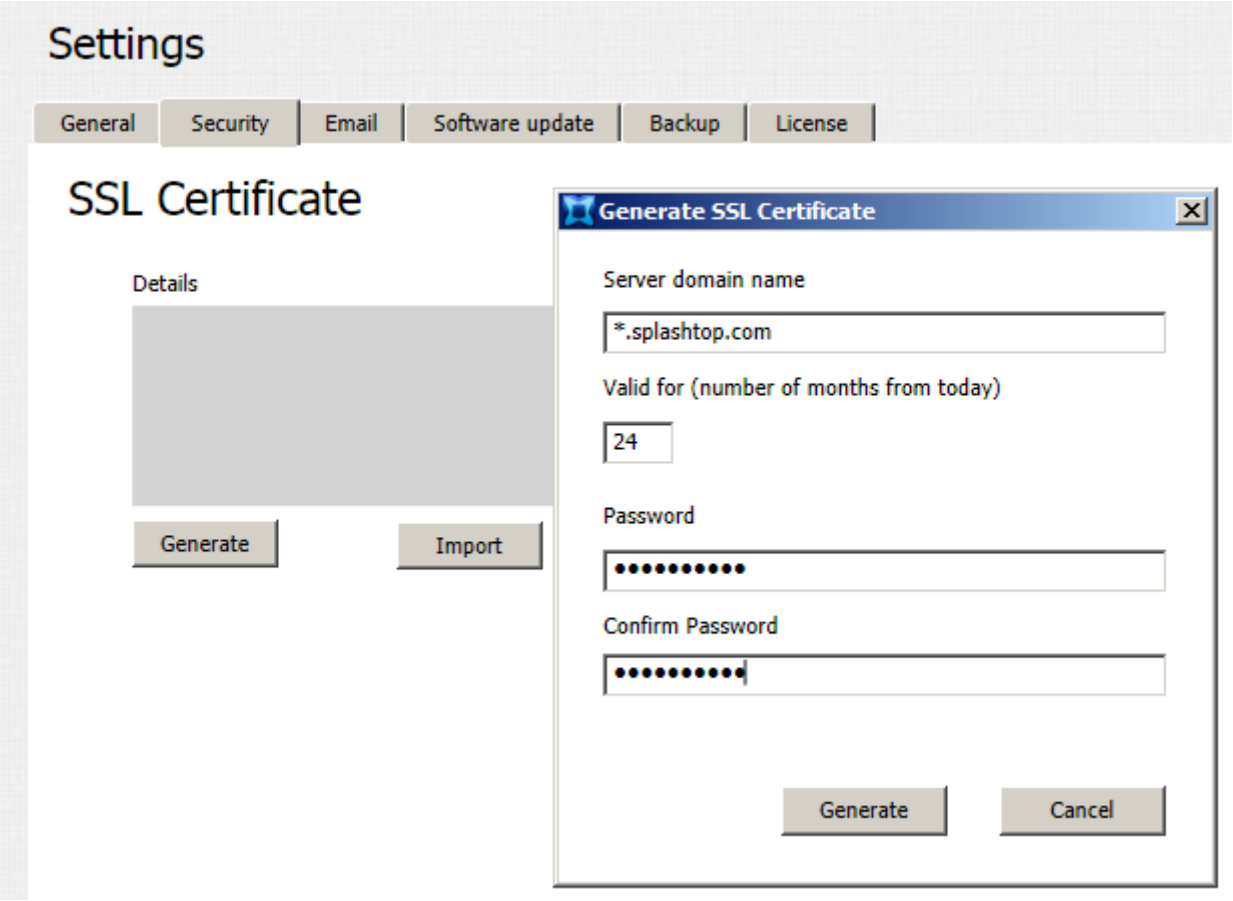


Import button:

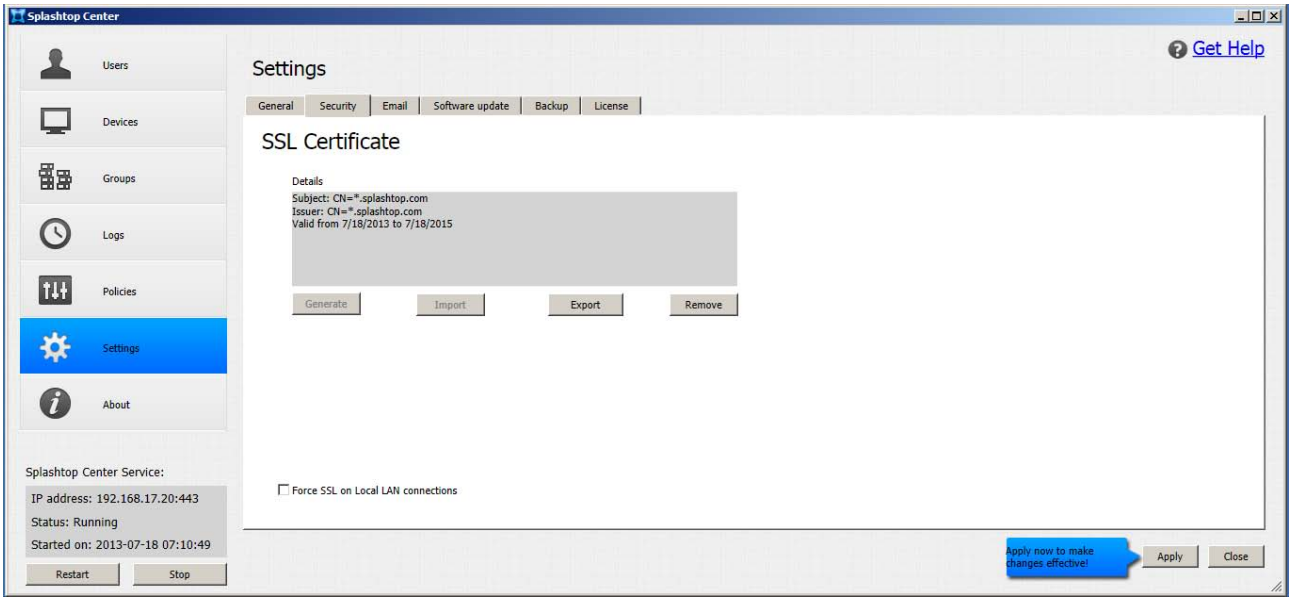
You can import your trusted or self-signed SSL certificate using the **Import** function. Clicking the **Import** button shown above will open the *Import Certificate Assistant* dialog box. Enter the information, then select **Import** in that dialog box. After that, you will need to click the **Apply** button to make the SSL certificate take effect. (If an SSL Certificate already exists, the **Import** button will be grayed out.)

Generate button:

Clicking the **Generate** button opens the *Generate SSL Certificate* dialog box:



If you don't have an SSL certificate to import, this dialog box allows you to use Splashtop Center to generate a self-signed SSL certificate. After clicking the **Generate** button shown in the dialog box above, you will have a certificate. The screen will display similar to the sample illustration on the next page, containing a certificate. Click the **Apply** button. (If an SSL Certificate already exists, the **Generate** button will be grayed out.)



⚠ CAUTION: Clicking **Apply** requires Splashtop Center to be re-started, which means all active remote sessions will be disconnected.

For importing the self-signed SSL certificate, please refer to section 7.3 , entitled **SSL Certificate Import/Export**. This is recommended.

Export button:

You can back up your SSL certificate using the **Export** function. A **Save As** dialog box will open, in which you can specify a filename and folder location.

Remove button:

Use the **Remove** function if you need to remove the certificate.

Force SSL on Local LAN connections

The **Force SSL on Local LAN connections** option on the **Security** tab provides more security protection for local LAN connections. The option is unchecked by default. Splashtop Streamer v2.4.0.x and Splashtop Enterprise clients v2.3.5.x will support the new SSL LAN connection method natively, without any need to go through Splashtop Center. If the option is turned on, it will serve as "fall-back" and will be used as the alternative, in case Streamer and client cannot successfully establish a new SSL LAN connection. After checking this checkbox, you will need to click the **Apply** button to make this option take effect.

4.8.2.1. Converting a certificate to PFX file format

If you have an SSL certificate which is *not* in PFX format, here's how to convert it into a PFX file so you can import it into Splashtop Center.

1. Click **Start** to open the Start Menu, followed by **Run**. Type **MMC.exe**, and then click **OK**. Click **File** and then **Add/Remove Snap-in**.
2. Click **Add**. Highlight the "certificates" and then click **Add** again.
3. Choose **Computer account** and then click **Next**. Select **Local Computer** followed by **OK**. Click **Close** and then **OK** to close the "Snap-in" window.
4. Open the **Certificates** (Local Computer) snap-in that you created. Go to **Personal** followed by **Certificates**.
5. Right-click on the server certificate you want to convert, and then select **All Tasks** followed by **Export**.
6. Click **Next** on the wizard that opens. If the wizard doesn't open, repeat Step 5. If it still doesn't open, restart your computer and go back to Step 4.
7. Choose **Private key** as your export, and then click **Next**.
8. Choose the Personal Information Exchange (PFX) file format to create a PFX file.
9. Click **Next** and choose a password for the file. Click **Next** again.
10. Choose the file name. Don't include an extension, as the wizard automatically adds the PFX extension.
11. Click **Next**, write down where the file is saved to, and then click **Finish**.

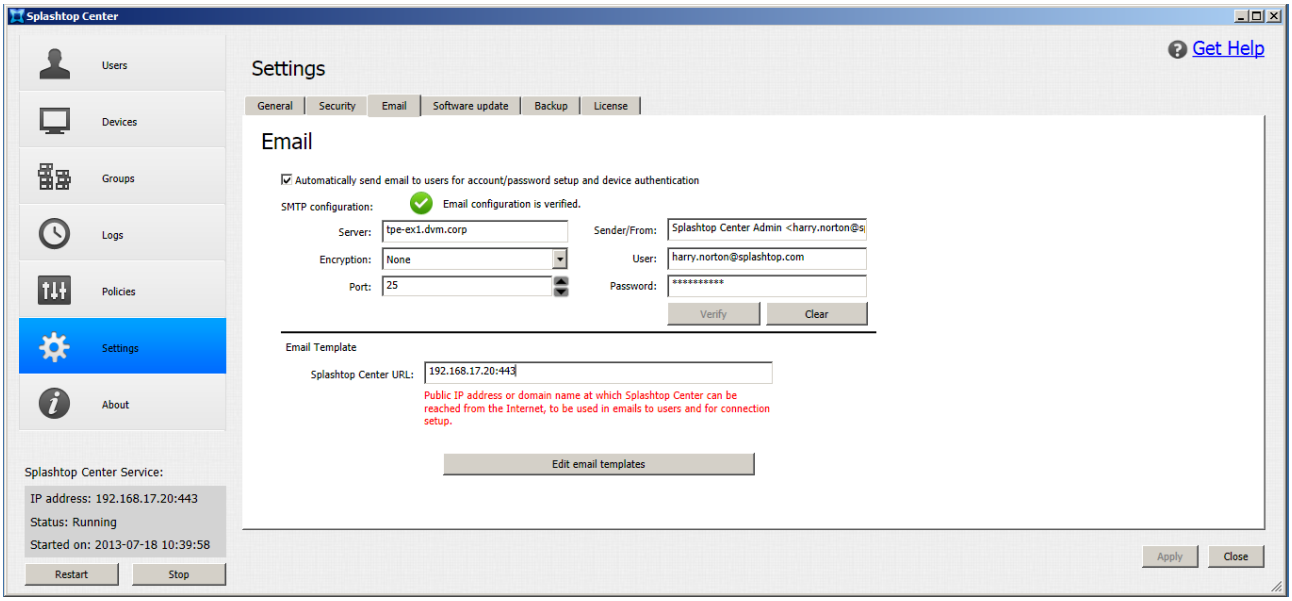
4.8.3. Email

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 automatic Emails will contain the related information and give the users instructions on how to proceed. 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.

For example, when you add a new user to Splashtop Enterprise via the **Users** tab in the Splashtop Center Console window, "Invitation Email" will automatically be sent to the user (if you choose to take advantage of this option). The Email will contain a link which the user can conveniently click to download the Splashtop Enterprise app to his/her mobile device, and the Activation Code to enter, plus instructions. In addition, if you assigned a temporary password to the user during the Add User process, the Email includes this password plus a link for the user to click on and then change the password.
The **Email** tab of **Settings** is shown below, with sample data entered.



Automatically send email to users for account/password setup and device authentication

If the **Automatically send email to users for account/password setup and device authentication** checkbox is checked, then when you add a new user to Splashtop Enterprise, "Invitation Email" will automatically be sent out to that user. Email will also be automatically sent for password resets/changes, and whenever additional activation codes are generated for a user. This simple checkbox is where the automatic Email feature is turned On or Off (but required fields in this Email tab also need to be set correctly).

Server

In this field, enter the address of the Mail server. For example, for Gmail, it could be **smtp.gmail.com**. (Please note that if the SMTP configuration is not using encrypted communication protocol, Splashtop Center does not handle Email encryption/protection.)

Encryption

In the Encryption drop-down list, you can select **None**, **TLS** (Transport Layer Security), and **SSL** (Secure Sockets Layer).

Port

This is the port number used by the server which is specified in the **Server** field above.

Sender/From

Enter your IT Administrator <Sender Display name> and <Relay Email address> one time here, and it will be retained and used for each automatic Email sent to users. The "Sender" portion of the text is optional, but of course your Email address is required. We suggest "Splashtop Center Admin" as the optional "Sender Display Name" text, followed by the Email address enclosed in "< >"

User

This is the SMTP account which sends the Email, so this basically only needs to be entered one time (unless the Email address used by the IT Administrator to send automatic Email changes someday).

Password

This is the password you use in conjunction with the Email address entered in the **User** field above it.

Verify

After entering all the data in the fields, click the **Verify** button. If any data is detected as invalid or missing, a message will inform you of such. If no problems, the message "Email configuration is verified" will display, as shown in the illustration above.

Clear

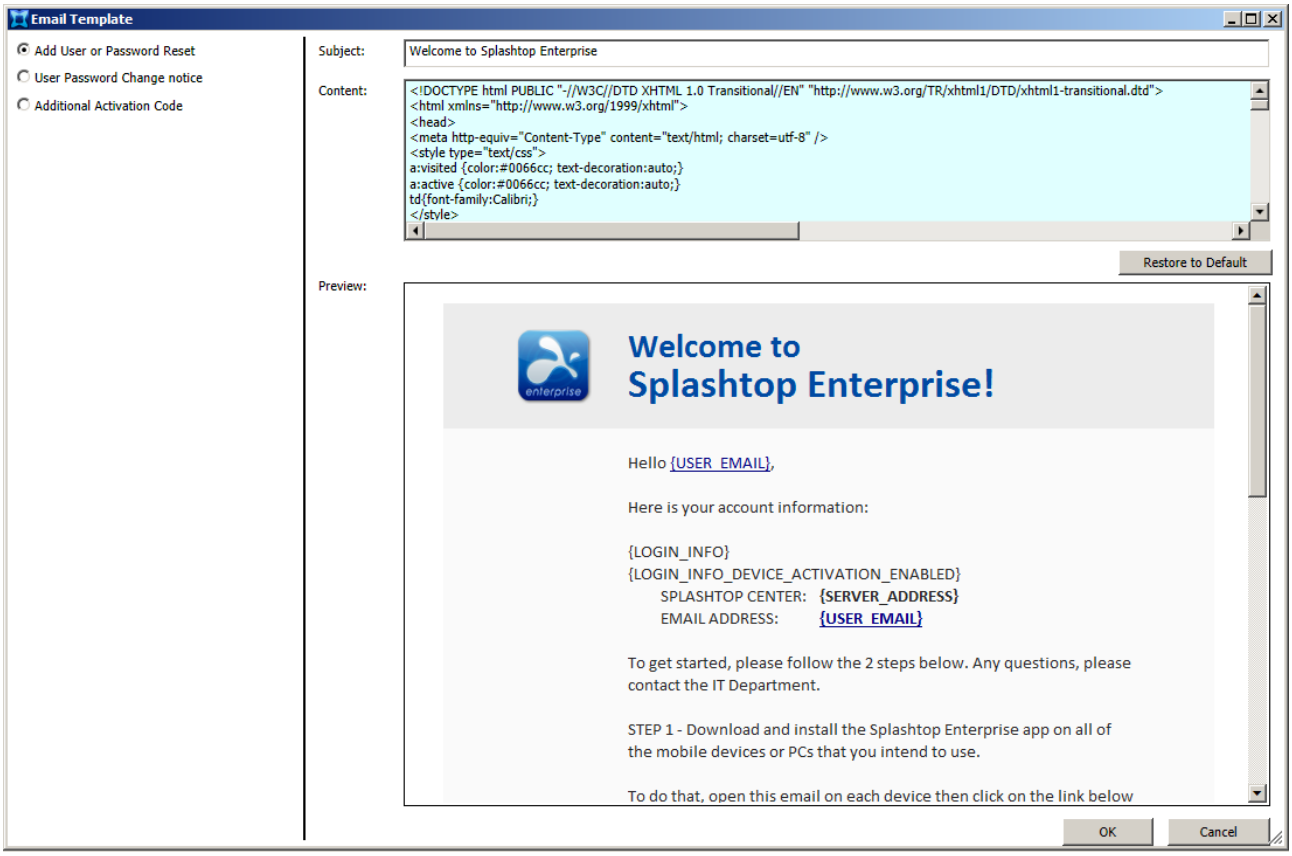
Clicking **Clear** will return all fields to their original default status. Basically, they will all be blanked out except for the default value in the **Port** field.

4.8.3.1. Email Templates

The content of the automatically sent Email will vary according to the situation. Splashtop Center takes that into consideration, and it provides multiple pre-written "templates" containing different text, as shown in the list at the left side of the illustration below.

You can, of course, modify the text before it gets sent. Select the template you want from the list in the left sidebar. You can edit the text in the blue **Content** area if necessary, and view it in the **Preview** area below. Once you click **OK**, the content is saved, and any automatic Email sent by Splashtop Center for that particular situation will use that content.

If you have made changes to customize the content just for temporary or one-time use, you can conveniently click the **Restore to Default** button when you are ready to cancel those changes and return to the original text.



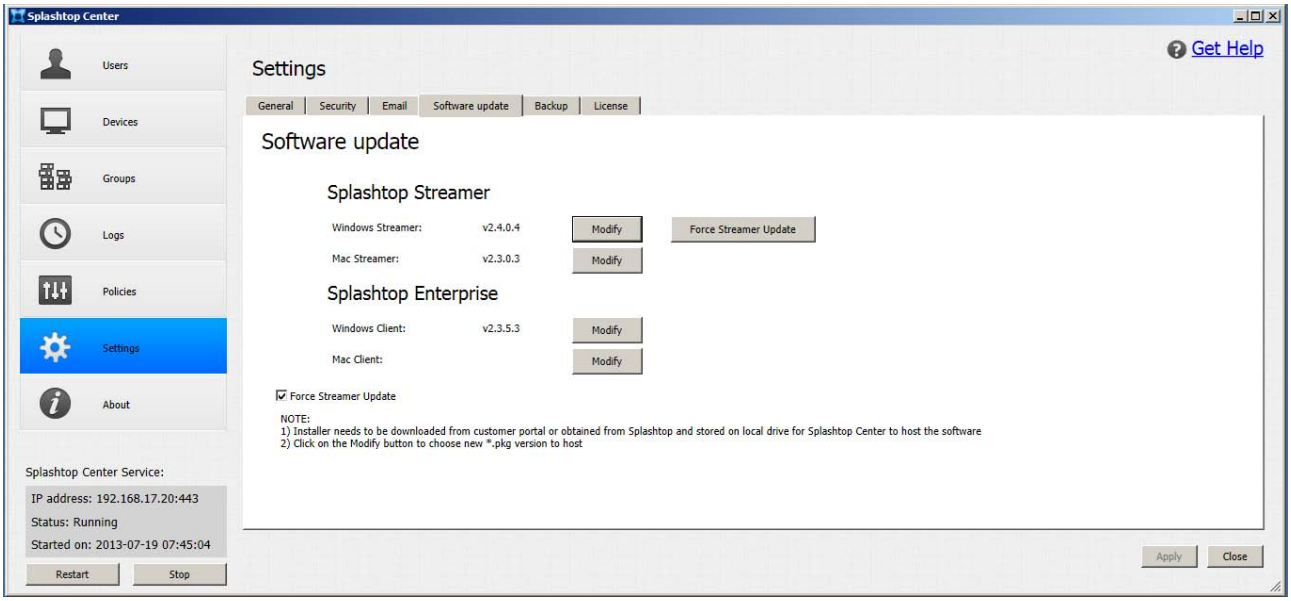
NOTE: Email is basically sent in HTML/Plain multi-part and the mail client will choose the best display (usually HTML). Bounced Email, and Auto-Reply Email from the user, will be ignored by Splashtop Center.

4.8.4. Software Update

The Splashtop Streamer and the Spashtop client app for Windows and for Mac are bundled into every new release of Splashtop Center. Users are given a specific Splashtop Center URL, to download the newest Streamer and Client app, in their Invitation Email.

At his/her discretion, the IT Administrator can designate updated Mac or Windows-based versions for users to download via Splashtop Center, when they become available, as approved for use by their IT Department.

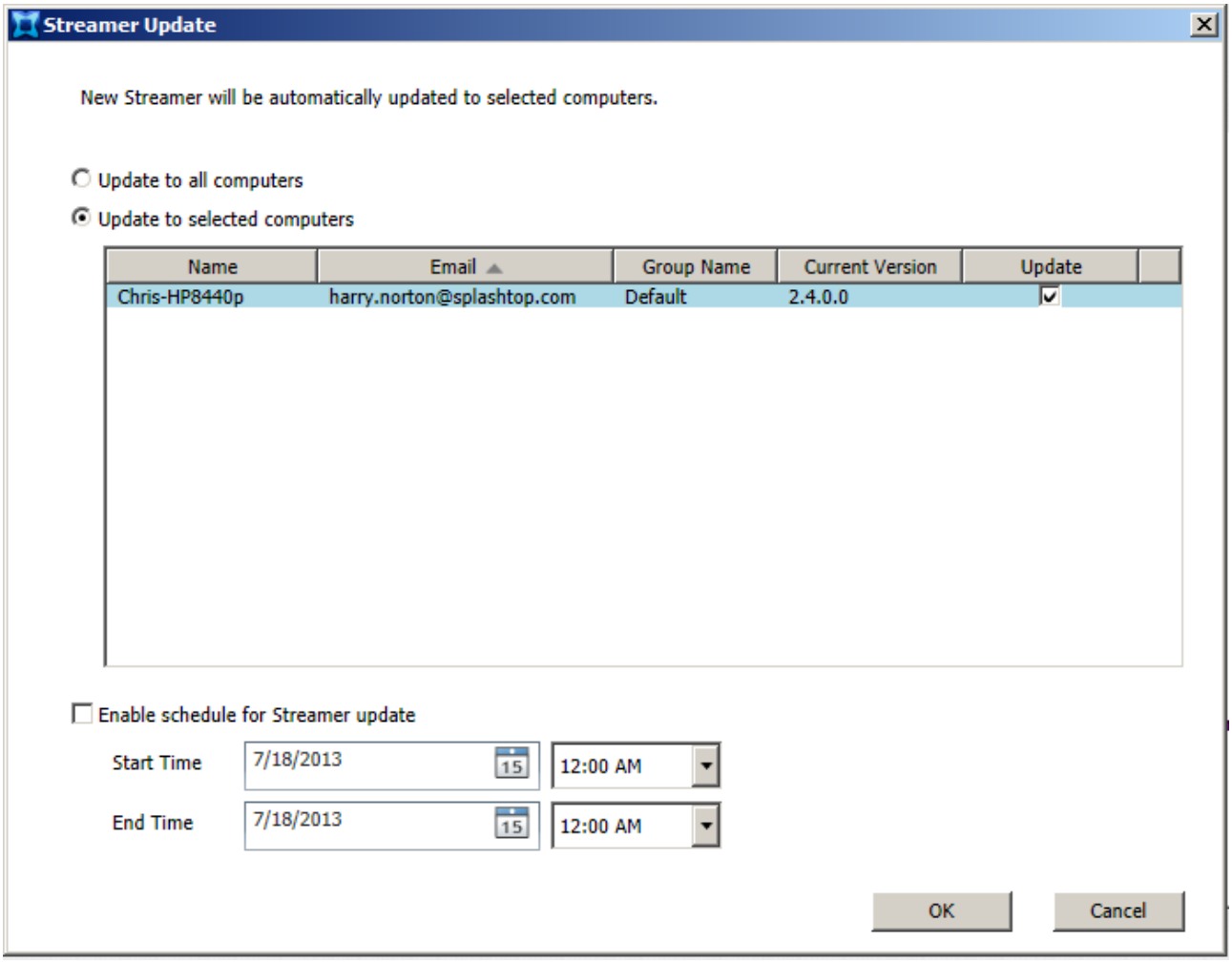
We at Splashtop Inc. will keep you informed of new Streamers when they become available. You can then download the **.pkg** file from our customer portal to a local folder on your server. Click the **Modify** button in the **Software Update** tab of **Settings** to open a "browse box" where you can navigate to and select the **.pkg** file of the new Streamer which you want to upload to Splashtop Center and replace the existing **.pkg** file.



When the **Force Streamer Update** checkbox is checked, the **Force Streamer Update** button will be enabled as shown above. In this case, the Splashtop Center upgrade won't replace the Windows Streamer with the newly bundled version. On the other hand, when the **Force Streamer Update** checkbox is not checked, the **Force Streamer Update** button will be disabled, and the Splashtop Center upgrade will replace the Windows Streamer, updating it to the latest bundled version. Please note that currently, the Windows Streamer is the only software that supports the **Force Streamer Update** function. The IT Administrator can still use the **Modify** buttons, shown above, to update the other software items anytime. Once modified, they will be reflected on the Download page of the Splashtop Center Web Portal.

Click the **Force Streamer Update** button to open the *Streamer Update* dialog box shown below. Select **Update to all computers** if you want to push the Windows Streamer update to all computers in the list.

Or, if you only want to force the Streamer update into certain computers, click the **Update to selected computers** button, and then select the corresponding checkboxes in the **Update** column for the desired computers.

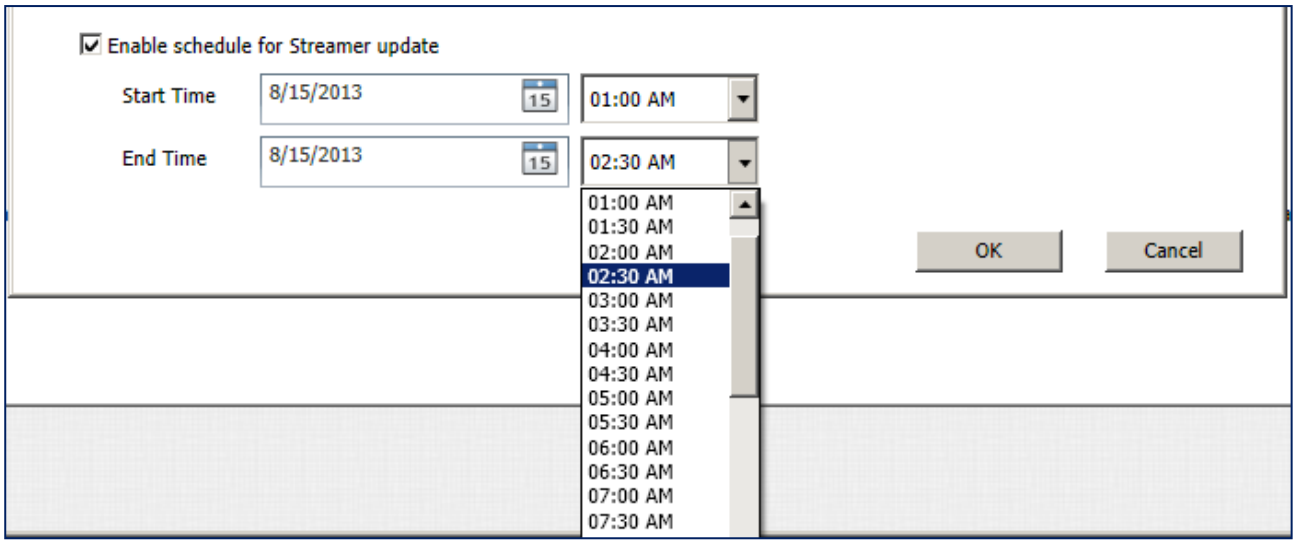


If the **Enable Schedule for Streamer Update** checkbox is *not* checked, as shown above, then the forced Streamer update process will begin immediately when you click the **OK** button. However, you might want to schedule the forced Streamer update to take place at a certain time, as explained in the next sub-section.

4.8.4.1. Scheduling the forced update

Currently, this feature will allow five maximum concurrent downloads from the Streamer, as a way to reduce the network traffic. In addition, as with any other software update, the Splashtop Streamer will of course be unavailable during the update installation process. Therefore, many IT Administrators choose to take advantage of our Scheduling option to set the forced Streamer update to take place at a specific, more convenient time, such as non-peak or after-office hours. In this way, the forced update has the least impact on the users and helps avoid the effect of the network traffic it may generate for the download.

Scheduling a date and time is easy. To do this, simply check the **Enable Schedule for Streamer Update** checkbox, then specify the Date and Time. Click **OK** to close the dialog box, and the forced update will then take place at the specified date and time.



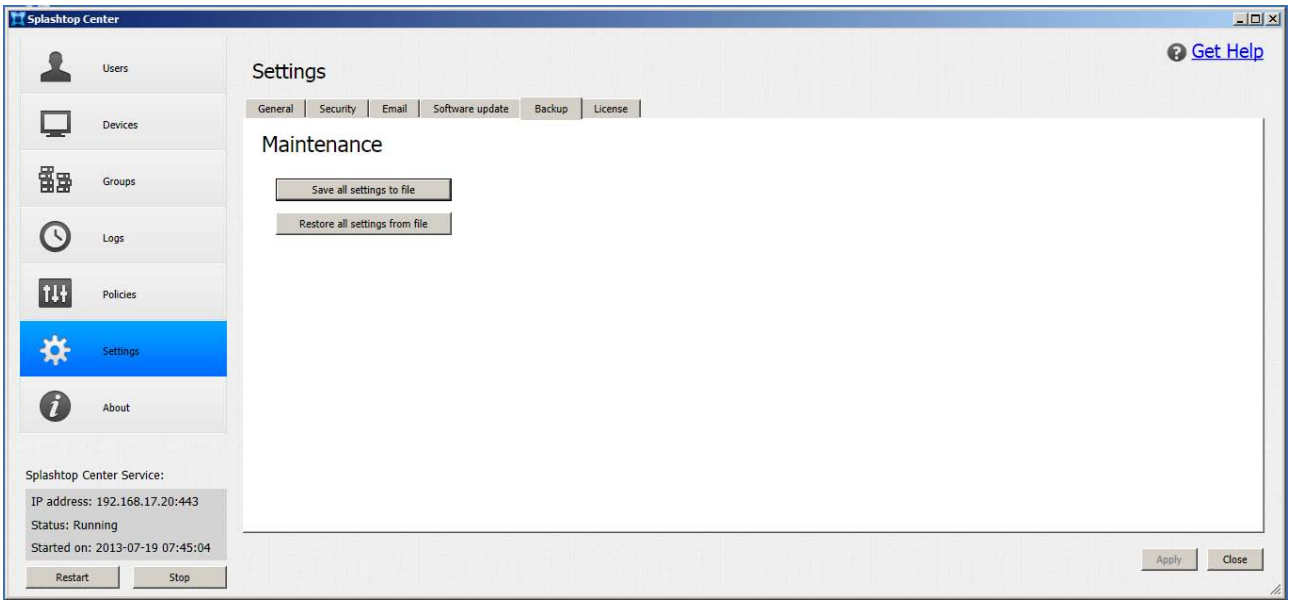
⚠ CAUTION: Please be reminded that, as with any other software update, there is always a small chance that the update installation could fail due to a variety of unforeseen factors, such as some type of conflict with system settings. If the forced update process should happen to fail, then the users may need to manually perform the update on their respective computers individually.

4.8.5. Backup

The **Backup** tab lets you save the whole Splashtop Center database to an .SQL file. In summary, the following data will be backed up:

- ✓ All IT Policies and their settings
- ✓ User settings
- ✓ History for Devices, both computers and clients
- ✓ Email (outgoing Email and templates)
- ✓ Group settings
- ✓ RDP-related data, if any (*RDP Desktop* data and *RDS* data) which has been entered by the IT Administrator via the Splashtop Center Web "Customer Portal" interface.

Clicking the **Save all settings to file** button opens a **Save As** dialog box in which you can browse to the folder where you want the backup file to be saved. By default, the filename automatically contains the date and time of the backup, such as **SC-Backup-20130719-1016.SQL**. Of course, you can change the filename if desired. Click the **Save** button in the Save As dialog box, and that's all there is to it. When the backup process is completed, a message will inform you of such.

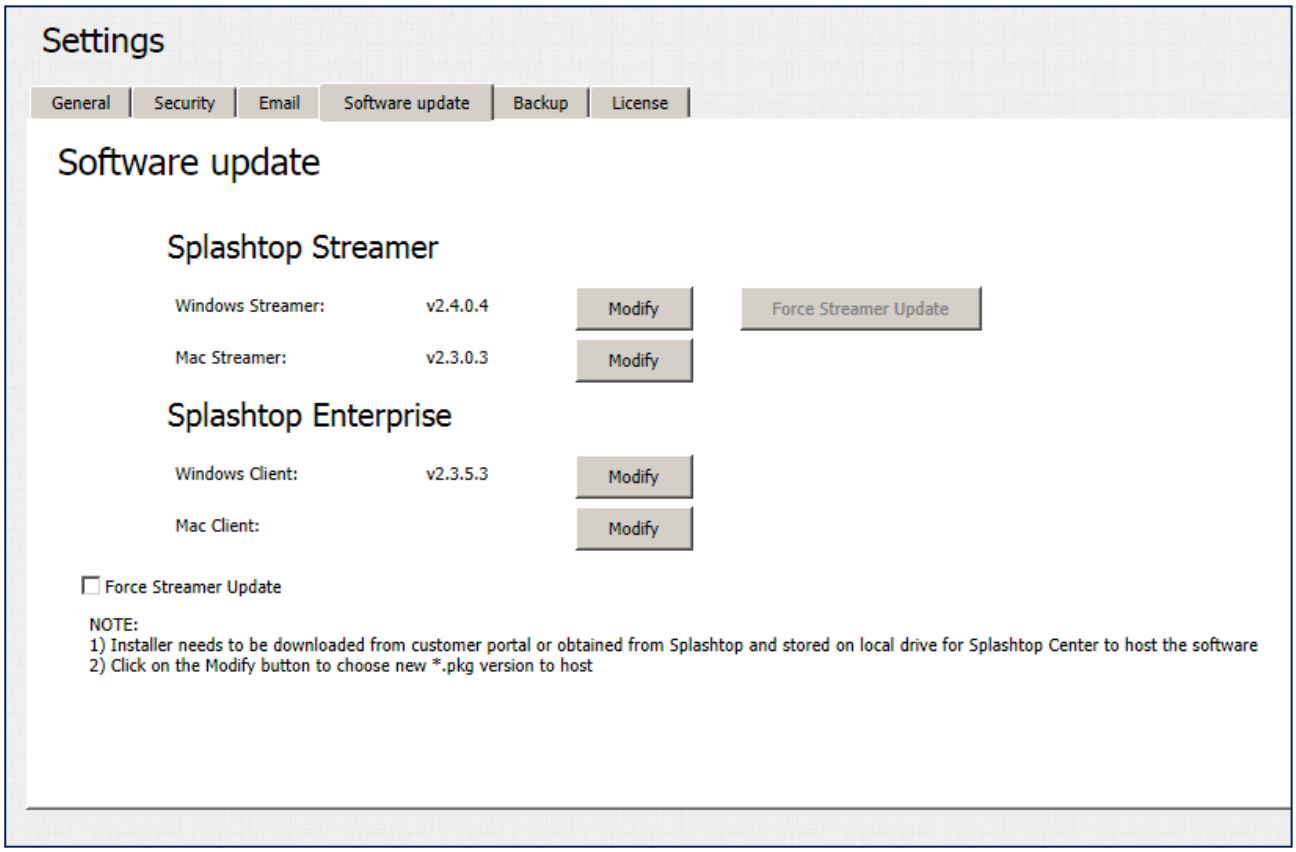


Please keep this backup file in case you need to recover your settings someday, or as a precaution when upgrading Splashtop Center. We recommend that you back up regularly. In addition, a reminder that it's a good idea to export and keep records of Session logs on a regular basis for auditing purposes, as explained earlier in the **Logs** tab section.

The **Restore all settings from file** button allows you to use the backup file to restore your settings.

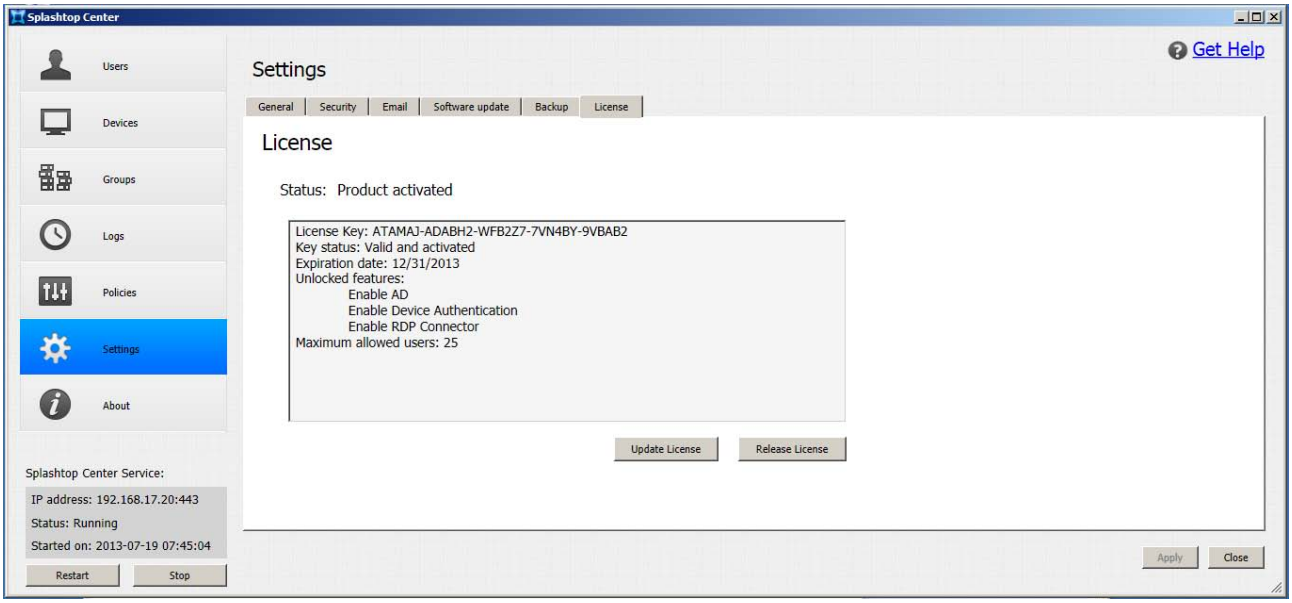
⚠ Caution: If you choose to do this,the Splashtop Center Service would be stopped, and current settings would be overwritten with the settings in the backup file.

NOTE: We at Splashtop Inc. will keep you informed of new versions when they become available, or you can get the latest Splashtop Center update from our website anytime. The latest updates for the Streamer and Client apps can be downloaded using the Downloads tab in the **Splashtop Center Web Portal**, as shown in the next chapter. And, a reminder that the newest Streamer and Splashtop Enterprise should be kept for access from the **Software Update** tab (shown below) as suggested earlier in section 4.8.4.



4.8.6. License

The **License** tab displays your License Key, the Key status, Expiration date, Unlocked features (if any), and maximum allowed users/computers ("Seats").



Assign License:

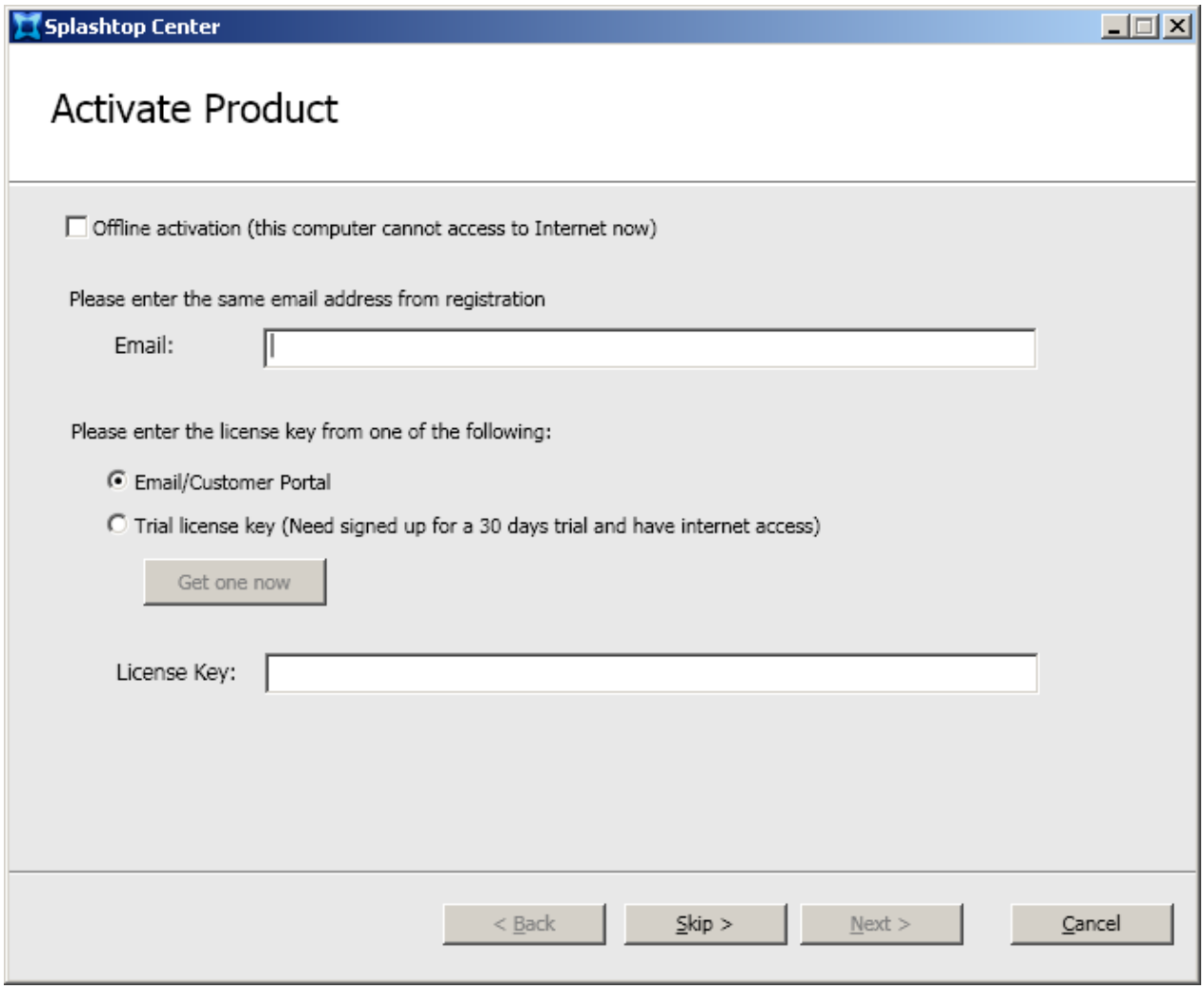
After initially installing Splashtop Center, and if you did not activate it during the installation process (see next page), you can click the **Assign License** button in the Settings/License tab to enter the required information and activate your License Key.

After Splashtop Center has been activated as shown in the example above, the **Assign License** button no longer displays. Instead, the **Update License** button will become available.

Release License:

Click the **Release License** button to remove the current License Key. Please note that a license cannot be "revoked" after it has been activated on a machine; nor is there currently any way to transfer a license.

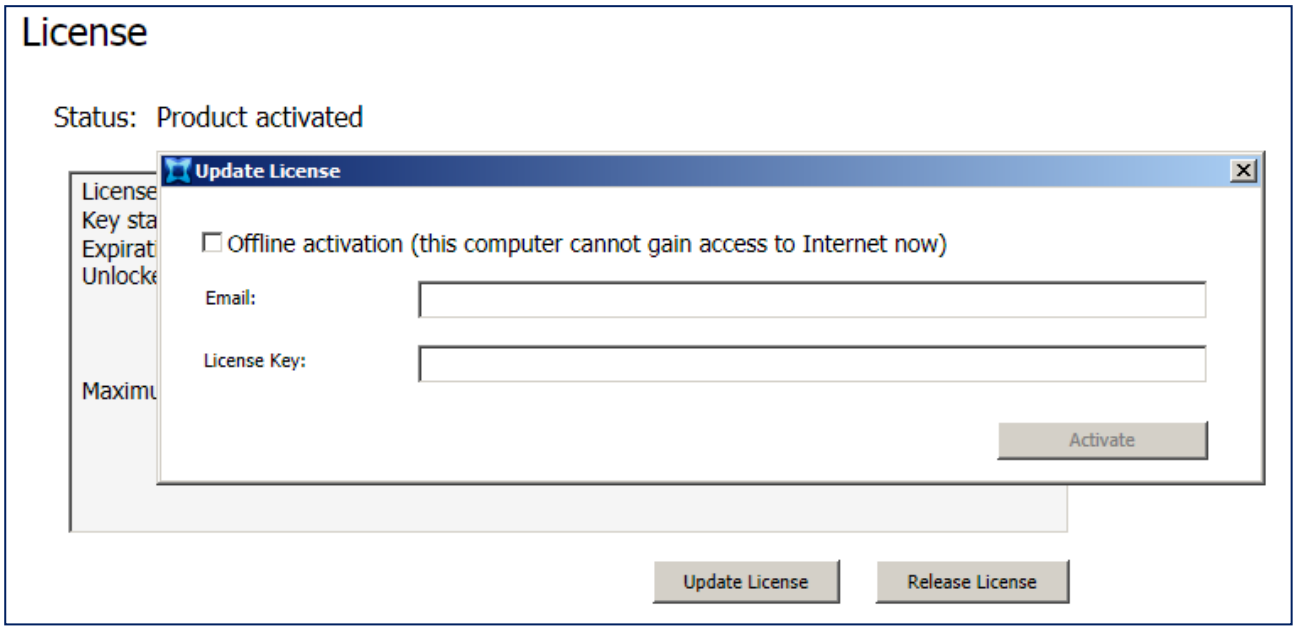
NOTE: It is not required to activate Splashtop Center during installation using the dialog box shown below (but you may find it more convenient to do so). If desired, you may opt to click the **Skip>** button, and just proceed with the installation process. At any time after the installation is finished, you can use the License/Tickets page in the Customer Portal to get the License Key that you will need in order to activate Splashtop Center. Then use the **License** tab of **Settings** to activate manually at anytime.



Don't forget that the License Key would need to be re-activated if you were to re-install the software someday. This includes situations wherein you upgrade or clean the installation of Splashtop Center — you would need to activate the License Key again. Please keep in mind that one License Key can be activated up to five times on the same machine.

4.8.6.1. Updating Online

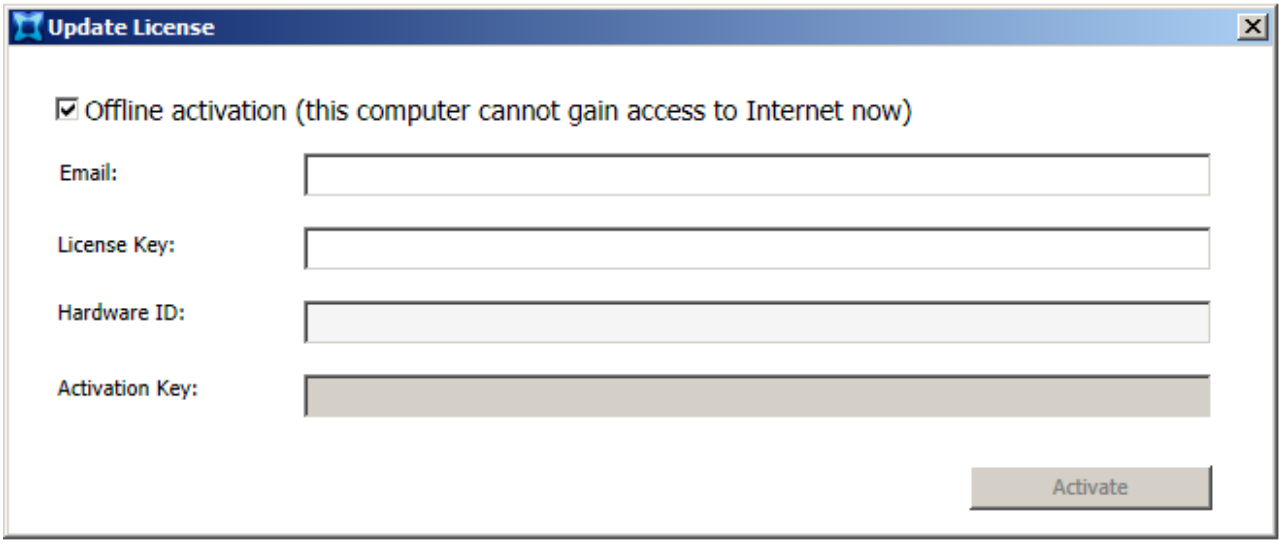
If you get a new license agreement (for example, you purchased additional Seats), click the **Update License** button in the Settings/License tab. The dialog box shown below will open, for activating the license online. Enter your **E-mail** address and the new **License Key** in the fields shown below. Then click the **Activate** button to activate the new license in Splashtop Center.



Of course, in order to activate the license online, the system needs to have Internet access to talk to the License Server. If you don't have Internet access, see "Updating Offline" below.

4.8.6.2. Updating Offline

For your convenience, offline updating/activation of the license is provided, for those Servers which cannot gain access to the Internet. In this case, check the checkbox for the **Offline activation** option and input the appropriate **Email** address and **License Key** in the related fields. Splashtop Center will generate a machine code for the **Hardware ID** field. Please send the Email address, License Key, and Hardware ID to your Splashtop contact or Systems Integrator. They will provide an Activation Key for you to enter into the **Activation Key** field and complete the license update/activation.

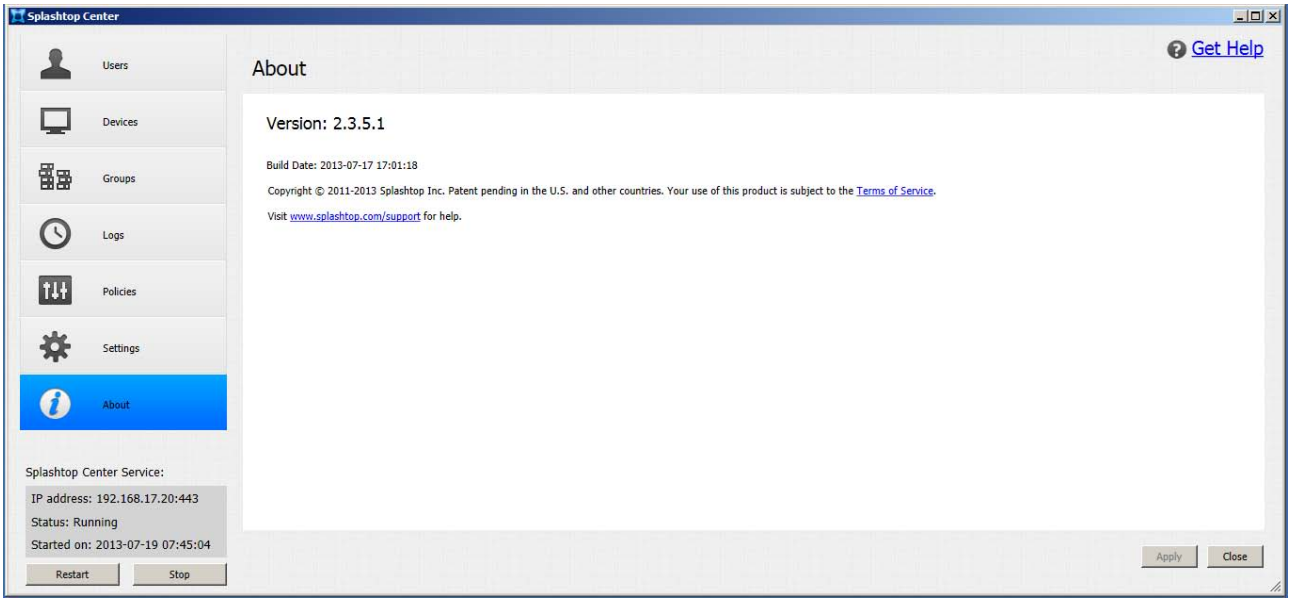


In any case, you can update or restore your License Key with no interruption to your Splashtop Center service. There is no need to restart the service, and the remote user connections currently in session will not be lost/disconnected.

NOTE: If you update/restore your License someday, and Splashtop Center detects that there are not enough available Seats at that moment, it will automatically disable users (as a way of continuing service so it will not need to be interrupted). A message will pop up, to notify you of the number of auto-disabled users, and the names of each user.

4.9. About

As shown in the sample illustration below, the **About** tab displays the version number of your Splashtop Center, and the related copyright information. It also contains links to some additional support/help information, and our Terms of Service agreement.



5. Navigating the Splashtop Center Web Portal

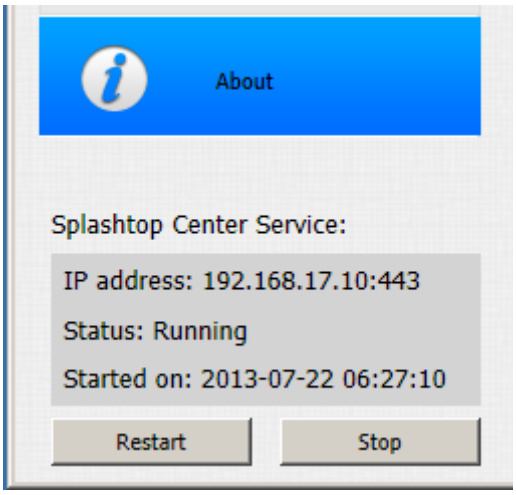
As your Splashtop Center Customer Portal, the Splashtop Center Web Interface ("Web portal"), provides a means for users to change passwords, download Splashtop Enterprise applications, and optionally to set up native SplashApp/RDP (Remote Desktop Protocol) support on Windows-based machines for remote desktop and applications using Splashtop Enterprise clients.

5.1. Accessing the Splashtop Center Web Portal

To access the Splashtop Center Web portal, open a web browser and enter a URL which is in the following format:

https:// *<your Splashtop Center IP Address>* /html/login.html

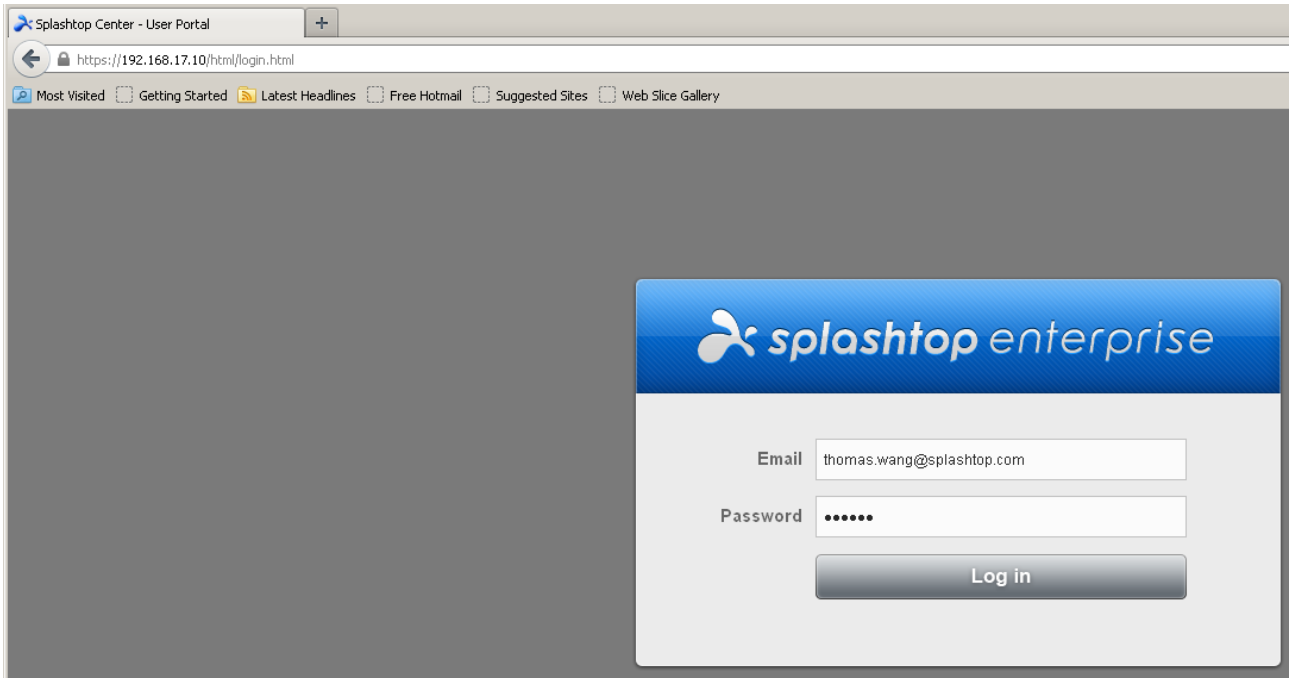
If you don't know the IP Address, to fill in the "*<your Splashtop Center IP Address>*" portion of the above URL formula, it is shown in the lower left area of your main Splashtop Center Console window. In the example below, the IP Address is shown as 192.168.17.10.



So, in this case, the URL would be: **https://192.168.17.10/html/login.html**

5.2. Logging in

After you enter this URL, the first screen that appears, shown below, requires you to enter the E-mail address and Password you use for your Splashtop Enterprise account. Then click **Log in**.



If you log in as a regular Gateway user

If you log in as a standard Gateway user with your personal Splashtop Account (E-mail and Password), you will have two tabs available in your Splashtop Center Web Portal: **Password** and **Downloads**. The user logging in above is a regular Gateway user (not Administrator), so an example of the "Password and Download" screen is shown on the next page.

If you log in as a Domain user

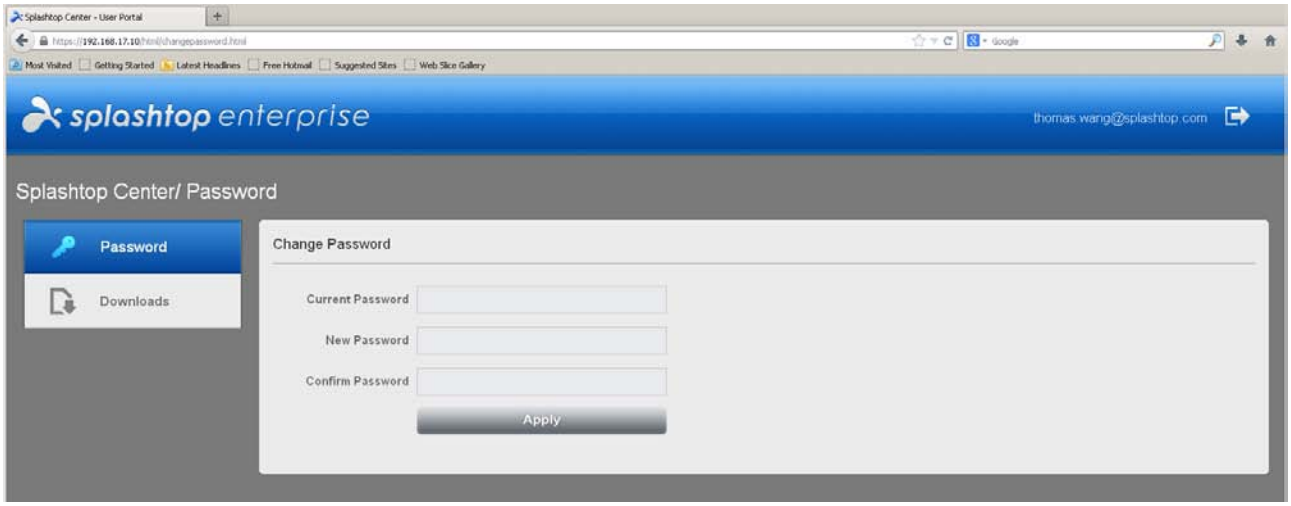
If you log in as a Domain user, you will only have one tab available: **Downloads**.

If you log in as Administrator

If you log in using an Administrator account, you will have all tabs available to you (example shown later in this chapter). This includes the new SplashApp/**RDP Connector** option, which allows you to use RDP (Remote Desktop Protocol) for remote connection, using Splashtop Enterprise clients, and to create groups. However, if you have not obtained the optional **RDP Connector** from us, then you will not have the **RDS** tab and **RDP Desktop** of the Web portal, which are shown and explained here in chapter 5.

5.3. Password tab

The **Password** tab is illustrated below. It allows you (or your regular users) to change your respective passwords.



If you had created a temporary password initially for a Gateway user when adding him or her to Splashtop Center, then the Invitation Email sent to the user will contain that password, and will include a link which he/she can click to change his/her password. This link will take the users to this **Password** tab in the Splashtop Center Web portal, where they can change their passwords.

The password policy mandates that the password must be at least six characters in length, and must contain at least one numeric character.

The allowed character sets are: Alphabetic: A-Z or a-z; and Numeric: 0-9.

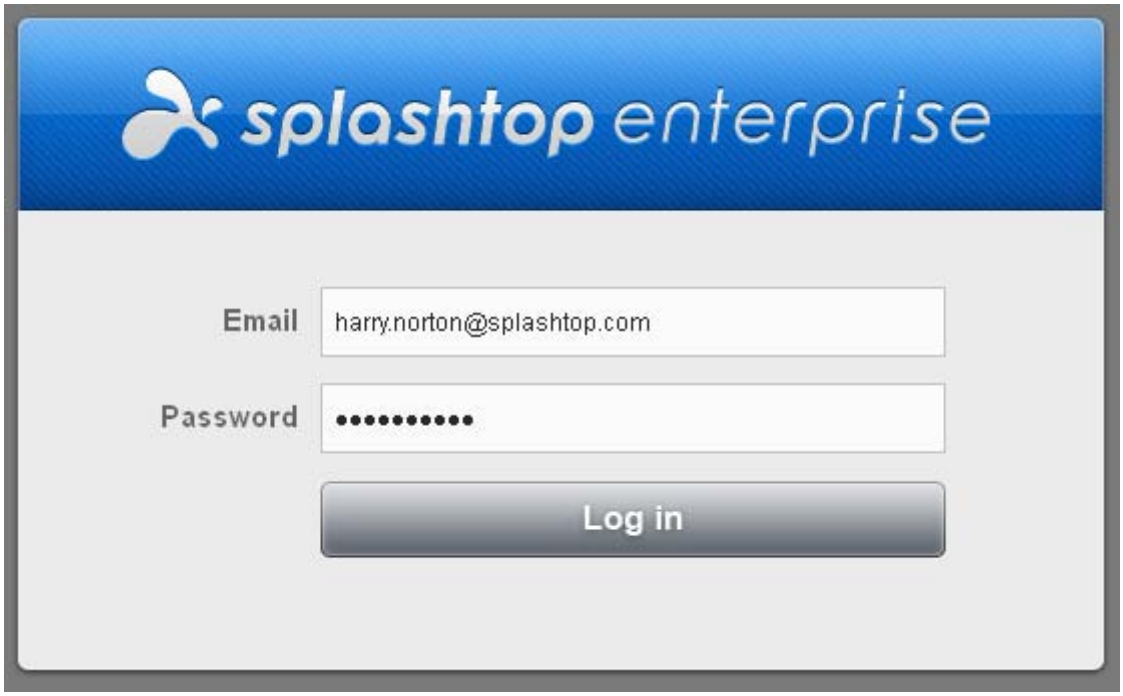
⚠ CAUTION: When you click the **Apply** button, a message will remind you that the new password will take effect immediately (after you click **OK** in the message box), *and will cause both Streamers and clients to be logged off.*

5.4. Downloads tab

The **Downloads** tab is illustrated below, and is available to *all* users who can access the Web Portal. It allows you or your users to conveniently download Streamers, Client Apps, an SSL Certificate; and may also contain pointers to the Apple and Google Play stores for the respective app downloads. The illustration below is an example for reference only.

NOTE: When ready to log out of the Web Portal, click the  button near the upper right corner.

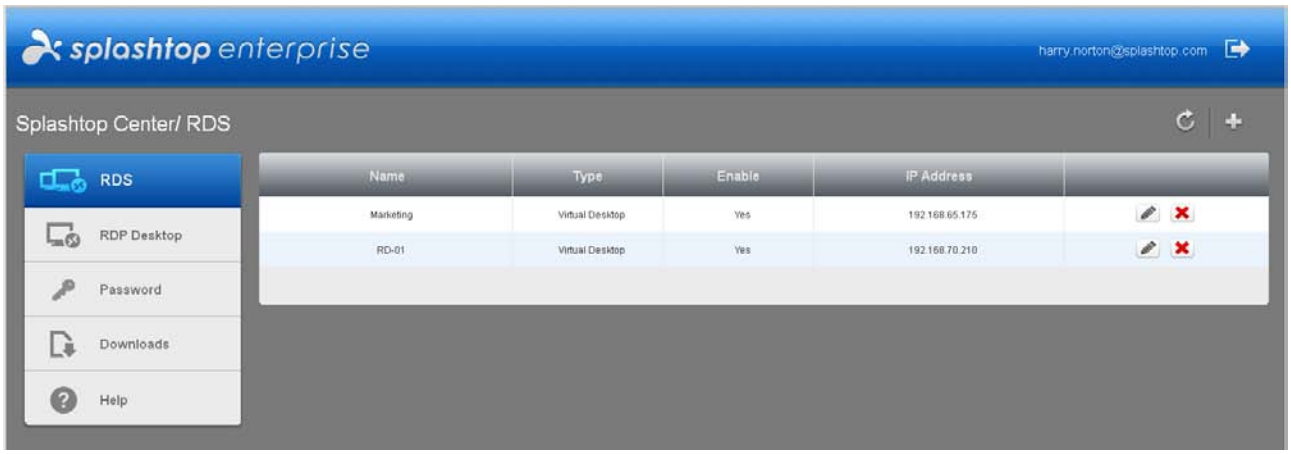
The illustrations in the previous two subsections (the Password tab in 5.3 and the Downloads tab in 5.4) were done when a regular Gateway user was logged in, so there were only two tabs available in the Web Portal screen. Now, we will log in using an Administrator Account. More tabs will be available.



Below, we explain the three additional tabs that may be available for Administrators: **RDS**, **RDP Desktop**, and **Help**. (The **Password** and **Downloads** tabs were already explained on the previous pages.)

5.5. RDS tab

If you have obtained our SplashApp/**RDP Connector** option, you may receive a new License key; and "*Enable RDP Connector*" will be shown in the **License** tab, as shown in the first illustration in section 4.8.6, License. Enter and activate your License Key in the **License** tab of **Settings** as explained earlier in this Guide, then (if you are logged in to the Web Portal as Administrator) you will be able to see the **RDS** tab and **RDP Desktop** tab, shown in the illustration below. In this example, the **RDS** tab shows two "Virtual Desktop" computers that have already been added. Later we will also add a Remote App.

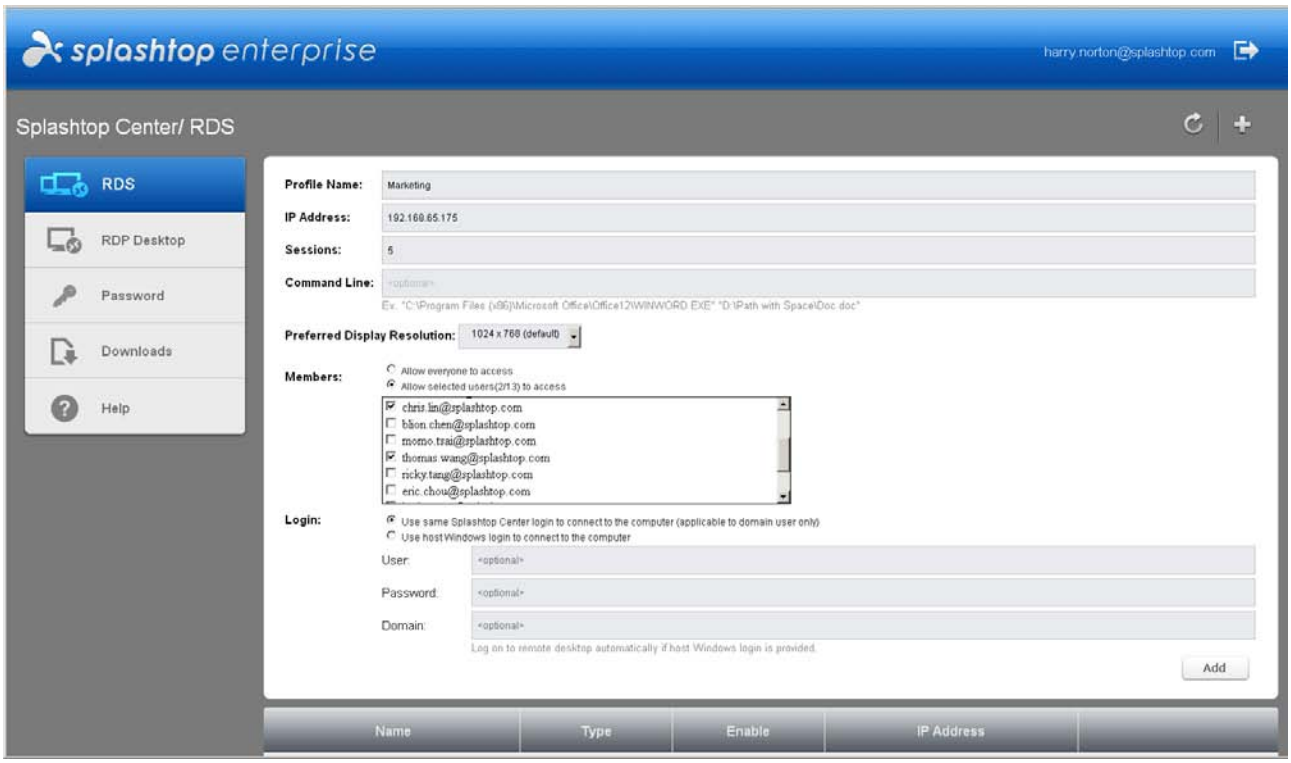


Formerly known as "Terminal Services," RDS (Remote Desktop Services) is a term used in Windows Server that refers to adding a centralized host which offers multiple, simultaneous, virtual desktop or application access to users. In Splashtop Center, IT Administrators can configure the Remote Desktop server to enable session-based virtual desktop and applications for all users (in the **RDS** tab). Here are a couple of definitions for terms as we use them in this chapter.

- **Virtual Desktop**: An entire desktop session from the remote RDS host, which allows users to perform a number of desktop-based tasks, including opening/interacting with applications.
- **Remote applications**: Avoids the necessity to access an entire desktop on the remote system in order to open an application. Users can launch individual applications remot88ely from the client, and each remote application will appear in its own window on the client. (See next subsection.)

Prior to setting up RDS, the server must already be set up to run Windows Server 2008 or later, with Remote Desktop Session Host (RD Session Host) properly configured for hosting Windows-based programs or the full Windows desktop to be accessed by Splashtop Enterprise clients.

Click the  button to **Add** a computer to the list. The *Add* dialog will then appear as shown below.



Profile Name

This is the name which is defined by the IT Administrator, displayed in the Client Profile list page, and is mainly for easy identification of their RDP hosts.

IP Address

This is the IP Address of the RDP host machine.

Sessions

This field is to define the number of concurrent remote access sessions allowed by the RDS server. If you attempt to enter an invalid number (that is, exceeding the limit), a message will pop up and inform you of such; for example, "The current maximum sessions allowed is 100. Please try again."

Command line

This optional field only applies to setting up remote applications. This is where you would specify the application path on the host machine; and the entry in this field is used by **RDP Connector** to invoke applications, using this command, at the time of RDP connection request. The exact command line content can be extracted from the Remote App Manager when setting up the remote application on the RDS server.

For example, below is a sample application path whose purpose is to launch the Internet Explorer browser remotely:

"C:\Program Files (x86)\Internet Explorer\iexplore.exe"

Another example would be a sample application path which includes command line arguments. Please be reminded that command-line arguments need to be set to "Allowed" for the program under RemoteApp Properties of RemoteApp Manager.

"c:\Program files (x86)\Microsoft Office\Word.exe" "d:\Path With Space\Doc.doc"

If an entry is made in the **Command Line** field, then after this item is added, the **Type** column will display "**Remote App**" for easy reference. On the other hand, if the **Command Line** field is left blank, the **Type** column will display "**Virtual Desktop**." See the next illustration for an example of "Virtual Desktop.

NOTE: Don't forget to insert opening (") and ending (") quotation marks for the application path, and additional parameters/arguments separately, in the **Command Line** field (as shown in the two examples above) if you are adding a Remote Application. This allows Splashtop Center to correctly parse the command line content.

Preferred Display Resolution

This option allows you to set the desired resolution of display from the RDP host. When connecting from the Splashtop Enterprise client app using the "Computer native resolution" selection, RDP Connector will use this resolution setting for connection. Currently, RDP Connector supports the following resolutions, which you can select from the drop-down list:

1920 x 1080
1440 x 960
1366 x 768
1280 x 1024
1280 x 768
1280 x 720
1024 x 768 (default)
800 x 600
640 x 480

Allow everyone to access

If this button is selected, all users will have access to the remote desktop or remote applications hosted by the RDS Server.

Allow selected users to access

On the other hand, if this button is selected, only the selected users (from among the Splashtop Center users) will have access to remote desktop or remote applications hosted by the RDS Server. The IT Administrator can select from the members list to set restricted access to RDP.

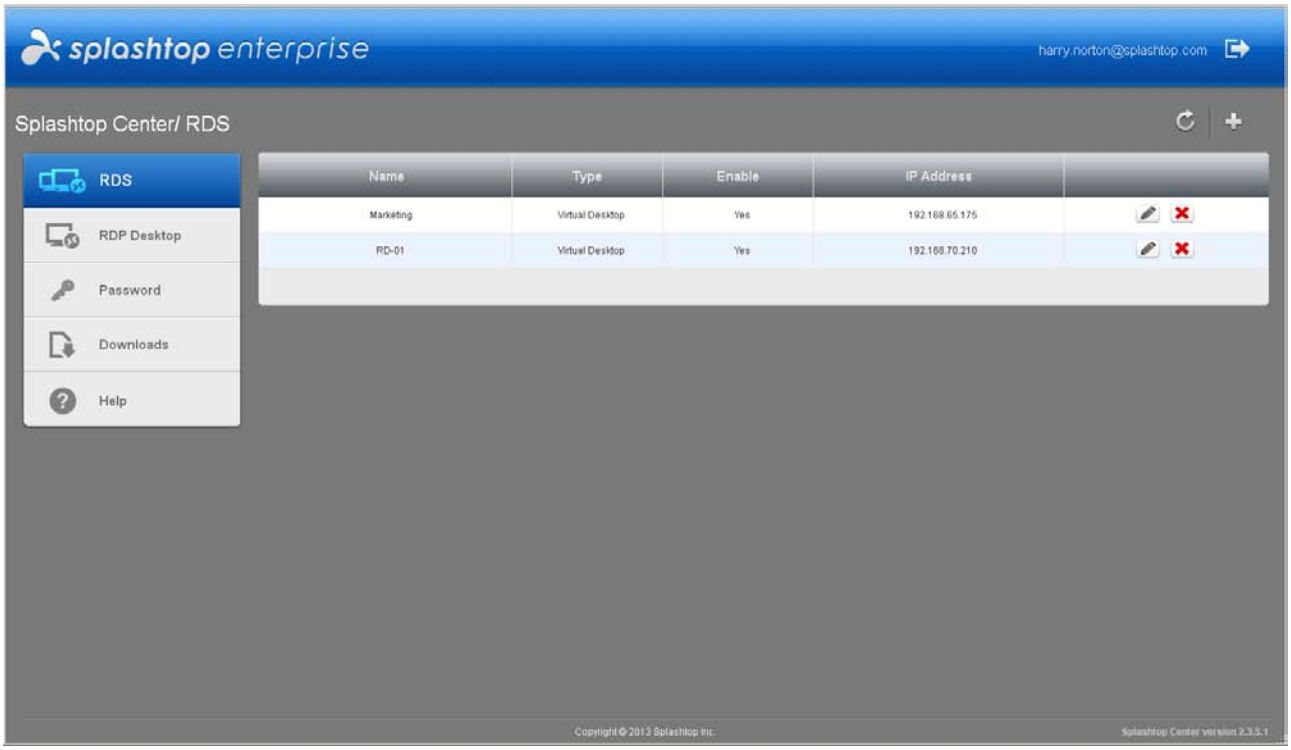
Use same Splashtop Center login to connect to the computer

This setting applies only to Domain (Active Directory) users. If this button is selected, RDP Connector will attempt to use the same Splashtop Center login credentials as the Windows account to log into the RDP Host to connect to the remote desktop or remote applications. Users will still need to enter the Splashtop Center password in the Windows logon page of the RDS server at the time of establishing connection.

Use host Windows login to connect to the computer

This setting applies to both Domain and Gateway users. If this button is selected, users will use the Windows account from the RDS server for connection. The User, Password, and Domain fields will be available. If the Windows account **is** configured, users will be able to log in to the remote desktop/remote application automatically, without seeing the Windows login screen of the RDS server at the time of establishing a connection. If this informaton is **not** entered, the user will need to manually enter the login credentials into the Windows login screen, and the login will have to be provided separately by the IT Administrator to the users.

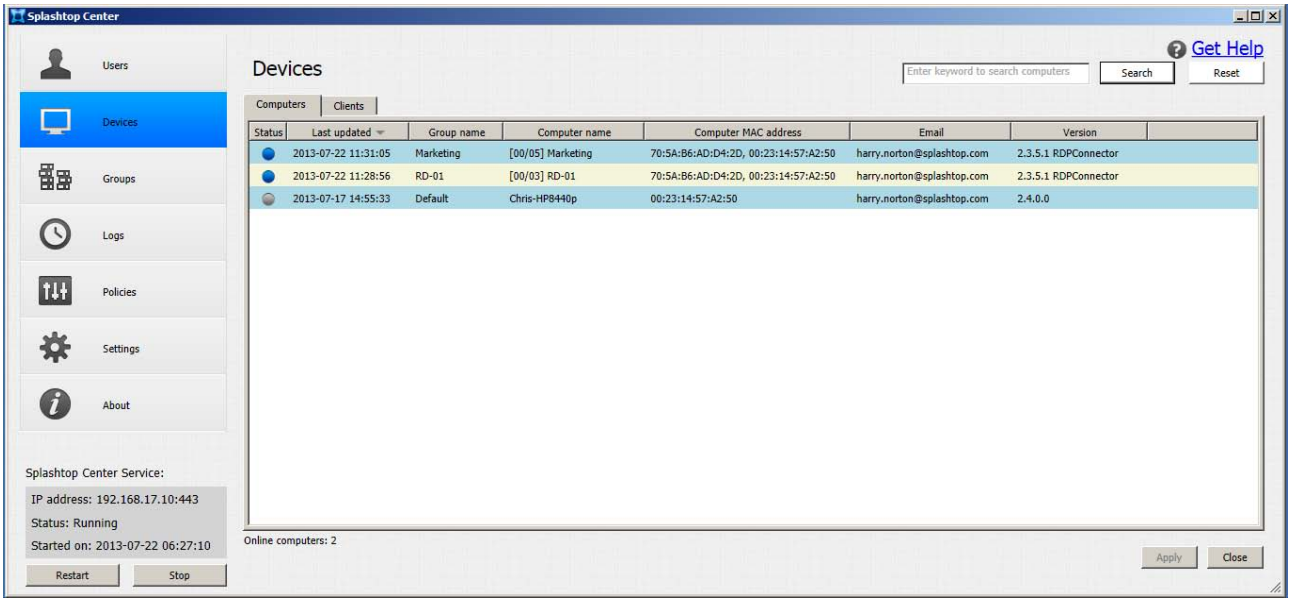
For an example of how to set up RDP remote desktop and RDP computer sharing, please see section 6.8 in the next chapter.



In the example above, we have added two computers, and these will also be shown in the **Devices** tab of your Splashtop Center console (see next page).

After an item has been added, you can view the details by clicking the **Edit** button ( ), or click the associated button to **Delete** a computer from the list.

After RDS servers have been added via the Web Portal, the **Devices** tab of the Splashtop Center Console will list those corresponding RDS servers (in the **Computers** sub-tab of **Devices**). The name in the **Computer Name** column for RDS servers will be prefixed by the connectable (RDP) sessions information, in the format of "[connected sessions / total sessions] RDS server Profile name". Also, the **Version** column will include the "RDP Connector" designation, as shown below.



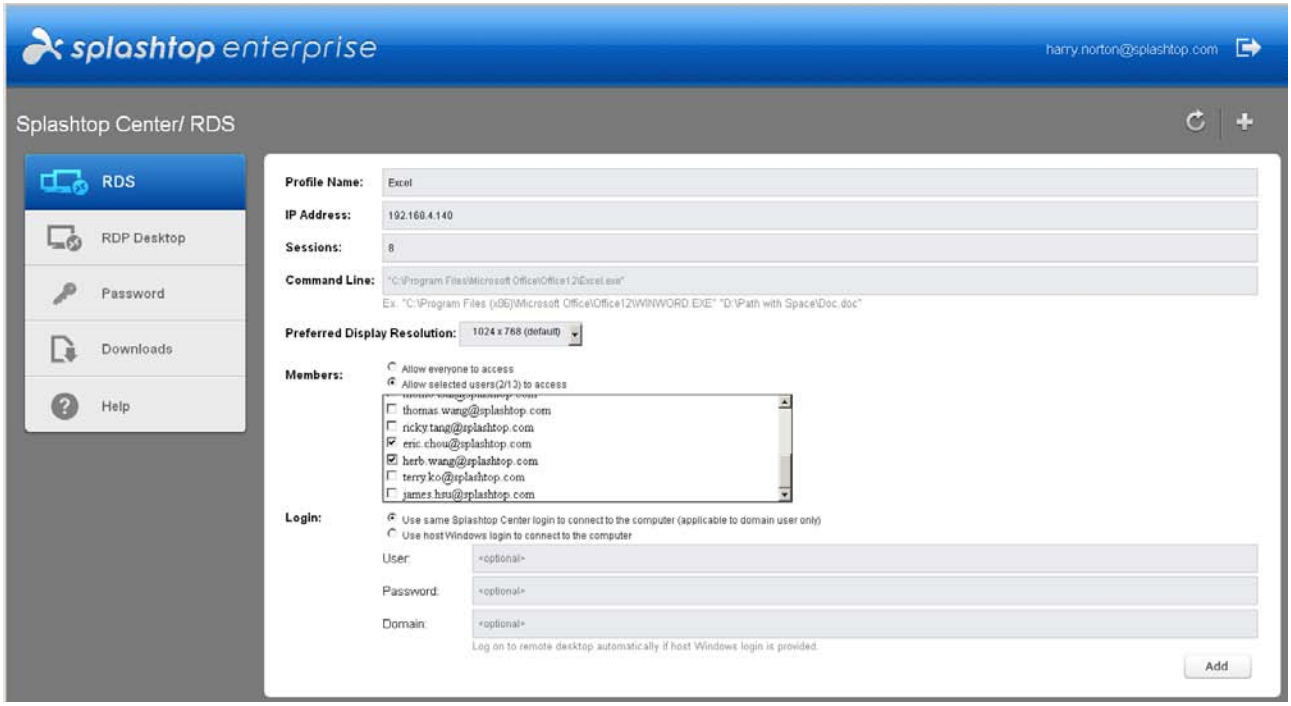
These two new items are shown with a blue dot in the **Status** column,meaning they are ready for connection. There is also an indicator at the bottom of the screen, "**Online computers: 2**."

5.5.1. Adding a Remote App

In the previous example, we added a Virtual Desktop. You can also use the **RDS** tab to add a remote application. As mentioned earlier, this means users would be able to launch that particular application remotely, without needing to access the entire PC remotely (on which the application resides) just in order to get to the application. You can choose which users will be allowed to use the application.

Click the  button to **Add** a Remote App to the list. The *Add* dialog will then open. All the fields shown in the *Add* dialog were explained on the preceding pages. The key difference is the **Command Line** field, where you must add the path where the target application resides on this remote computer.

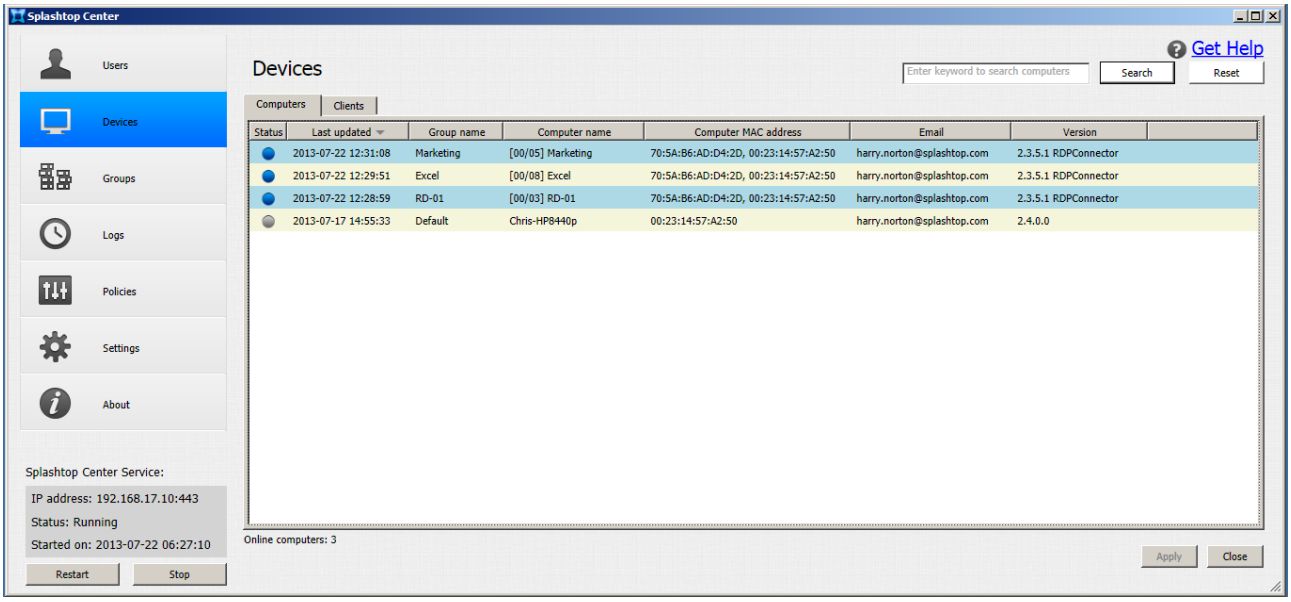
In the example below, the application we are adding is Microsoft® Excel®.



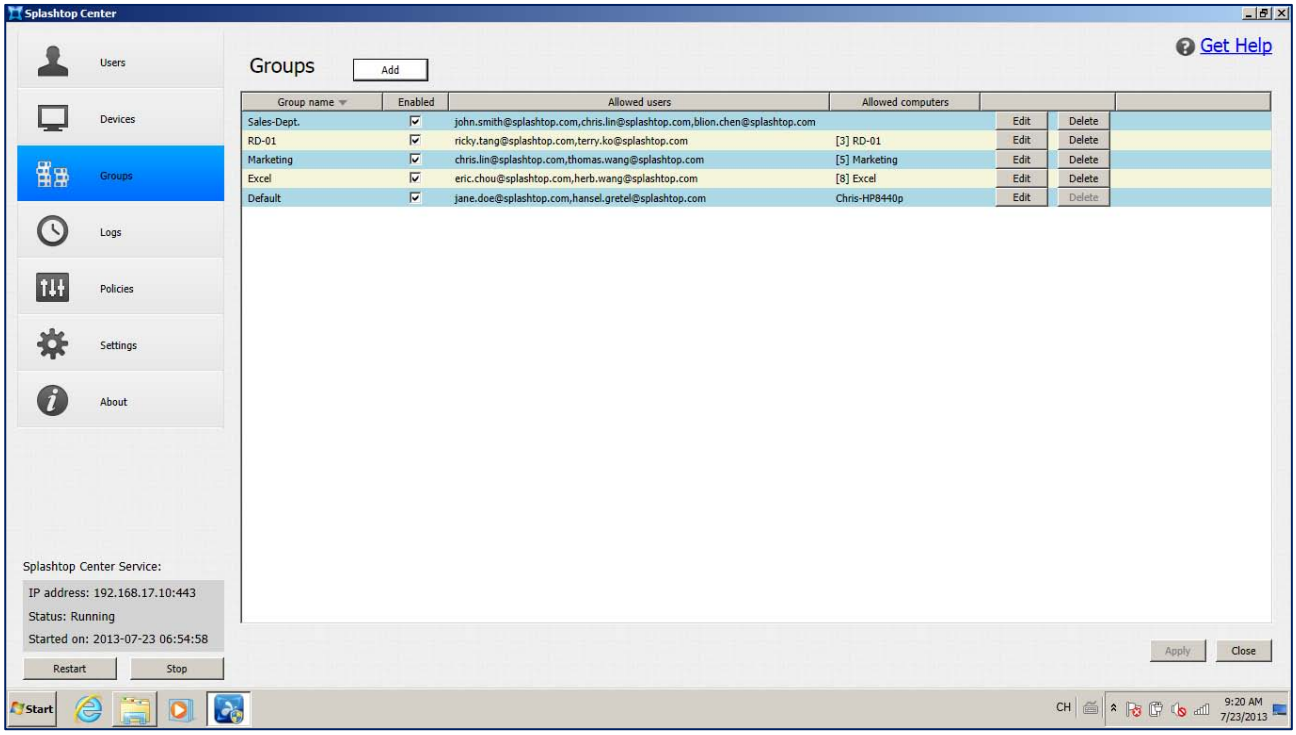
Click the **Add** button above to add this item.

After clicking **Add**, you will be returned to the list of added items within the main **RDS** tab. The illustration below shows that it has been added as the third item. Note that the **Type** column displays "**Remote App**."

In addition, it is now listed in the **Devices / Computers** tab of Splashtop Center, in the same manner in which our Virtual Desktops are listed. In the illustration below, it is the second item listed in the **Devices / Computers** tab. When adding this remote app, we specified "**Excel**" as the *Profile Name*, which becomes the *Group Name* in the **Devices / Computers** tab.



Likewise, the three items we have just added via **RDS** in the Web Portal (two Virtual Desktops and one Remote App) are listed in the **Groups** tab, as shown below. In the **Allowed Computers** column, the name is preceded by the number of Sessions allowed which we specified at the time of creating the Virtual Desktop/RemoteApp.



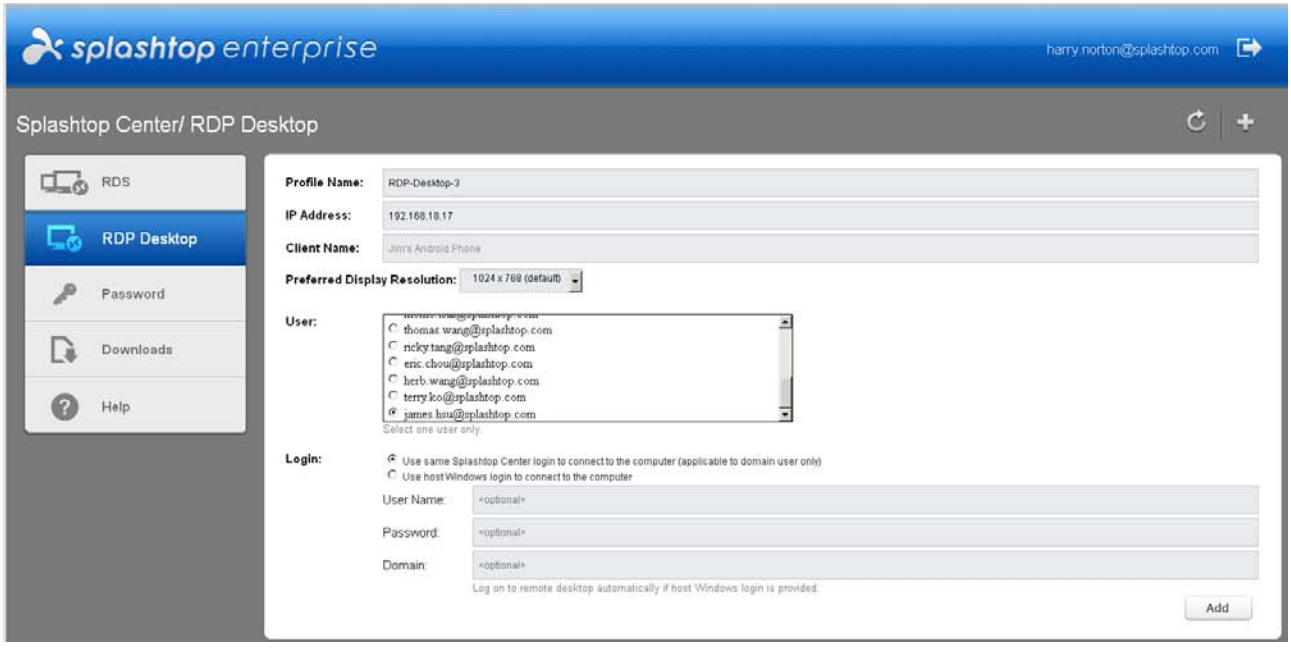
5.6. RDP Desktop tab

As with the **RDS** tab, the **RDP Desktop** tab will be displayed and available only if you have our SplashApp/**RDP Connector** option. Again, this tab will only be available if you are logged in to the Web Portal with the Administrator account.

Unlike **RDS** (wherein a server is hosting simultaneous remote sessions for multiple users), the function of **RDP Desktop** is to allow one user to remotely access the desktop of a host PC via RDP (Remote Desktop Protocol).

Basically, just enable RDP on a Windows-based host computer, then configure your RDP settings here in the **RDP Desktop** tab of your Splashtop Center Web Portal, and then simply connect to the RDP host computer.

When first opened, this tab displays the message "List Empty." Click the  button (near the upper right of the screen) to **Add** a computer to the list. The *Add* dialog will open. In the illustration below, we have already entered some sample data.



Profile Name

This is the name which is defined by the IT Administrator, displayed in the Client Profile list page, and is mainly for easy identification of their RDP computers.

IP Address

This is the IP Address of the RDP host machine.

Client Name

This field is optional. It is the name of the Client computer as defined and associated with the Windows Operating System. If left blank, it will not affect your attempts to make a remote connection.

Preferred Display Resolution

This option allows you to set the desired resolution of display from the RDP host. When connecting from the Splashtop Enterprise client app using the "Computer native resolution" selection, RDP Connector will use this resolution setting for connection. Currently, RDP Connector supports the following resolutions, which you can select from the drop-down list:

1920 x 1080
1440 x 960
1366 x 768
1280 x 1024
1280 x 768
1280 x 720
1024 x 768 (default)
800 x 600
640 x 480

User

This is the same User Name used for the Windows login on the RDP host machine. Select only one User Name from the list.

Use same Splashtop Center login to connect to the computer

This setting applies only to Domain (Active Directory) users. If this button is selected, RDP Connector will attempt to use the same Splashtop Center login credentials as the Windows account to log into the RDP Host to connect to the remote desktop or remote applications. Users will still need to enter the Splashtop Center password in the Windows logon page of the RDS server at the time of establishing connection.

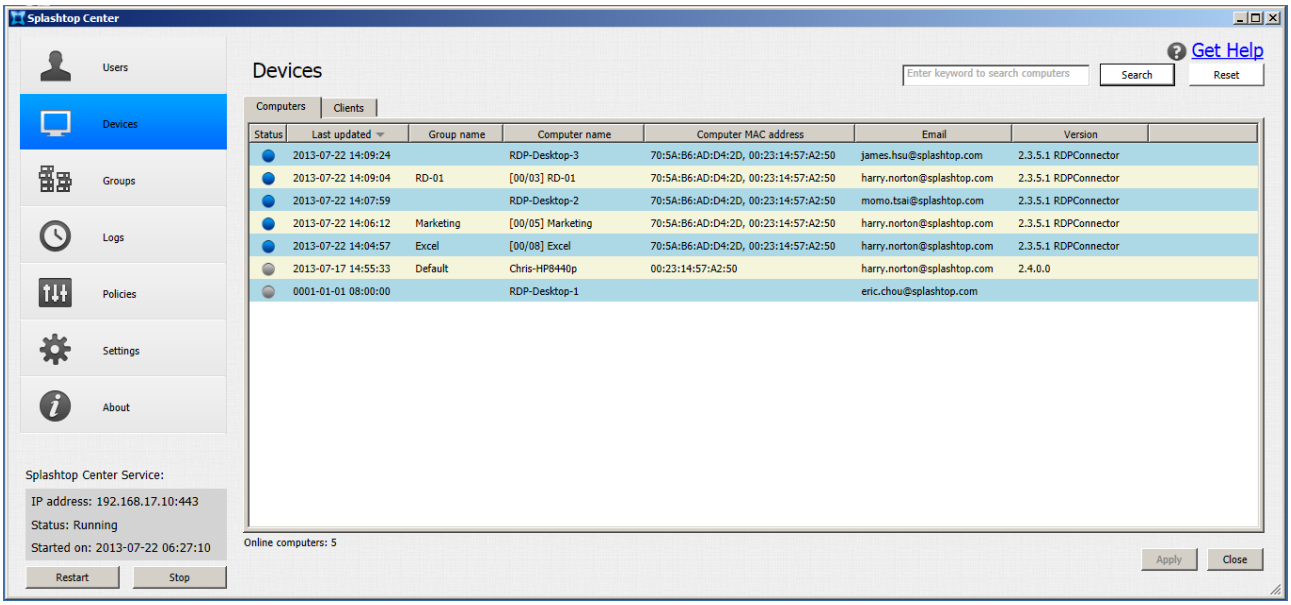
Use host Windows login to connect to the computer

This setting applies to both Domain and Gateway users. If this button is selected, users will use the Windows account from the RDS server for connection. The User, Password, and Domain fields will be available. If the Windows account **is** configured, users will be able to log in to the remote desktop/remote application automatically, without seeing the Windows login screen of the RDS server at the time of establishing a connection. If this informaton is **not** entered, the user will need to manually enter the login credentials into the Windows login screen, and the login will have to be provided separately by the IT Administrator to the users.

The example below shows three RDP computers that have been set up, and these will also be shown in your Splashtop Center console (see next page).

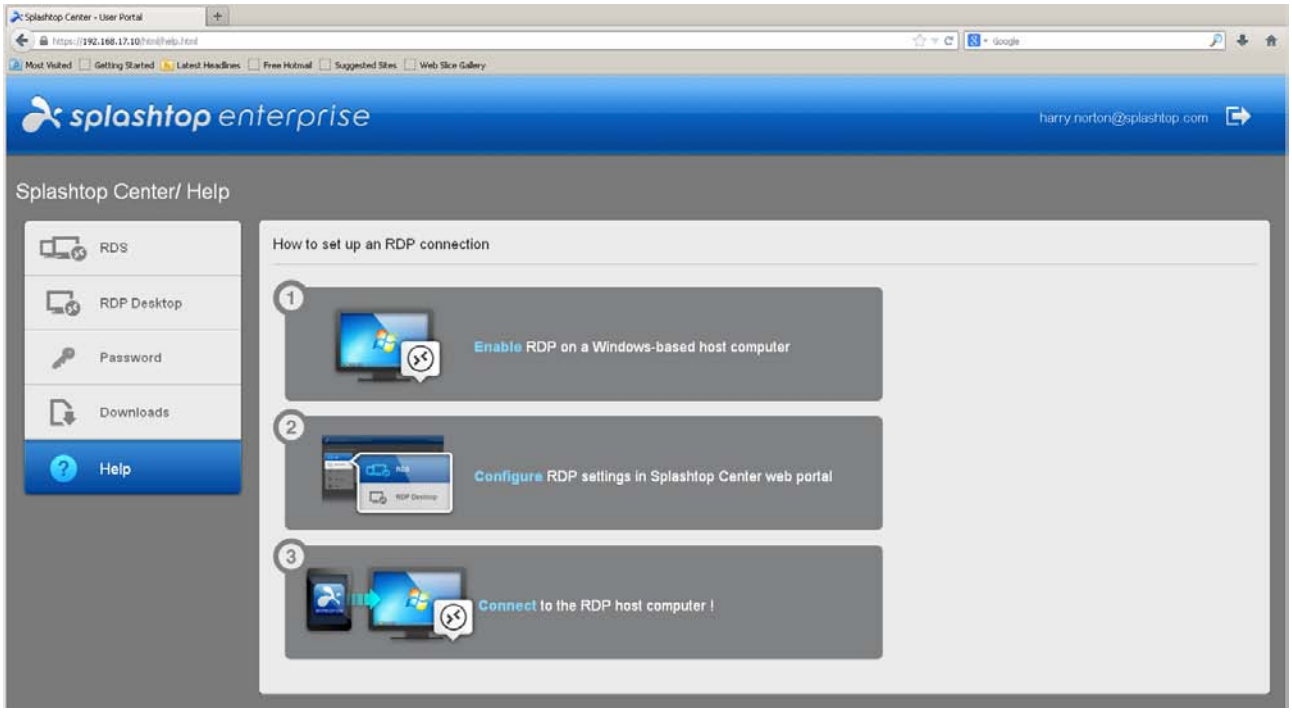
After an item has been added, you can view (and modify) the details by clicking the **Edit** button ( ), or click the associated button to **Delete** a computer from the list.

After **RDP Desktop** computers have been added via the Web Portal, the **Devices** tab of the Splashtop Center Console will list them (in the **Computers** sub-tab of **Devices**). The three computers (**RDP-Desktop-1**, **RDP-Desktop-2**, and **RDP-Desktop-3**) which were shown as having been added in the illustration on the previous page are now also listed below in Splashtop Center.



5.7. Help tab

Clicking on the **Help** tab will display the diagram shown below, which provides an easy to understand Step 1-2-3, for setting up an RDP connection.



6. Common Tasks

6.1. Changing Ports

By default, Splashtop Center will use Port **443**. However, you can configure Splashtop Center to use a different port if another application is already using this port.

If another application is not using this port, we recommend *not* changing the default port number of 443. This is because, if you change it, you will also need to update all the Clients and Streamers to the new Port number you chose, so they will continue to function as intended.

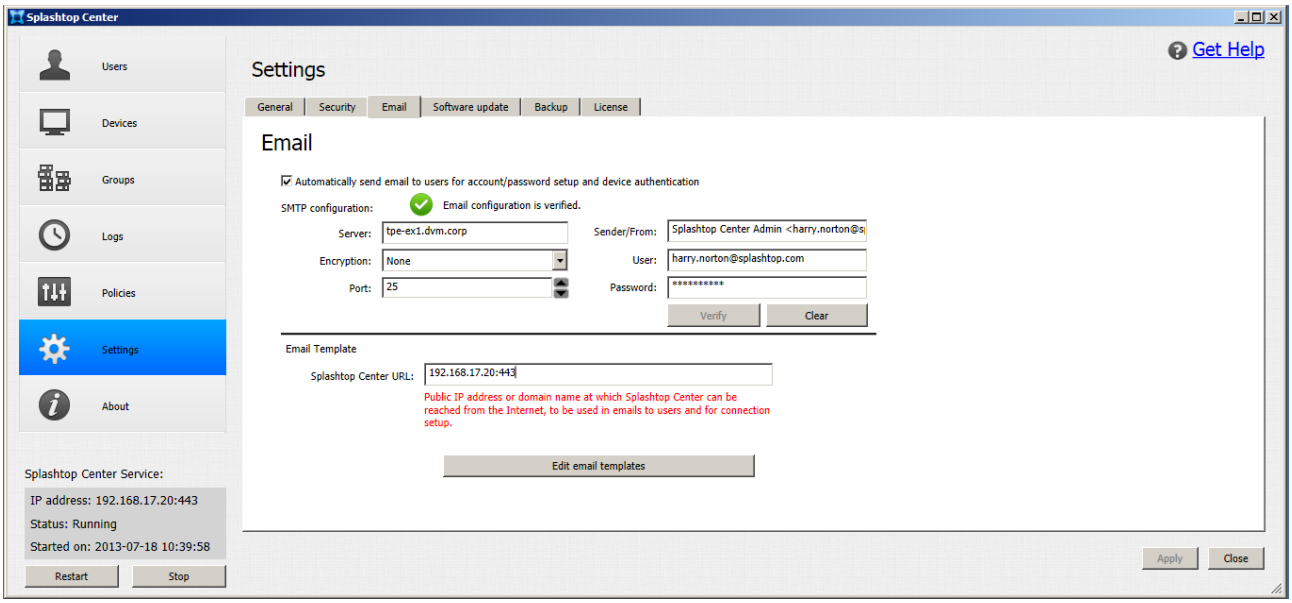
If necessary, you can assign any network port you want. To change the port number:

1. Launch the Splashtop Center application.
2. Go to the **General** tab in **Settings**.
3. Change the network **Port** number.
4. Click **Apply** to restart the Splashtop Center service and make the change take effect.

The port that Splashtop Center uses does not affect the security of the connections. If you have external firewalls, which provide additional security for certain ports, then the security of the connection may be affected outside of the Splashtop Center settings.

If you change the port number, you must modify the URL in the **Splashtop Center** field of the **Status** tab in the Streamer dialog box to include the correct port number.

In addition, the Splashtop Center URL is included in the **Email** tab of **Settings**. As shown in the illustration below, the message in red reminds you to keep the **Splashtop Center URL** field up-to-date.



NOTE: IT administrators *can* set Splashtop Center to use port 80. However, it will still use **https** — *not* **http**. Splashtop Center does not support the unsecure **http** protocol.
Therefore, we recommend that you do not use port 80, as this may have conflicts with other web servers using http on port 80 in the system.

6.2. Re-installing Splashtop Center

If someday you find it necessary to re-install Splashtop Center (for example, you rebuild your host OS), follow these simple steps:

1. We recommend that you first use the **Save all settings to file** button in the **Backup** tab of **Settings** (shown in section 4.6.5) which opens a dialog box that lets you save all your Splashtop Center settings to an XML file.
2. Re-install Splashtop Center on the *same* host machine. (When you re-install, your current Splashtop Center will be automatically un-installed.)
3. Open the **License** tab in **Settings** and re-enter your license key (in the same way you entered it the first time you installed Splashtop Center).
4. After re-installing, use the **Restore all settings from file** button to restore your settings from the XML backup file.

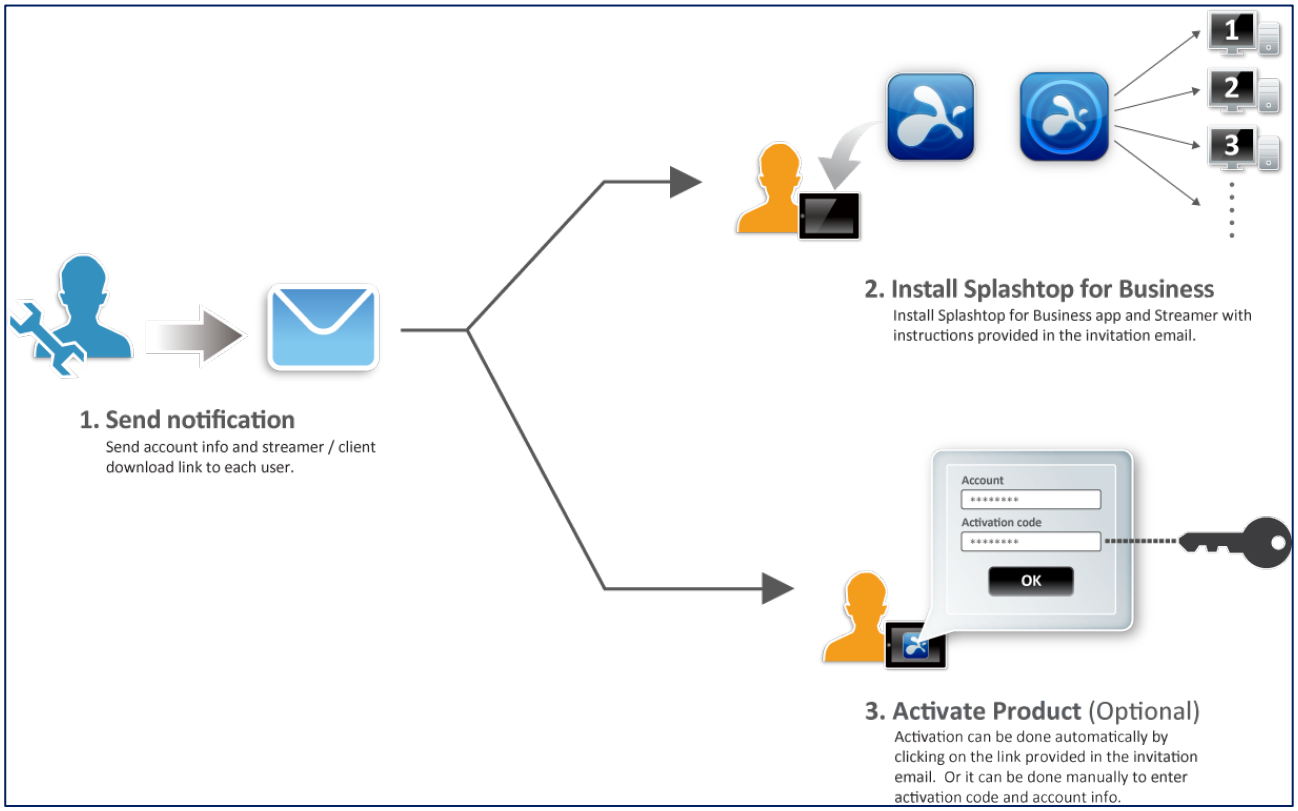
Each license key is good for up to five (5) activations. The activation count is determined by the number of successful activations performed. If you need more than five activations, you will need to contact a Splashtop representative to acquire a new license. And, before activating the new license, you must release the old license. As mentioned earlier in section 4.8.6, you can do this by clicking the **Release License** button in the **License** tab of **Settings**.

NOTE: The initial license activation is only valid in conjunction with the one, original hardware on which Splashtop Center was installed. The license key cannot be migrated to a different server. Each license key can only be used on the *same* host machine. Therefore, you will receive an error message that says "Hardware changed" if you are trying to activate the same license key either:

- on a *different* host machine, or,
- on the same host machine *but* with some hardware peripherals disabled or replaced.

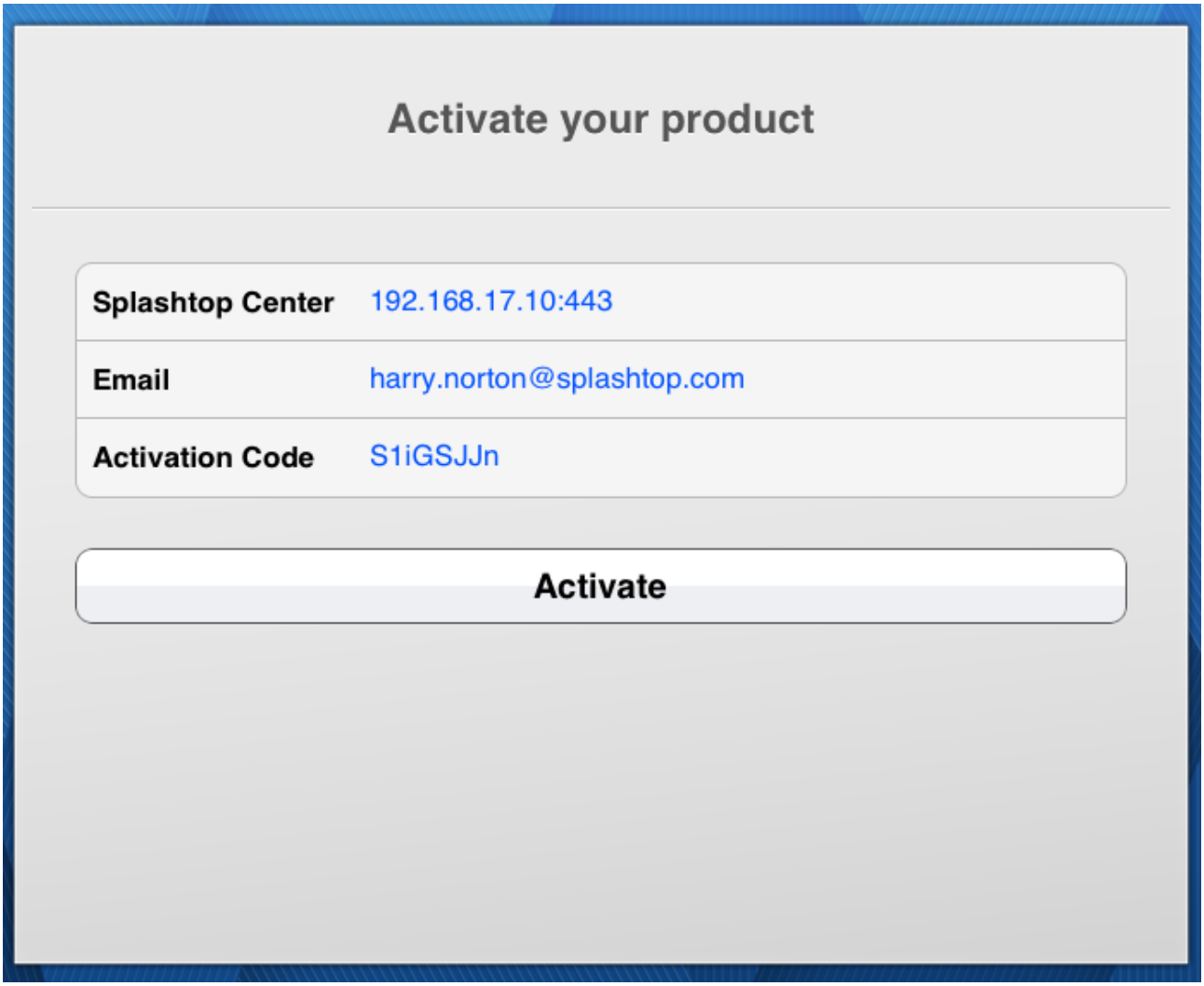
6.3. Activating a Mobile Device

As explained earlier in section 4.8.3, users will normally receive "Invitation Email," and can conveniently activate their mobile device just by clicking on the link provided in that Email.



However, in the case that it is necessary to activate a device manually, follow the steps below, which use the iPad client as an example:

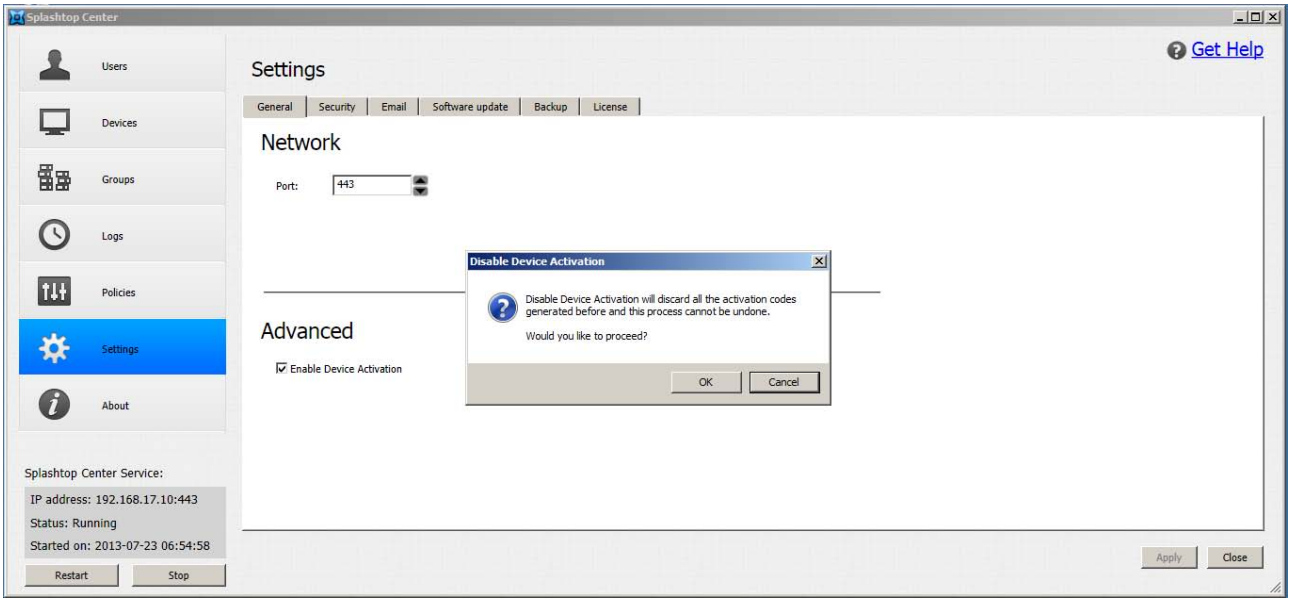
1. Launch the Splashtop Enterprise app on the mobile device.
2. Tap the **Activate this product** link on the **Enter your account** login page.
3. In the **Activate your product** screen shown below, enter the **Splashtop Center URL**, **Email** address, and **Activation Code**.
4. Tap the **Activate** button to activate this device.



NOTE: If a device has already been activated for use, but for any reason you want to deactivate it, click the **Deactivate** button in the Clients tab of Devices to immediately block the related device for use with Splashtop Enterprise. You can deactivate permanently (such as due to employee terminated), or temporarily (such as when a device is lost/stolen and then recovered). The **Deactivate** button is shown to the right of each item listed in Clients of the Devices tab, as illustrated in **section 4.3.2, Clients**.

6.4. Re-issuing Device Activation and Authentication Codes

If the **Enable Device Activation** option is enabled (checked) in the **Settings/General** tab as shown below, then the IT Administrator can add and issue more device activation codes by clicking the **Edit** button for a particular user in the **User** tab.



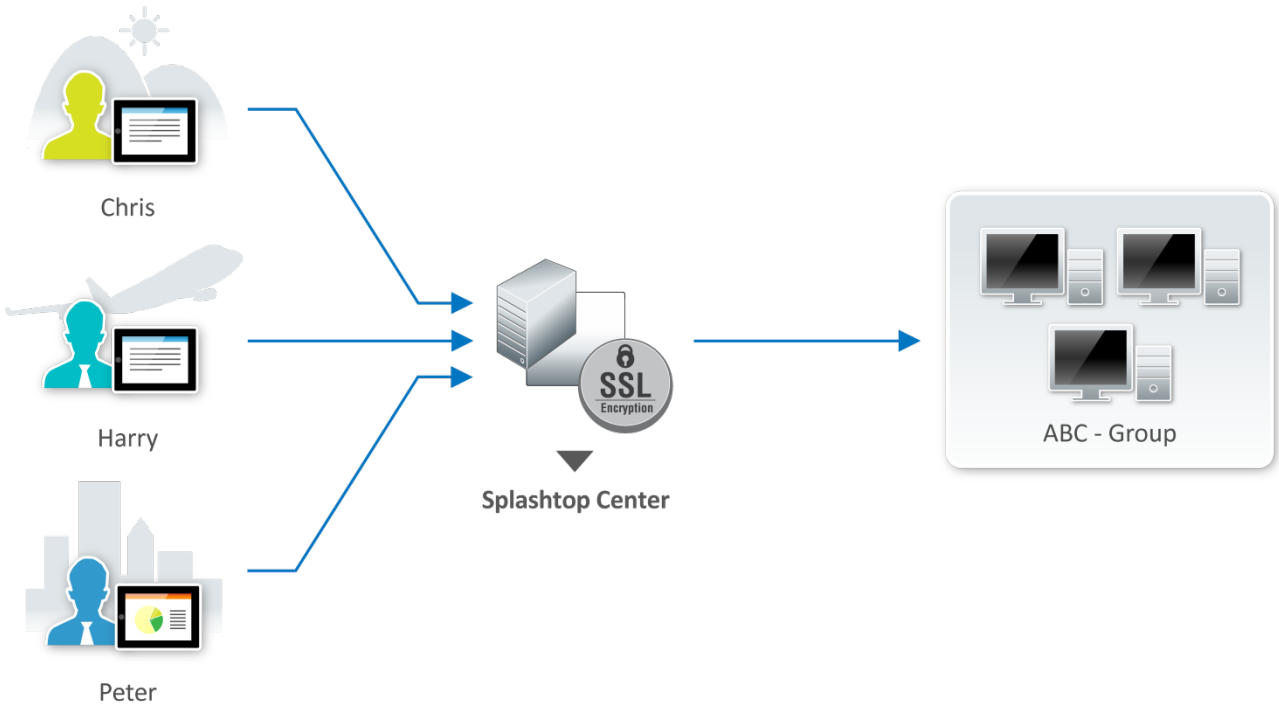
If you disable (un-check) the **Enable Device Activation** option, then there is no need to re-issue device activation codes. This process cannot be undone, so a warning message will require you to confirm, as shown in the example above.

⚠ CAUTION: Un-checking the **Enable Device Activation** checkbox will discard all the activation codes that were generated previously!

6.5. Creating and Administrating Groups

If you have not yet created the users you will want to add to a group, you need to do that first. Also, the Windows computer(s) in the office (on which you want to install the Splashtop Streamer) must be running either Windows 7, Windows XP, Windows Vista, or Windows Server 2008 R2.

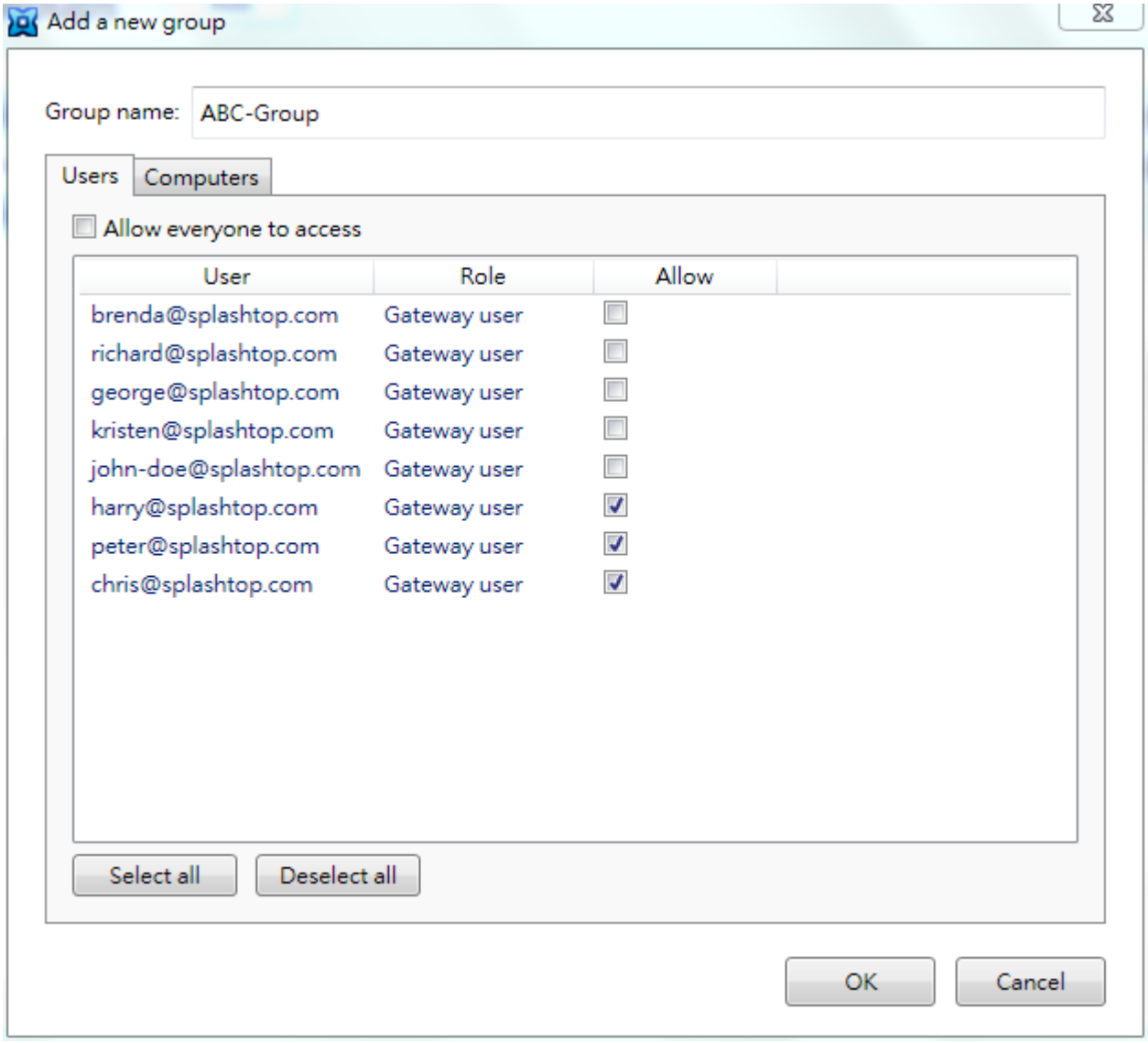
In this example, we will create a group consisting of three iPad users who are *out* of the office, but will be able to share remote access to three computers *in* their office, via Splashtop Enterprise. As shown at the left side of the illustration below, the first employee ("Chris") is on vacation in the mountains; the second one ("Harry") is flying to another country on business; and a third employee ("Peter") is just roaming around in the city, outside the office.



The IT Administrator will need to do the following in order to enable these employees to use Splashtop Enterprise to remotely access computers in their office:

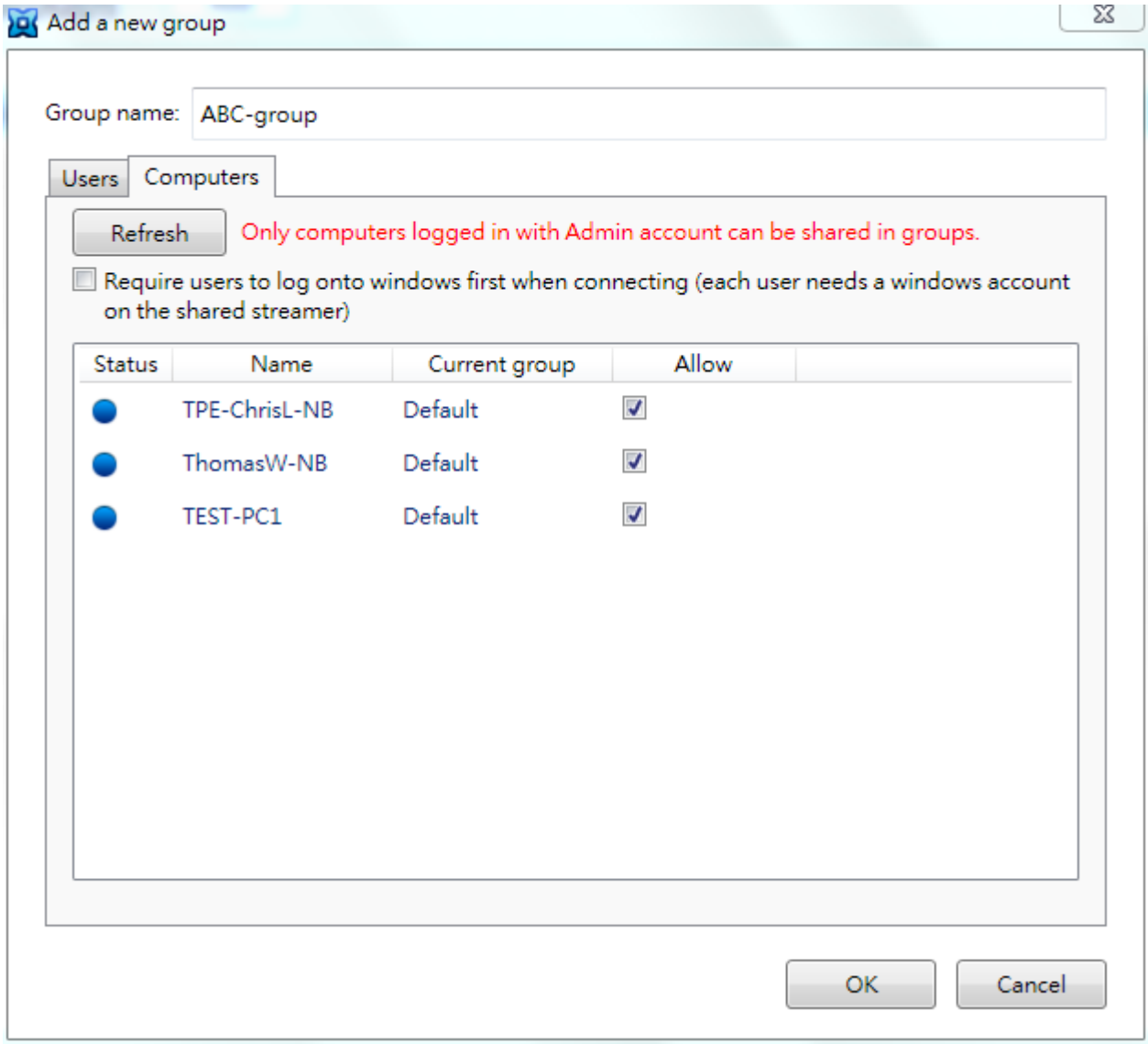
1. On the remote Windows computer: Create users on the Windows OS (if not yet created).
2. On the remote Windows computer: Install Splashtop Streamer and then log in to Splashtop Center using the Splashtop Center Administrator's account on the Streamer.
3. Splashtop Center: Create the users on Splashtop Center in the **Users** tab as explained earlier in section 4.1.

4. Splashtop Center: In the **Groups** tab of the Splashtop Center Console window, click the **Add** button. The **Add a new group** window will open. All users who have been previously added to Splashtop Center will be listed, as shown in the example below.
5. In the **Add a new group** dialog box, enter the desired name for the new group in the **Group name** field. We entered "ABC-Group" below.



6. In the **Users** tab shown above, select the users you want to be included in the new group by checking the corresponding checkboxes in the **Allow** column. We have selected three checkboxes for purposes of this example.

7. Click **Computers** to open the Computers tab. In this tab, you must select the computers you want the authorized users to be able to access remotely. In the example below, we have selected all three computers in the list in the same way — by checking the **Allow** checkbox. This means all users in the group will be able to connect to these computers using the Splashtop Enterprise app on their mobile client devices. However, please be reminded that Splashtop Enterprise users cannot choose a specific computer to connect to remotely. When a user in the group attempts to make a remote connection, a connection will be made to any of these computers in the group that might be currently available.



8. The "**Require users to log onto Windows first when connecting**" option is disabled by default, as shown in the example above. If you check the checkbox to enable this option, then each user in the group would need a Windows account on the computer hosting the shared Streamer, because these users would be forced to log in to Windows whenever they want to make a remote connection. After the session is disconnected, the user will automatically be logged out of Windows.

NOTE: In addition, please note that if there is already one Windows user (on the Windows OS computer with this group-shared Streamer), and then another user logs in to this same shared computer, only the first one to log into it will have control of the Streamer OOBE and its settings. Other users will inherit the first user's Streamer settings and will not have the Streamer OOBE available to them.

9. Click **OK** in the **Add a new group** dialog box. You will be returned to the main **Groups** tab, and now you can see the new **ABC-group** listed.

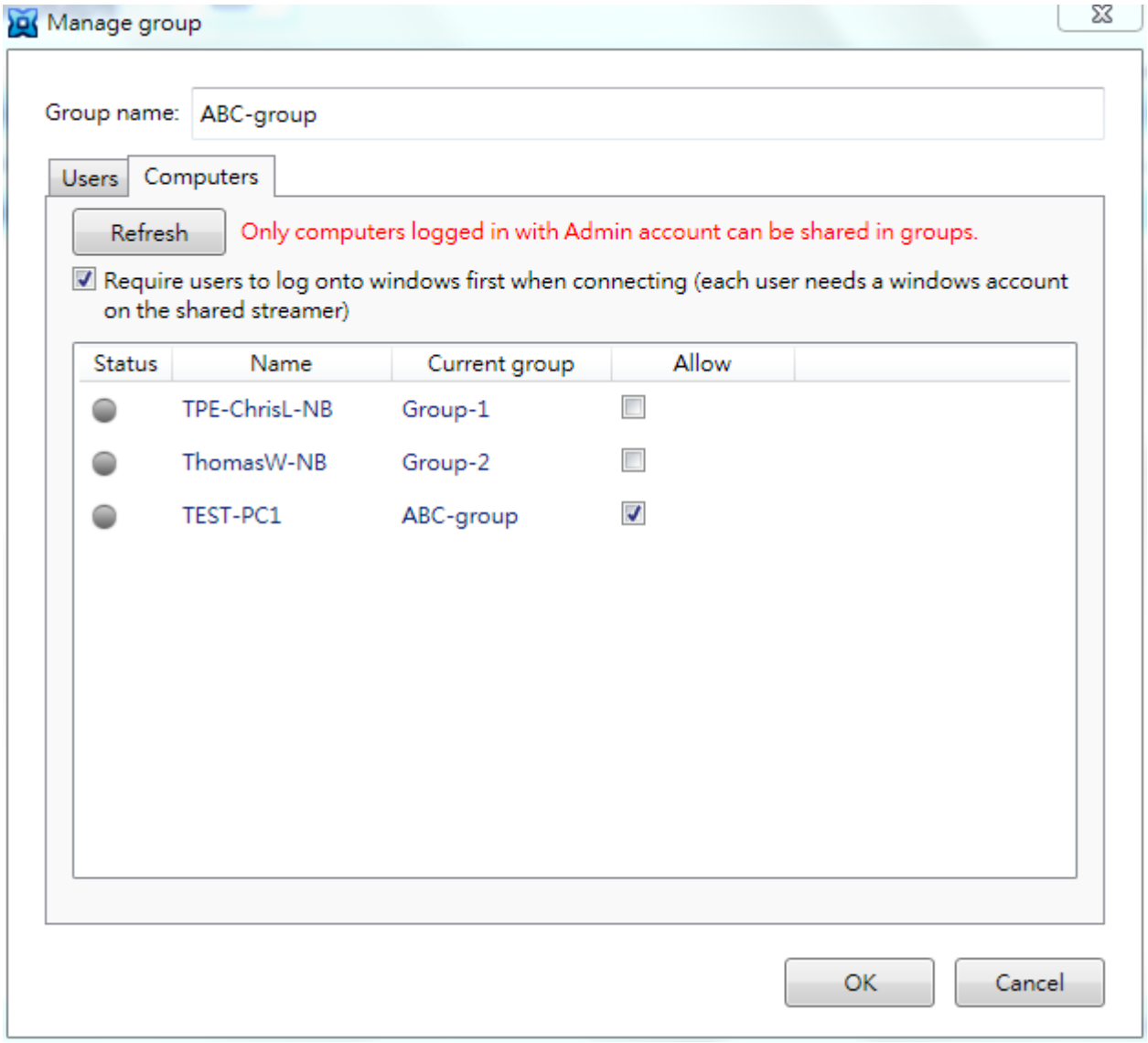
6.5.1. Deleting a Group

To remove a group from Splashtop Center, simply click the **Delete** button in the **Groups** tab, at the far right of that group's information. (Removing a group does not delete any users or computers that were in the group; just the group name itself.)

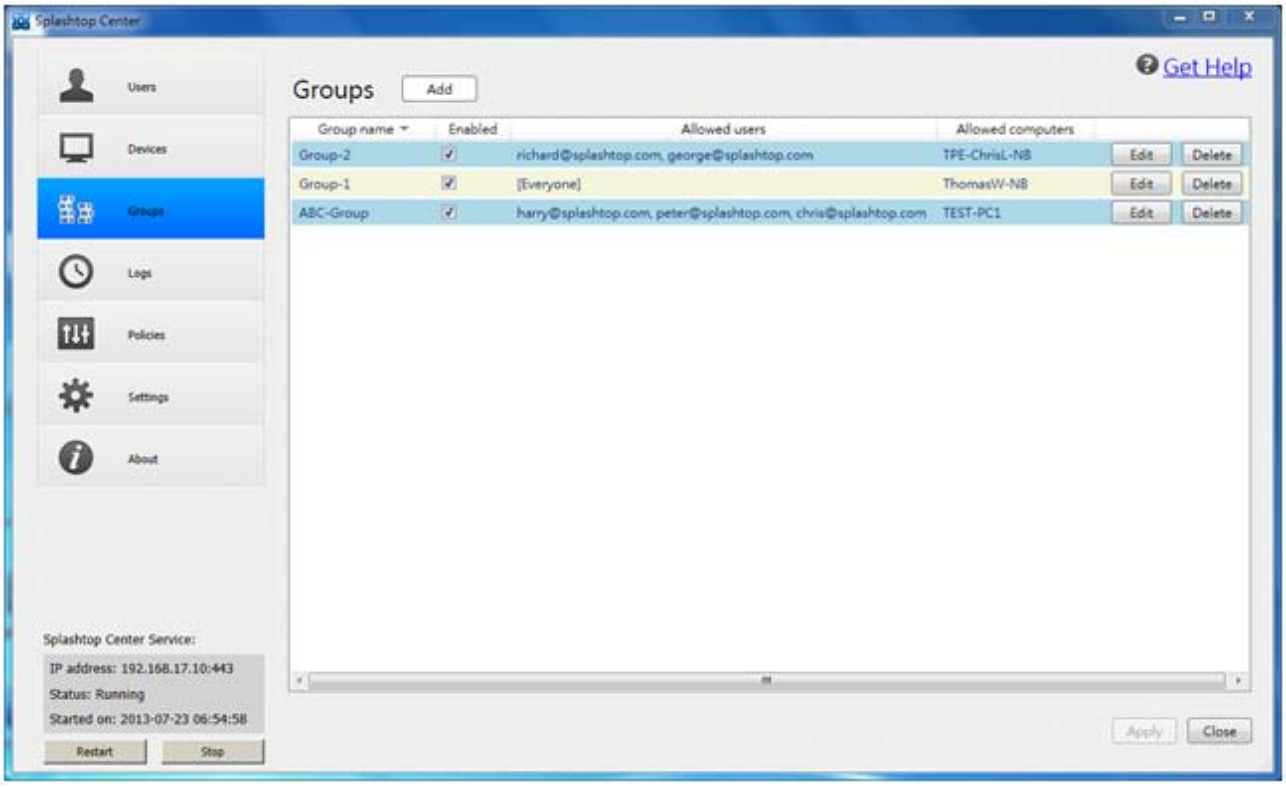
6.5.2. Modifying a Group

If you want to make changes to your original designations for a particular group, click the **Edit** button for that group. The **Manage Group** dialog box will open. You can change the group name, the allowed/disallowed status for users, the allowed/disallowed status for computers, and the enabled/disabled status for the "Require users to log onto Windows first when connecting" checkbox.

For purposes of this example, in the **Manage Group** dialog box shown below, we have changed our original designation in the **Computers** tab to allow only one of these computers ("TEST-PC1") to be accessed by the ABC-Group.



After clicking **OK** in the **Manage Group** dialog box above, the **Groups** tab now shows that **ABC-Group** includes three users, and they will share access to one computer named **TEST-PC1**.



Please also see **section 4.3** entitled **The Groups Tab**.

6.6. How to perform Wake-on-LAN with Splashtop Enterprise

Splashtop Enterprise provides a "Wake up this Computer" function to allow a user to wake up the target remote computer from a sleeping state so that he or she can connect to it. That is, Splashtop Center will wake up the Streamer on behalf of the mobile client device, provided the computer supports WoL (Wake on LAN) and the option has been enabled, and that the computer is connected by Ethernet, not WiFi.

Previous Splashtop Enterprise users might recall that Wake-on-LAN could only be used when the Streamers and Splashtop Center were on the same subnet (or when the nets were capable of forwarding magic packets). Due to customer demand, we are happy to say that we have enhanced this feature to be capable of waking up a computer even if it is on a different subnet. It can now handle these situations:

- The mobile client device (app) and the off-line Streamer (remote computer to be awakened) are both on the same subnet, OR
- The mobile client device and the off-line Streamer are on different subnets, but Splashtop Center and the off-line Streamer are on the same subnet, OR
- The mobile client device and the off-line Streamer are on different subnets, but there is at least one on-line Streamer on the same subnet as the off-line Streamer you want to awaken.

After you initiate a Wake-on-LAN request from your mobile device app, Splashtop Enterprise will automatically detect and take the necessary action according to which of the three topologies you have, and attempt to awaken the target computer.

First, we ask that you make sure the following conditions have been satisfied completely. Otherwise, there is no chance to make Wake-on-LAN work successfully. Please verify that the:

- Computer is connected by Ethernet, not WiFi. **This requires LAN and will *not* work with WiFi.**
- PC BIOS supports WoL and that the option has been enabled in both OS and BIOS of the computer with the off-line Streamer.
- Settings in Windows or Mac have been properly set up.

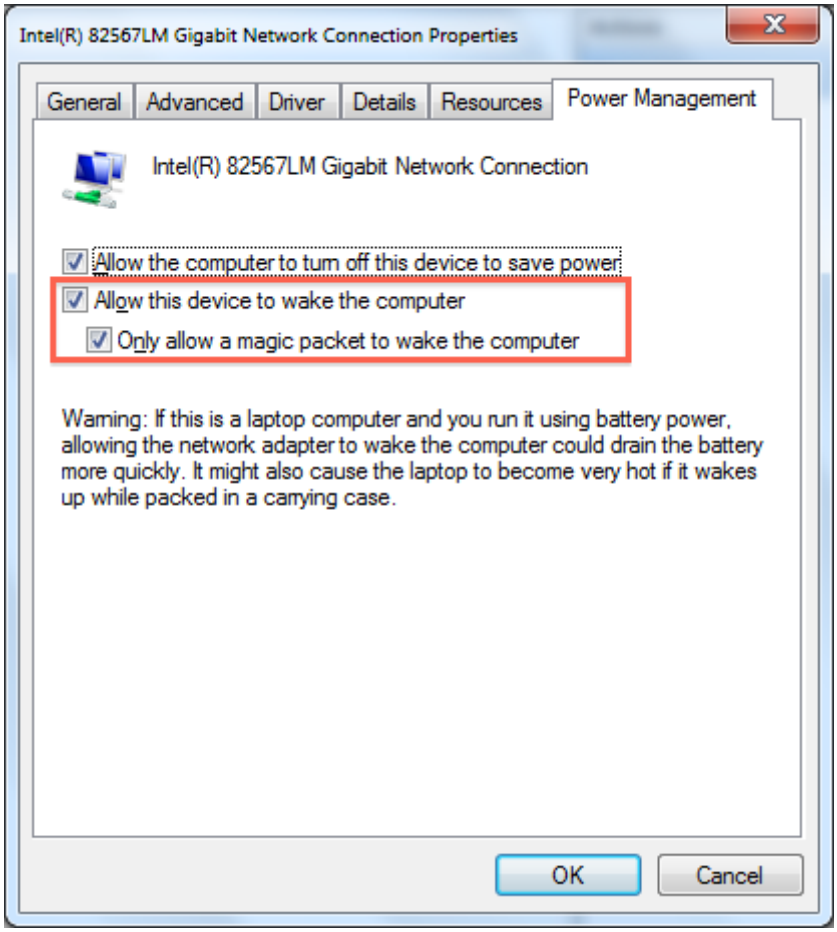
6.6.1. Settings on Streamers:

To connect to your computer when it is in Sleep or Hibernation mode, you need the following:

1. Make sure your BIOS supports Wake-on-LAN, and that this option has been enabled. (This step pertains to Windows PCs only; Mac users can ignore this.)
2. Configure your computer to be Wake-on-LAN ready. Please note that the term in BIOS might vary. For example, it might be "Wake on LAN," or "Onboard LAN Boot ROM," or something else.

For Windows users:

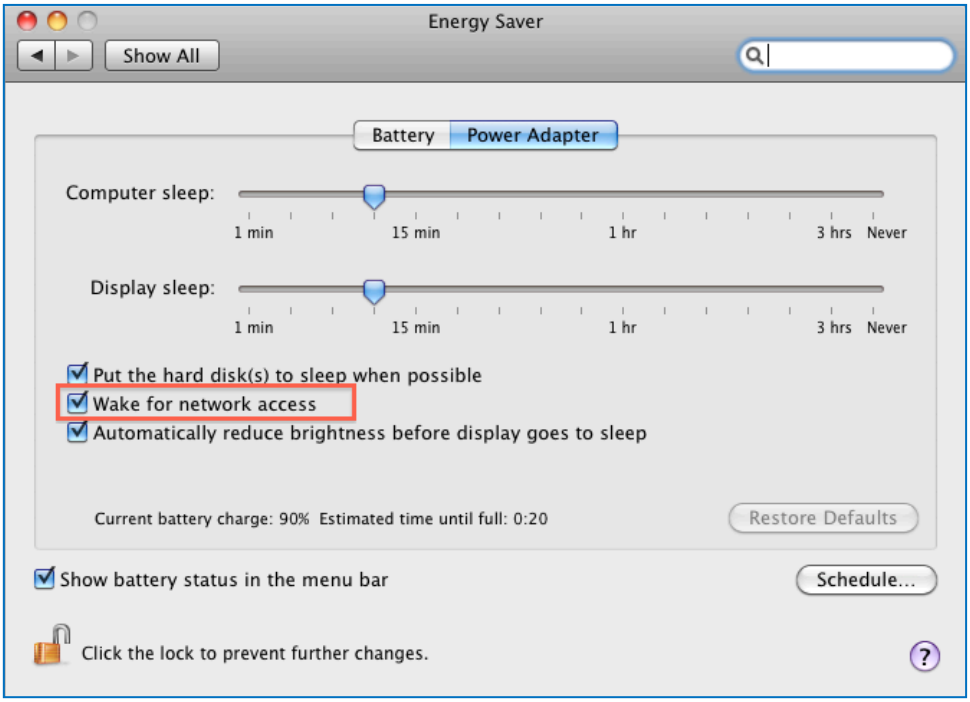
- Enable Wake-on-LAN in the system BIOS if you want to allow your computer to wake from a powered-off (i.e., Hibernate) state.
- Configure your LAN network interface adapter (*Control Panel -> Device Manager -> Network adapters*).



If the offline Streamer is a Notebook, please use AC electrical power (not battery power). Otherwise, the Notebook hardware will not allow Wake-on-LAN.

For Mac users:

- Make sure the **Wake for network access** option is selected in the *Energy Saver* settings.

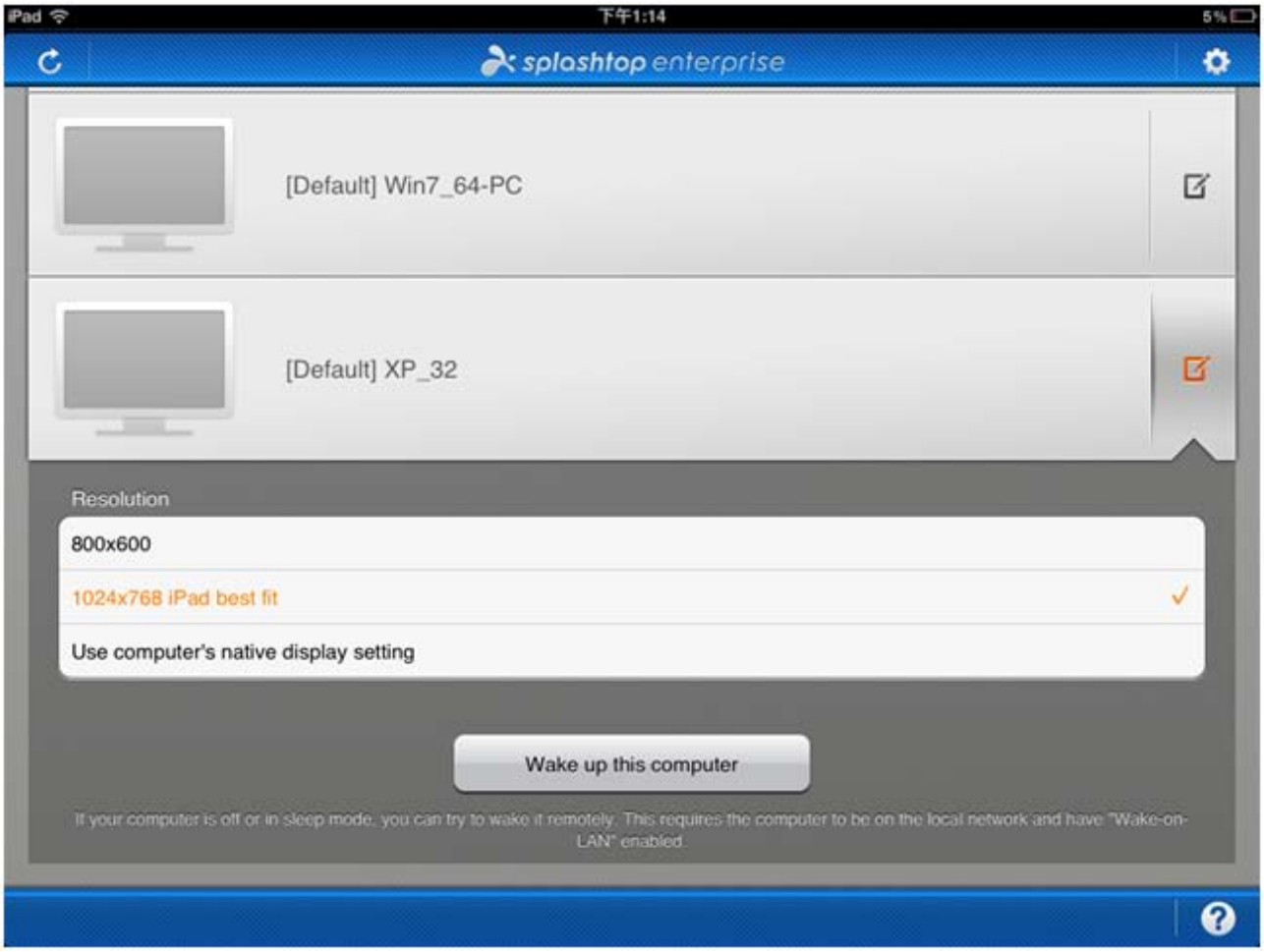


3. Your computer must be connected to your wireless router using the network cable (Ethernet).
4. If your Mac computer is a laptop (for example, a MacBook Pro or a MacBook Air). please make sure the power cable is plugged in to an electrical power source. If you are using only battery power on the laptop, this may cause the WoL feature to fail.

6.6.2. Steps to trigger Wake-on-Lan

Steps required to wake your computer from Sleep or Hibernation mode:

1. On your tablet/phone, launch the Splashtop Enterprise app. Turn **ON** the "Show offline computers" option in Settings.
2. Keep your computer **ON**, and make a successful connection, then shut down your computer (power-off).
3. From your tablet/phone, you should see the computer you want to awaken is an unavailable one (gray computer icon), like the ones shown in the sample illustration below.



4. Tap the "Edit" icon (at the far right of the desired computer name) as shown above. A **Wake up this computer** button will appear.
5. Tap on the **Wake up this computer** button to attempt to wake up the PC computer from either a **Powered-off, Sleep** or **Hibernation** state; or a Mac computer from a **Sleep** state.

6.6.3. Wake-on-LAN usage timing and limitations:

- **PC —** If your PC is in a **Sleep**, **Hibernate**, or **powered-off** state, Splashtop Enterprise can awaken it to a "waiting for login" screen via the "Wake-on-LAN" feature.

Type	Sleep	Hibernate	Powered off
XP	v	N/A	v
Vista	v	v	v
Win7	v	v	v
Win8	v	v	v

- **Mac —** Currently, if your Mac is in a **Sleep**, **Display sleep**, or **powered-off** state, Splashtop Enterprise can only awaken it to a "waiting for login" screen (via the "Wake-on-LAN" feature) when it is a Mac OS X 10.6.x and in **Sleep** mode (shown in the table below).

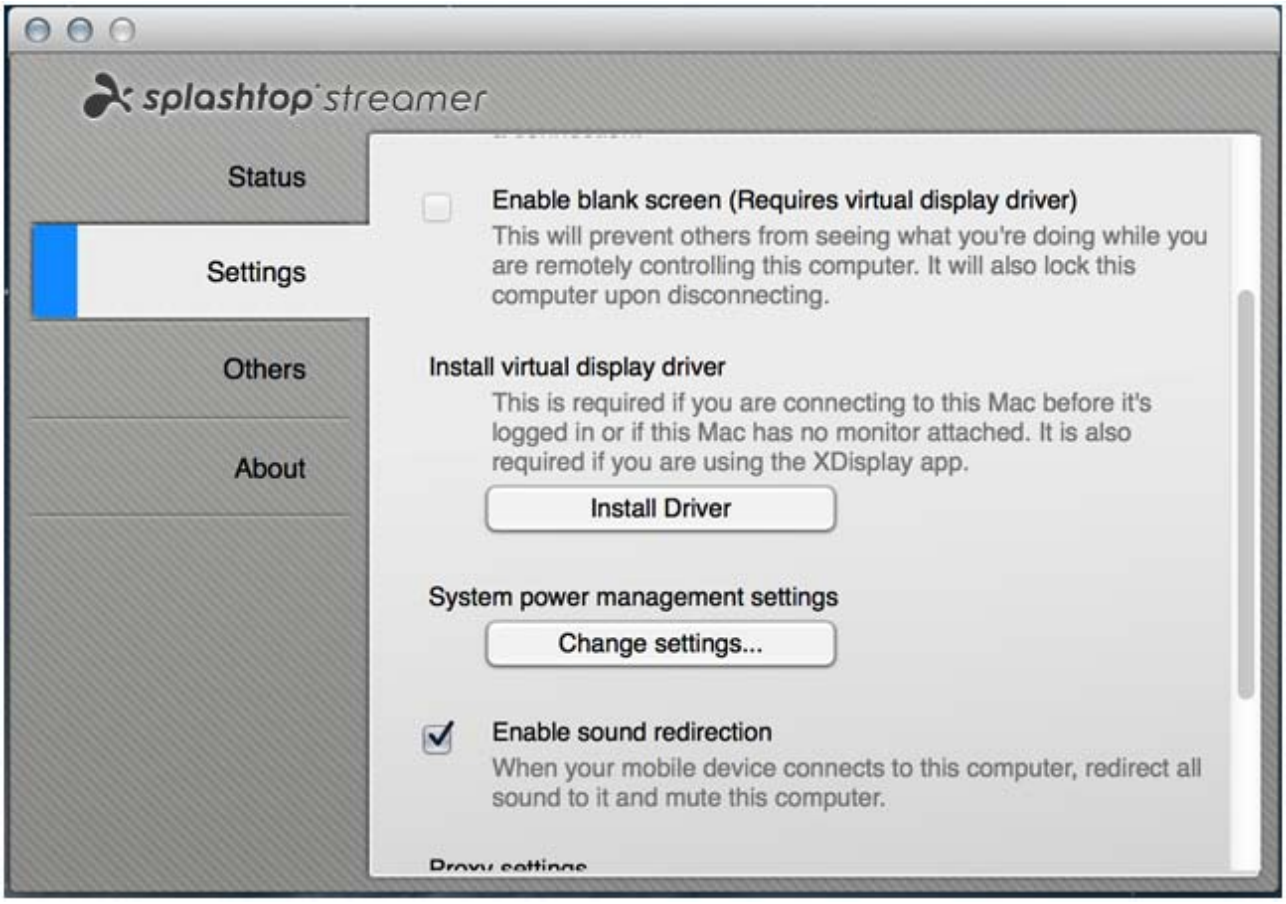
Type	Sleep	Display sleep	Powered off
OS X 10.6.x	v	v **	x
OS X 10.7.0	v*	v **	x
OS X 10.7.1	v*	v **	x
OS X 10.7.2	v*	v **	x
OS X 10.8.2	v*	v**	x

* A *Lion (or Mountain Lion)* computer could be awakened from **Sleep mode** to be in a **Low Power wake mode (=Dark Wake mode)**, and then connected to, by tapping the computer again in a Discovered Computer list. Please note that it is essential that the **Virtual Driver** be installed. This is very different from the *Snow Leopard* computer. (If the first screen displayed on the tablet is abnormal, just tap again. This is a known issue.)

** When your computer goes to **Display Sleep**, the following conditions will normally be necessary in order to awaken and connect your computer:

I. The computer listed on the tablet/phone should be in an "available" state (colorful), and can be directly tapped to connect to the Streamer.

II. Before awakening the computer from **Display Sleep** mode, install our Virtual Driver from the Mac Streamer / **Settings** tab / **Install Driver** button, shown below. In addition, don't use a resolution of 800 x 600. Instead, please use 1024 x 768 or Native resolution.



Please note that currently, it is *not* possible to awaken a **Mac** computer from a **powered-off** state via the WoL feature.

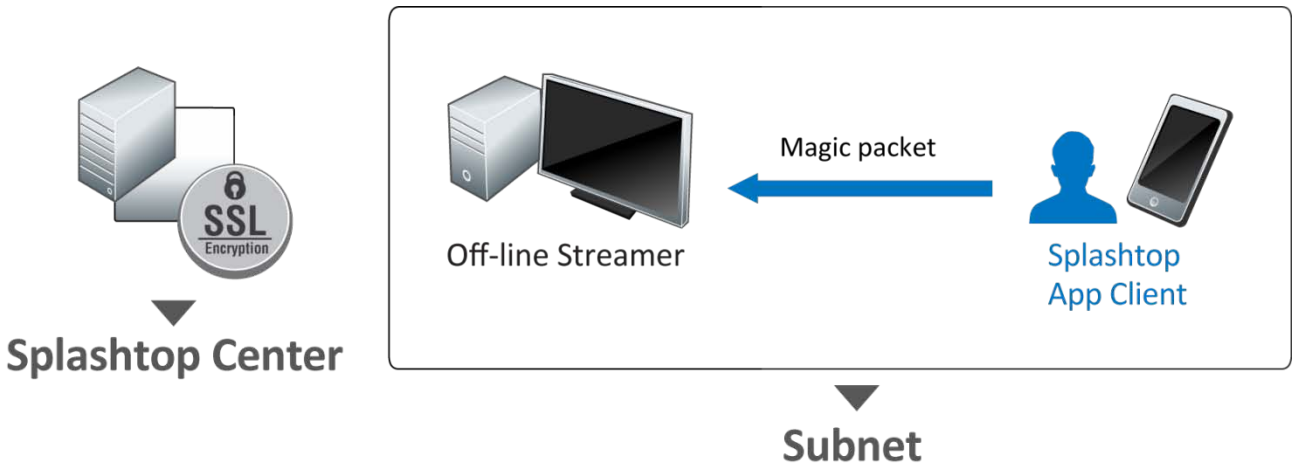
⚠ CAUTION: Wake-on-LAN might not work well when "**Force SSL over local connection**" is enabled. We recommend that you turn off this option to ensure more stable performance of Wake-on-LAN.

6.6.4. How it works in different topologies

As mentioned at the beginning of this section, we listened to our customer feedback and enhanced our **Wake up this computer** feature so that it can now adapt to various topologies — and even better news is that you don't need to do anything additional or different than you did in the previous version, when initiating the WoL request from your mobile device app. Splashtop Enterprise will take care of the additional detection/processing transparently. In this section, we provide some reference details about what goes on in the background in these three topologies.

The App Client and off-line Streamer are on the same subnet:

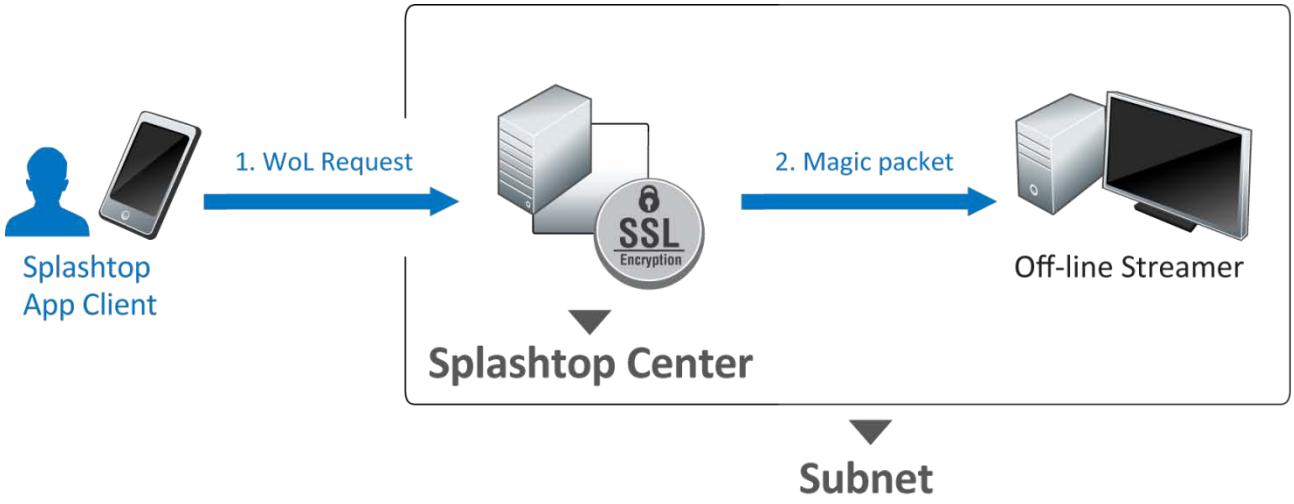
This is our original **Wake up this computer** functionality. In this topology, Wake-on-LAN is supported only if the mobile client device (App Client) and the off-line Streamer (remote computer to be awakened) are both on the same subnet. If your situation is like this, the App Client will broadcast a magic packet directly to its subnet to wake up the computer (Streamer), and then send a WoL request to Splashtop Center.



Wake-on-LAN network topology wherein the App Client and Streamer are on the same subnet

The App Client and off-line Streamer are on different subnets, but Splashtop Center and the off-line Streamer are on the same subnet:

Splashtop Center can now support this type of topology. The mobile client device(App Client) will send a WoL request (step 1 shown below) to Splashtop Center. Splashtop Center will then broadcast a magic packet to its subnet to wake up the off-line Streamer (step 2) and will forward the WoL request and MAC Address list to the Relay server. If the off-line computer is in Splashtop Center's subnet, the computer will be awakened.

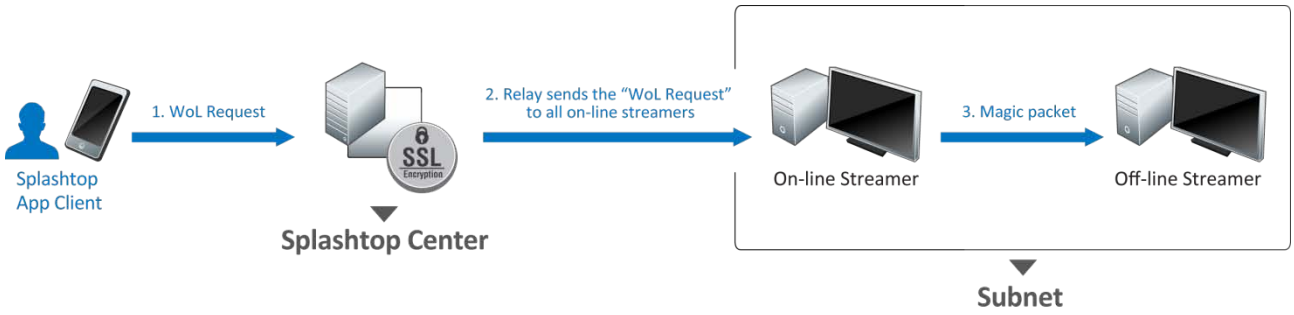


Wake-on-LAN network topology wherein App Client and Streamer are on different subnets, but Splashtop Center and Streamer are on the same subnet

App Client and off-line Streamer are on different subnets, but there is at least one on-line Streamer on the same subnet as the off-line Streamer you want to awaken:

In this situation, the mobile client device (App Client) sends a WoL request (step 1 below) to Splashtop Center. Splashtop Center forwards the request to its relay server. The relay then sends the WoL packet (step 2) to **all** on-line Streamers. All the Streamers that receive the packet will broadcast the magic packet (step 3) to their respective subnets to wake up the target off-line Streamer.

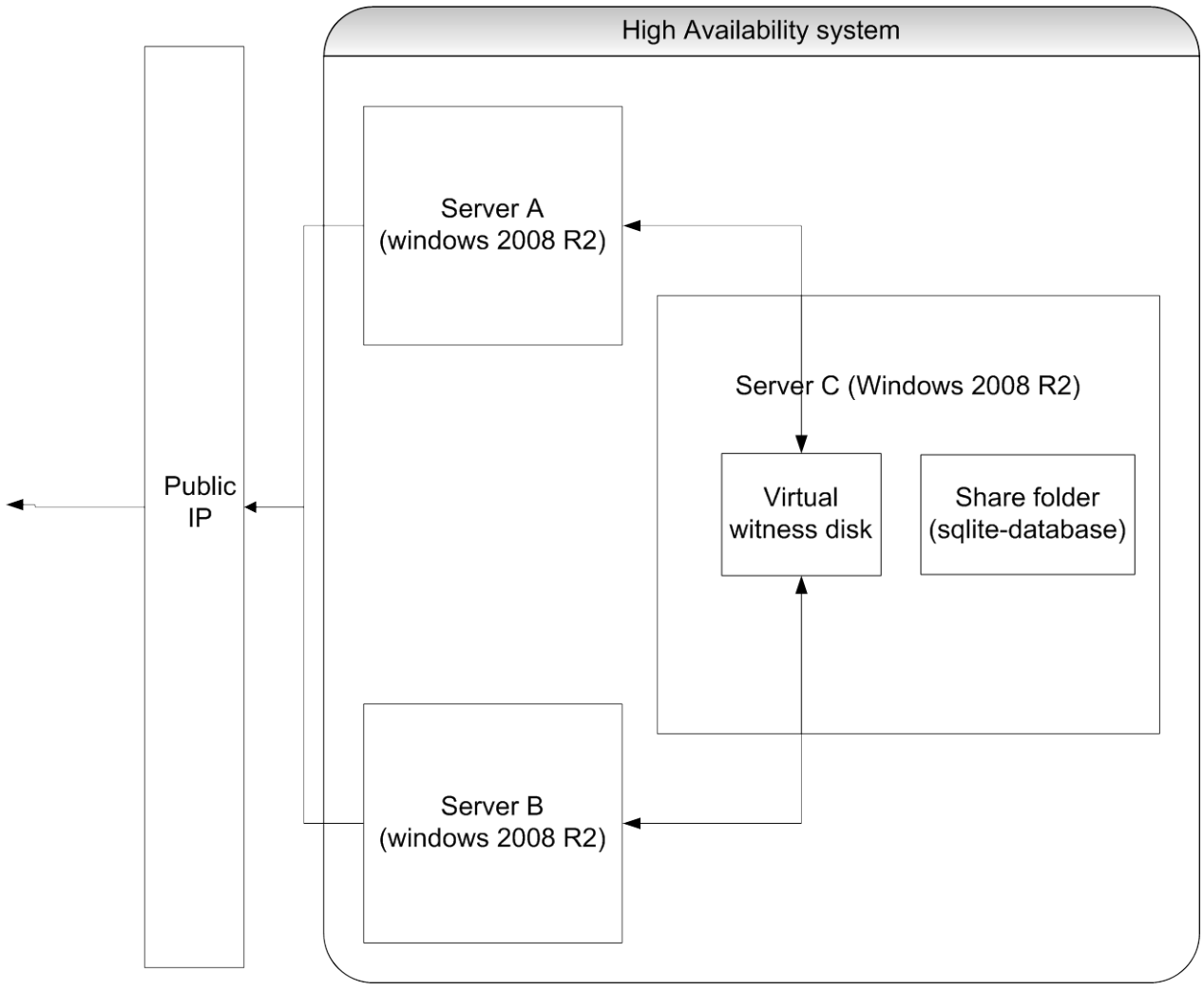
If an on-line Streamer is connecting to a mobile client device, the relay server will not send a WoL request to it. Currently, in order for this topology to wake up an off-line Streamer, there needs to be at least one on-line Streamer and one idle Streamer in the subnet, to wake up an off-line Streamer.



Wake-on-LAN network topology where On-line Streamer and the off-line Streamer on the same subnet

6.7. Keep Splashtop Center running in case of disaster

At Splashtop, we want to help your company's Splashtop Enterprise users stay up and running. With this in mind, we have devised a specific topology to offer our suggestion for setting up a Splashtop Center "High Availability" fall-back system. That is, if your main Server running Splashtop Center goes down, the backup Server you set up (using our instructions) will take over, so you can keep using Splashtop Enterprise with no interruption in remote connection service and ideally no loss of data. Basic architecture of the setup looks like this:



Referring to the illustration above:
If Server A somehow gets disconnected from the virtual witness disk in Server C, then Server B will automatically take over and launch the service for Splashtop Enterprise.

This assumes that:

- Server A is providing the Splashtop Center service, and Server B is the backup server.
- Prior to Server A's disconnection or other problem, it was reading and writing to the Sqlite database on the shared folder of Server C.

Then disaster strikes:

- A problem occurs which prevents Server A from operating, such as a disconnection from the network. Its status is "offline" and/or the Splashtop Center service simply cannot run.

If you have performed the setup instructions on the following pages, your High Availability fall-back solution kicks in:

- Server B will then become the main server and automatically provide Splashtop Center service to access the Sqlite database on the shared folder of Server C.

NOTES:

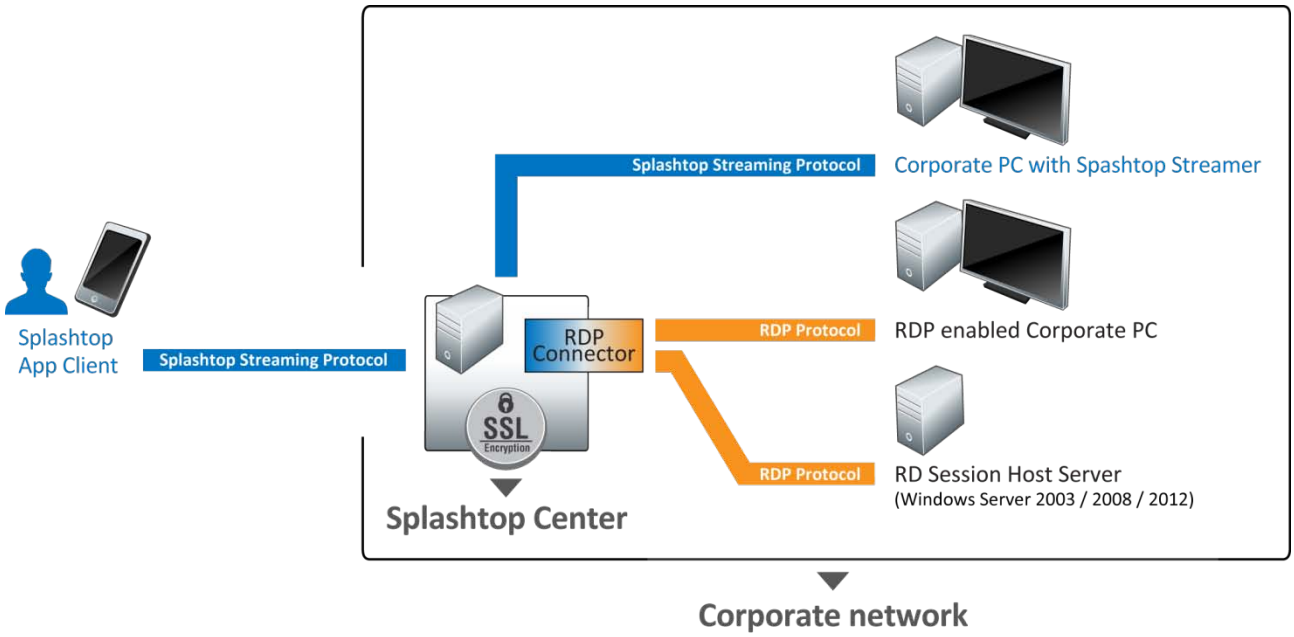
- The Failover Cluster uses an iSCI disk partition as a witness disk. The entire High Availability system can sustain failures of half the nodes (rounding up) as long as the witness disk keeps online.
- In the event that Server A is later restored to full service, it would then become the backup server for the entire High Availability system.

*For complete details, please see our separate document entitled "**Splashtop Center High-Availability Setup Guide**."*

6.8. Setting Up RDP Connector and Making a Connection

Our new SplashApp/**RDP Connector** paid option supports various configurations of Remote Desktop Services from Windows-based host machines:

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



Chapter 5 contains complete details about how to access the Splashtop Center Web Portal.

NOTE: This section focuses on setting up RDP Connector in Microsoft Windows **Server 2008 R2**. For tips concerning how to set up Microsoft Remote Desktop (RDP) and Remote Desktop Services (RDS) in Microsoft Windows **Server 2012**, please see Section 7.4 in the Appendix.

6.8.1. OS Compatibility

In general, **RDP Connector** is compatible with the Remote Desktop Protocol 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 (*details concerning RDP and RDS, in Server 2012, are in Section 7.4*)

… , and above.

On the other hand, for remote applications, only **Microsoft Windows Server 2008** (**Terminal Services**), **Windows Server 2008 R2**, and above, support the capability to specify a program to start when connecting. Other Windows editions ***DO NOT*** support this feature.

6.8.2. Scalability (Bandwidth Requirements)

Required productivity usage (output) bandwidth per RDP session is: **250 kbps; and reserve 510 kbps for optimal performance**. This is based on an RDP configuration of 1024 x 768 display resolution, with 16-bits color depth.

Referral Configuration of Splashtop Center (either RDS Host computers):

CPU: Intel i7-2600 3.4 Ghz

Memory: 16 GB RAM

Switch: 1000M Ethernet Switch

OS: Microsoft Windows 2008 R2 SP1 (64bit)

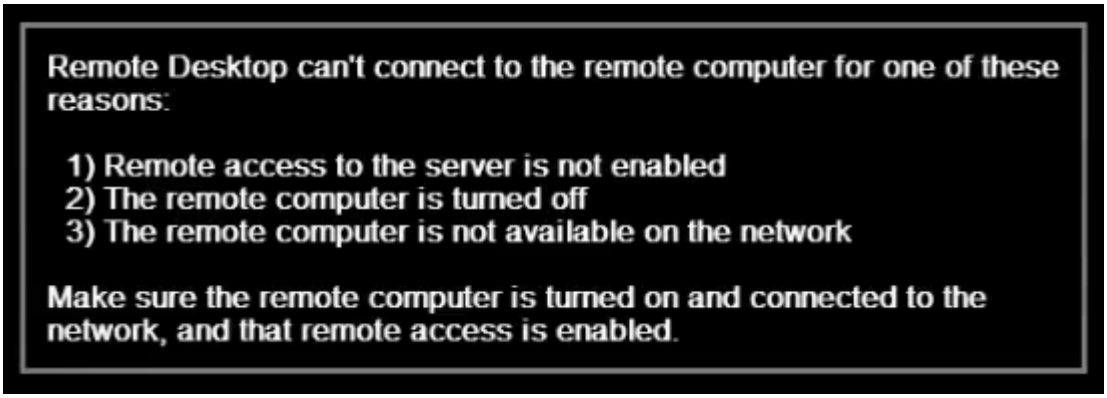
Bandwidth of Splashtop Center	Output (Bps)	Input (Bps)
MS Word, Excel, … document processing	5.8K ~ 8.3K	5.4K ~ 10.0K
Web/Portal pages (include Ad.) browsing	39.8K ~ 59.3K	59.0K ~ 372.0K
Video playing (30 FPS)	248.2K ~ 509.1K	2.4M ~ 26.7M

6.8.3. How to set up remote desktop for an RDP-enabled computer

6.8.3.1. Windows setup

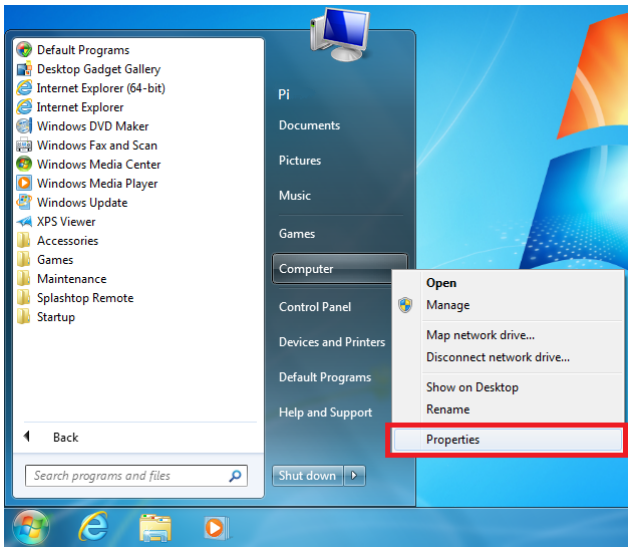
RDP remote desktop is disabled by default in Microsoft Windows 7 and Vista, but it's easy enough to turn it back on.

Please be aware that if RDP is *not* turned on, the following message will appear during connection.

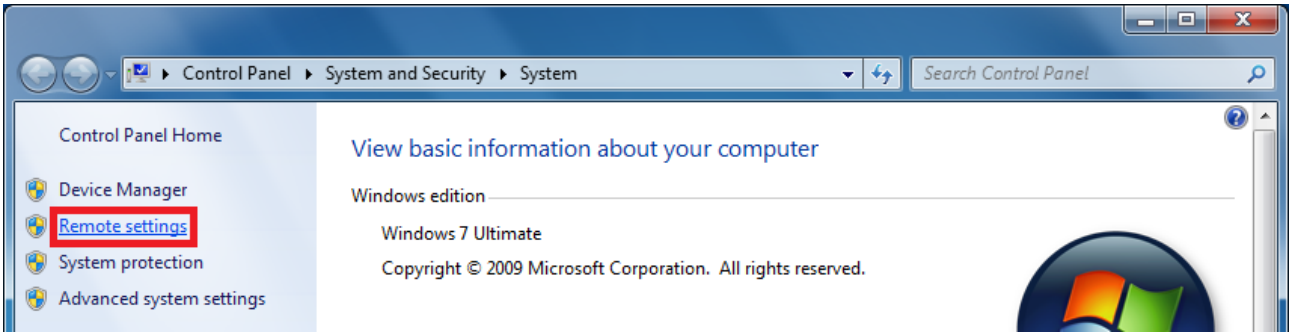


NOTE: Please be aware that RDP remote desktop is only included in the Professional, Business, and Ultimate versions of Microsoft Windows. The Home editions *__DO NOT__* have the remote desktop feature.

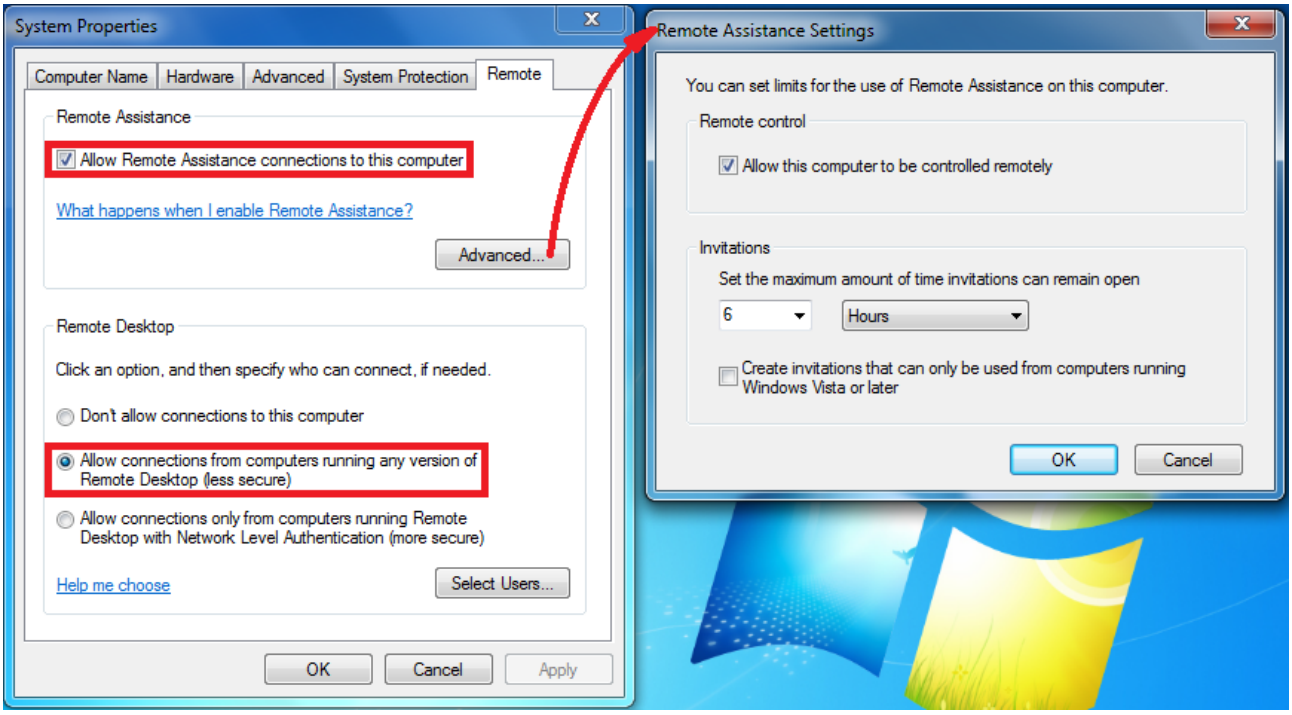
To get to the configuration page, you can either right-click the **Computer** icon and choose **Properties** as shown below, or you can type the word "system" into the Start Menu search box, and then find the entry for System.



Next, click the **Remote Settings** link on the left side, as shown below.



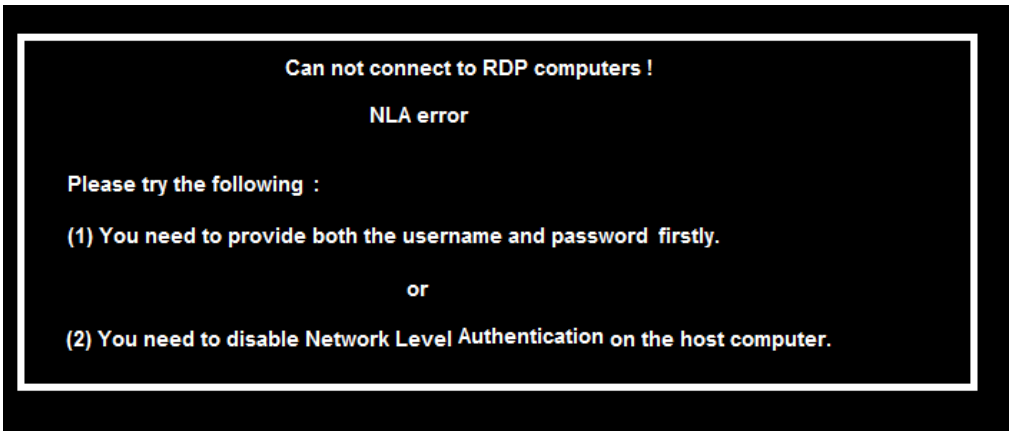
Now you can turn on Remote Desktop, as shown below:



To connect from a Splashtop App Client, please click the **Allow connections from computers running any version of Remote Desktop** button.

NOTE: Don't worry about setting up Firewall rules; Microsoft Windows Vista and Windows 7 will do that for you automatically.

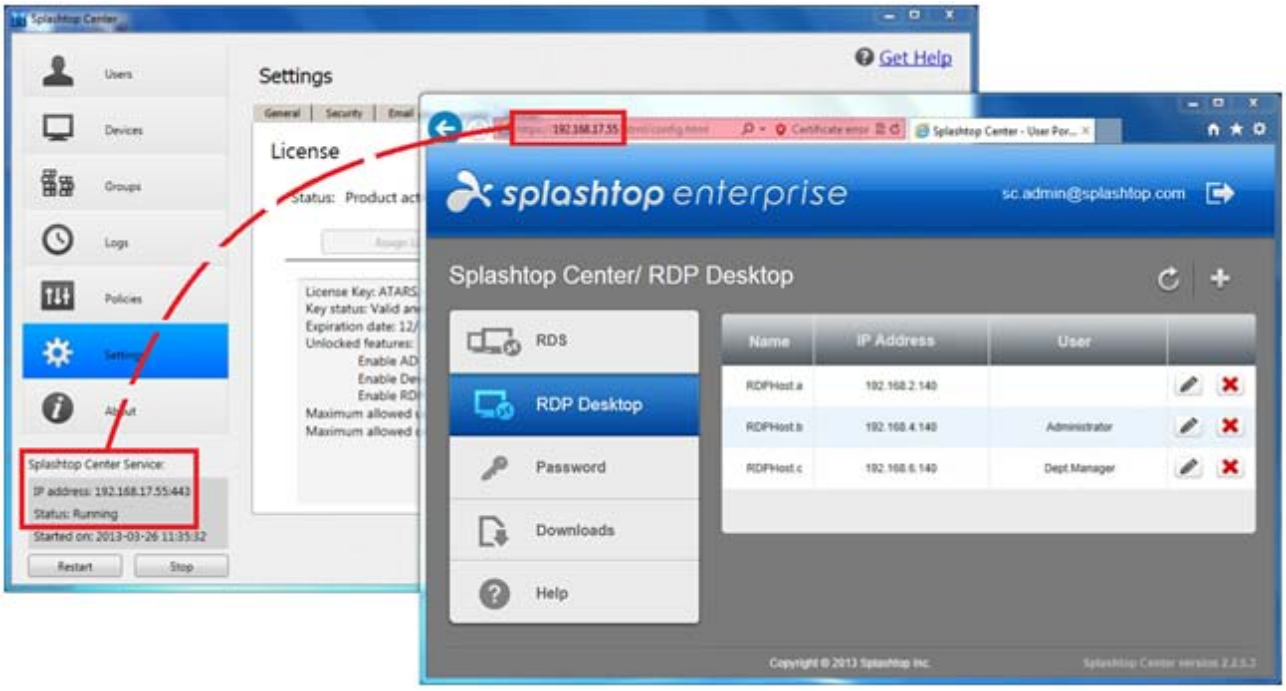
Also, please be aware that if you select the **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)** option, the User Name and Password fields must be filled in, when setting up the RDP in the Splashtop Center Web portal. Otherwise, the following error message will be seen at the time of attempted connection.



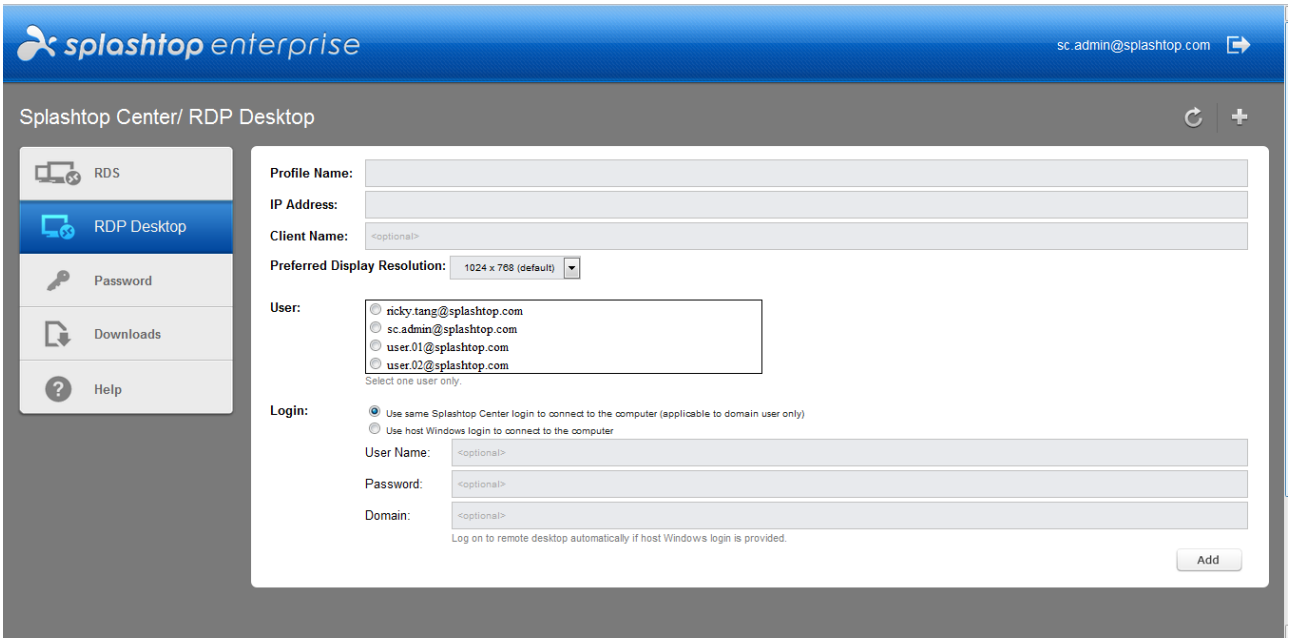
6.8.3.2. Splashtop Center setup

You will have to enter the **Splashtop Center Web portal** to configure the settings. The URL of the **Splashtop Center Web portal** is the same as the IP address of Splashtop Center, as explained earlier in section 5.1, Accessing the Splashtop Center Web Portal.

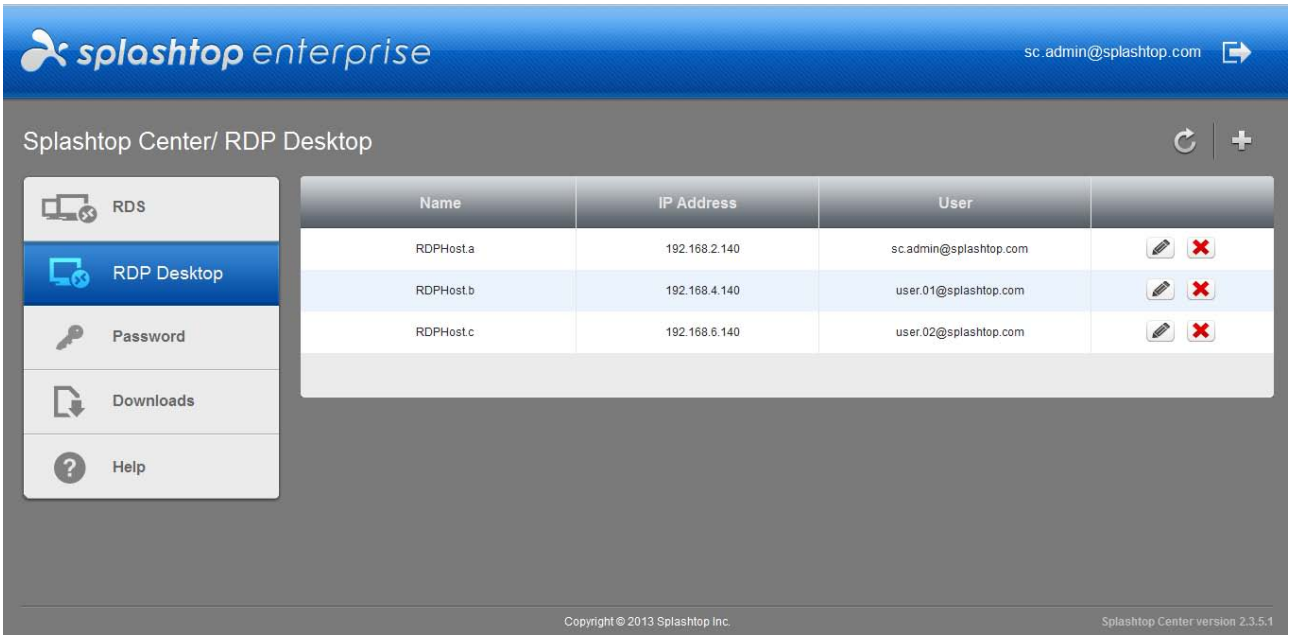
NOTE: You must log in using the IT Administrator account of Splashtop Center to set up **RDS** (Remote Desktop Services) and **RDP Desktop**. Logging in using a regular Splashtop Center user account only allows usage of the **Password** tab and **Downloads** tab (if a Gateway user), and only the **Downloads** tab if a Domain user.



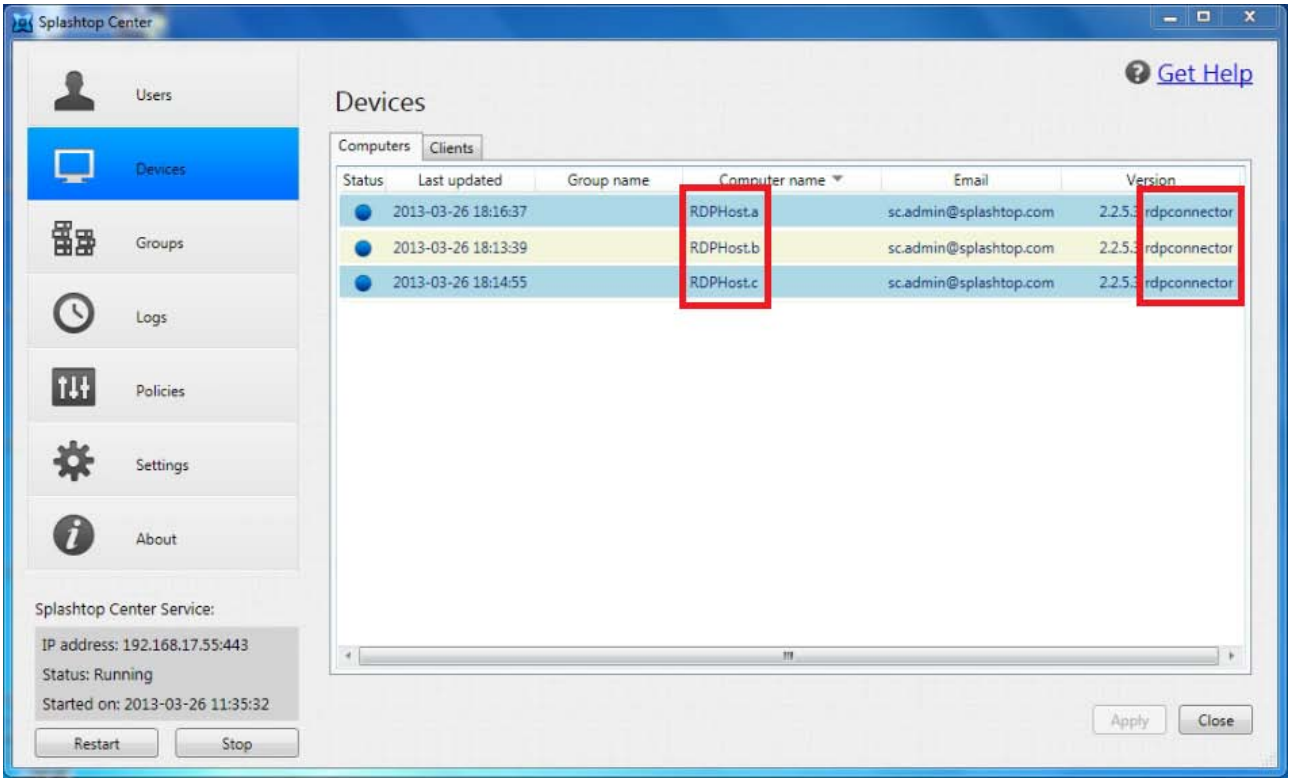
To add an RDP-enabled computer to the **RDP Desktop** list, you can click on the  button to open the *Add* dialog, as shown in the example below. Each field was explained earlier in section 5.6, RDP Desktop tab.



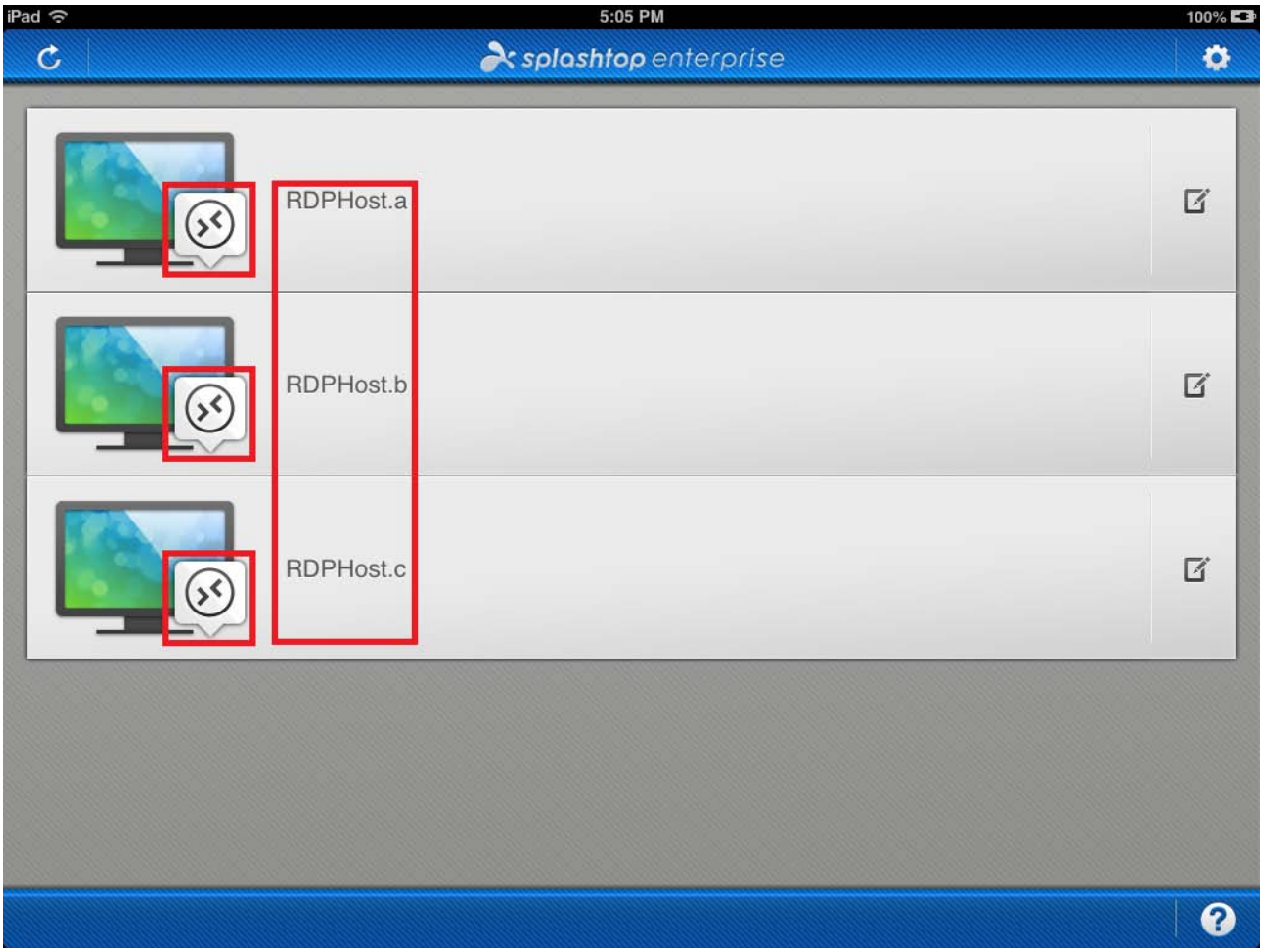
After you have done the settings, that RDP computer will be shown in the **RDP Desktop** list:



Meanwhile, in the **Devices** tab of Splashtop Center, you will find that there are new computers listed in the **Computers** sub-tab ("**RDPHost.a**," "**RDPHost.b**," and "**RDPHost.c**" in the example below); which you just added from the **Splashtop Center Web portal**.



And, on the **Splashtop Enterprise app** side, all RDP-enabled computers that have been set up via the **Splashtop Center Web portal** will be shown in the computer list with an RDP logo on the icon, as shown in the example below, which was taken from an iPad.



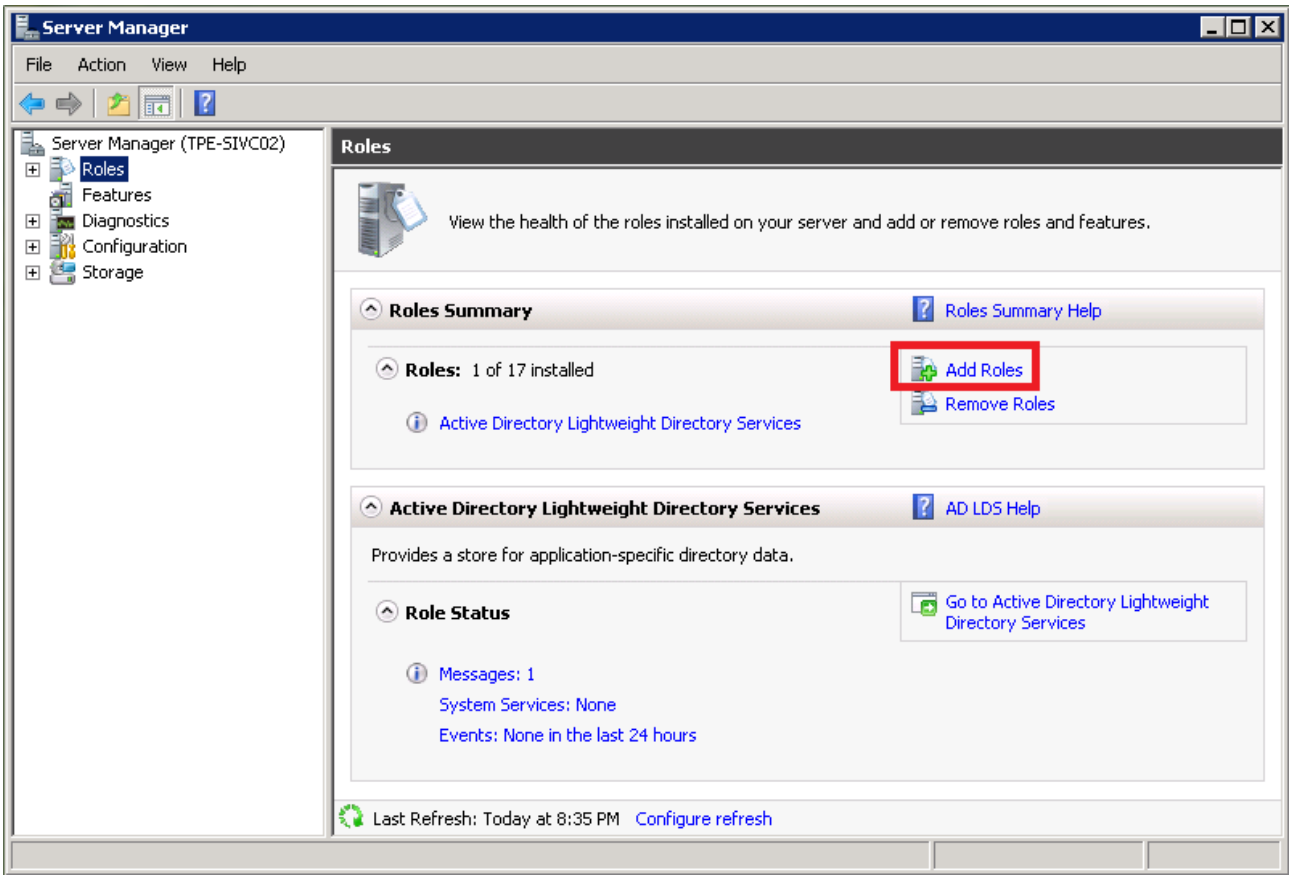
If you click an "RDP computer" icon in the computer list of the **Splashtop Enterprise app**, the remote desktop connection will then be established (connection to the RDP-enabled computer) via the RDP protocol.

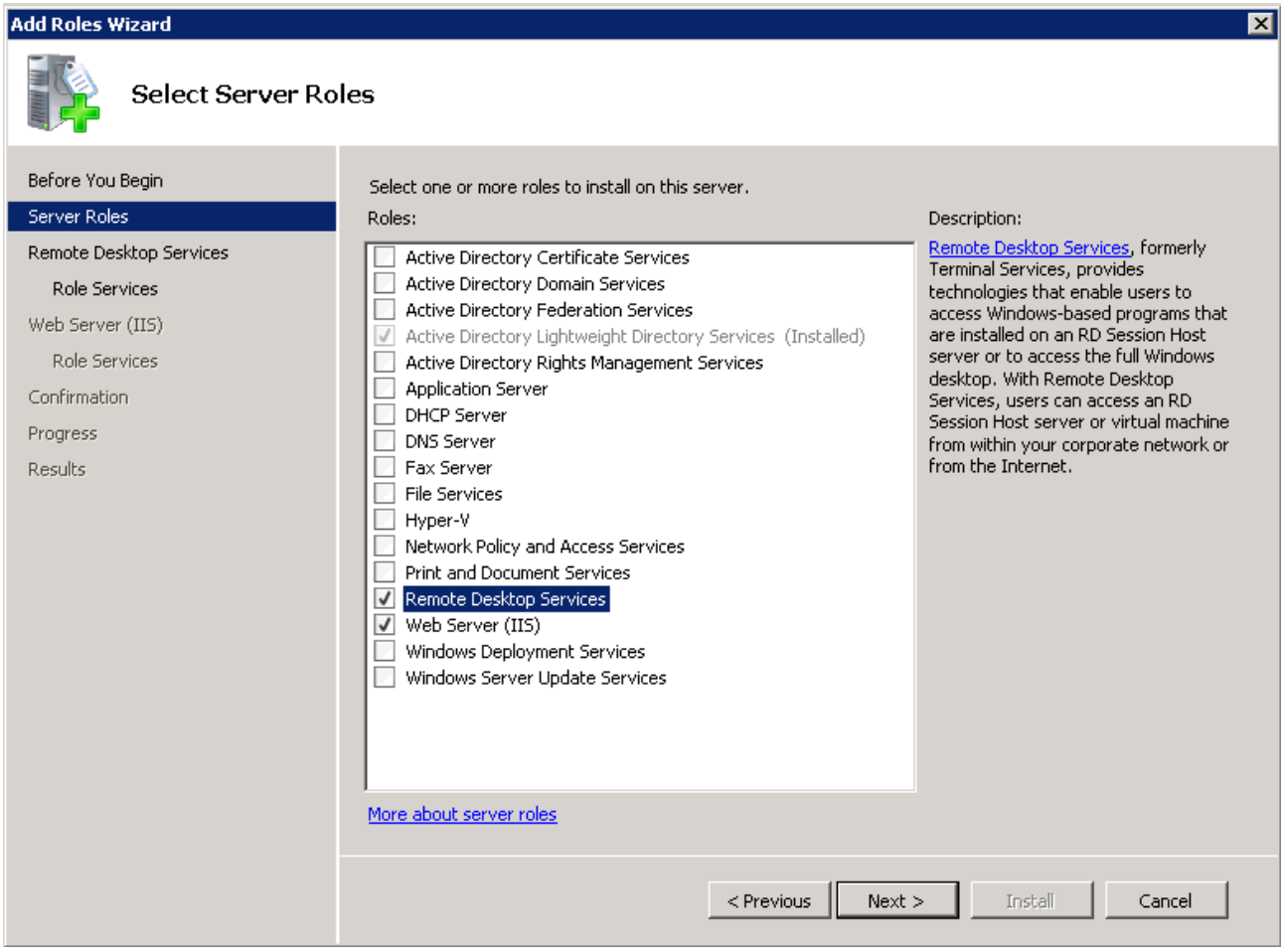
6.8.4. How to set up remote desktop from a Remote Desktop server with the RD Session Host configured

6.8.4.1. Windows setup

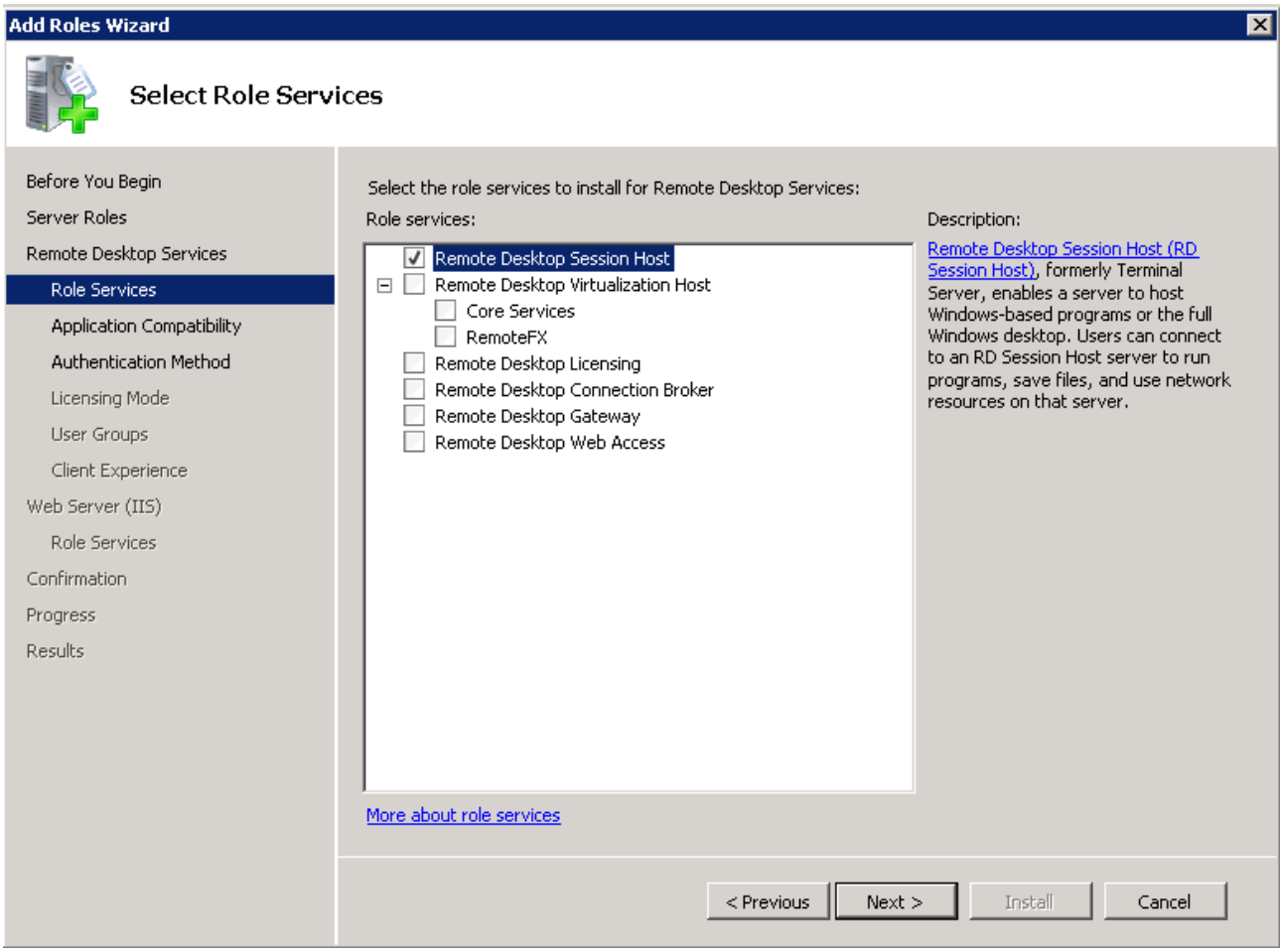
We recommend that you set up Windows Server 2008 (or later version) on the hosting server.

Launch the **Server Manager**, go to **Server Roles**, and install **Remote Desktop Services** and **Web Server (IIS)**.

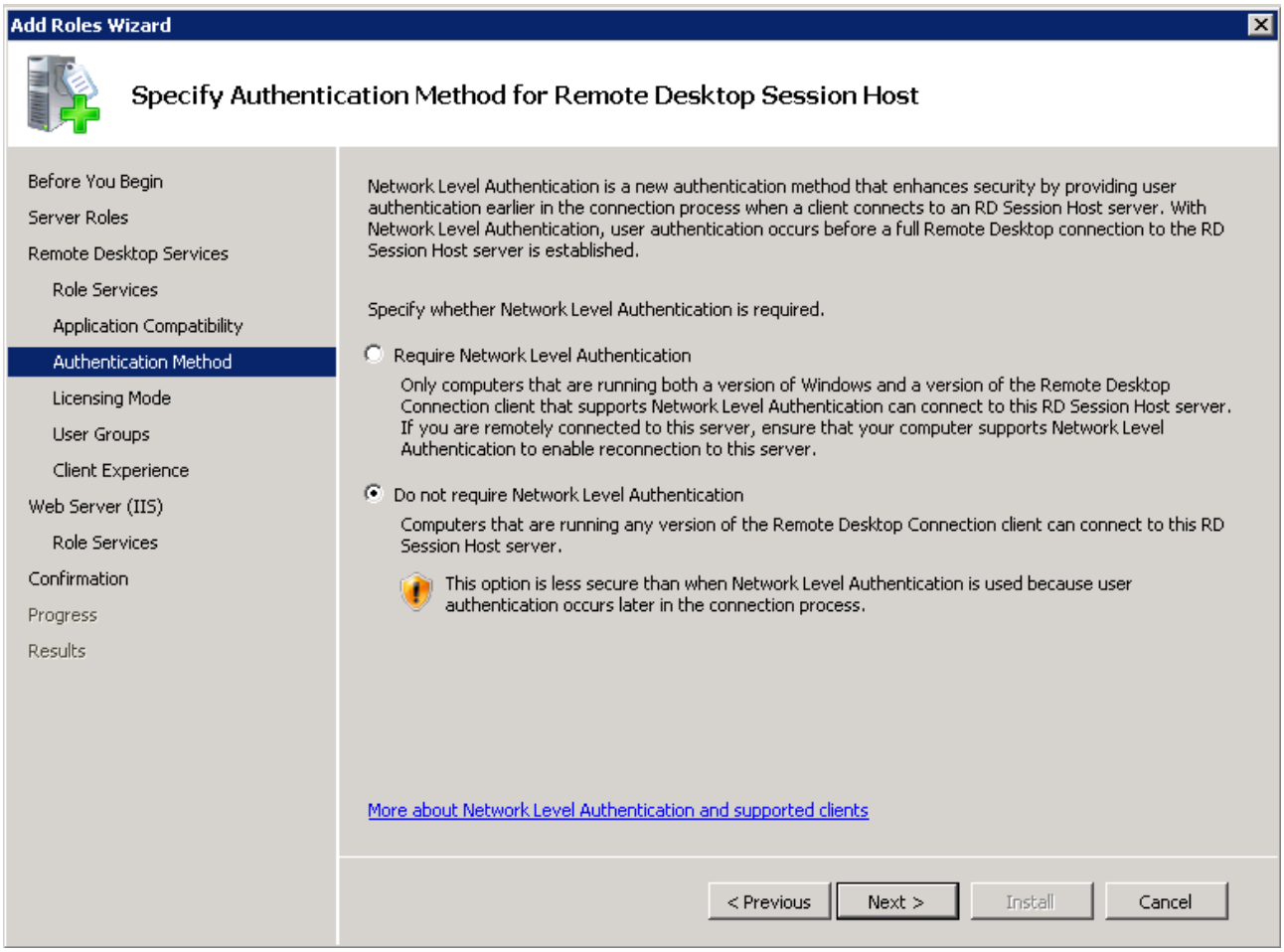



Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Remote Desktop Services
Role Services
Web Server (IIS)
Role Services
Confirmation
Progress
Results
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services (Installed)
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File Services
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Desktop Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description:
Remote Desktop Services, formerly Terminal Services, provides technologies that enable users to access Windows-based programs that are installed on an RD Session Host server or to access the full Windows desktop. With Remote Desktop Services, users can access an RD Session Host server or virtual machine from within your corporate network or from the Internet.
More about server roles
< Previous
Next >
Install
Cancel

Then, install **Remote Desktop Session Host** for the role.



In addition, in the settings for **Authentication Method**, we suggest that you select the **Do not require Network Level Authentication** option as shown below, so as to support any version of the Remote Desktop Connection client.



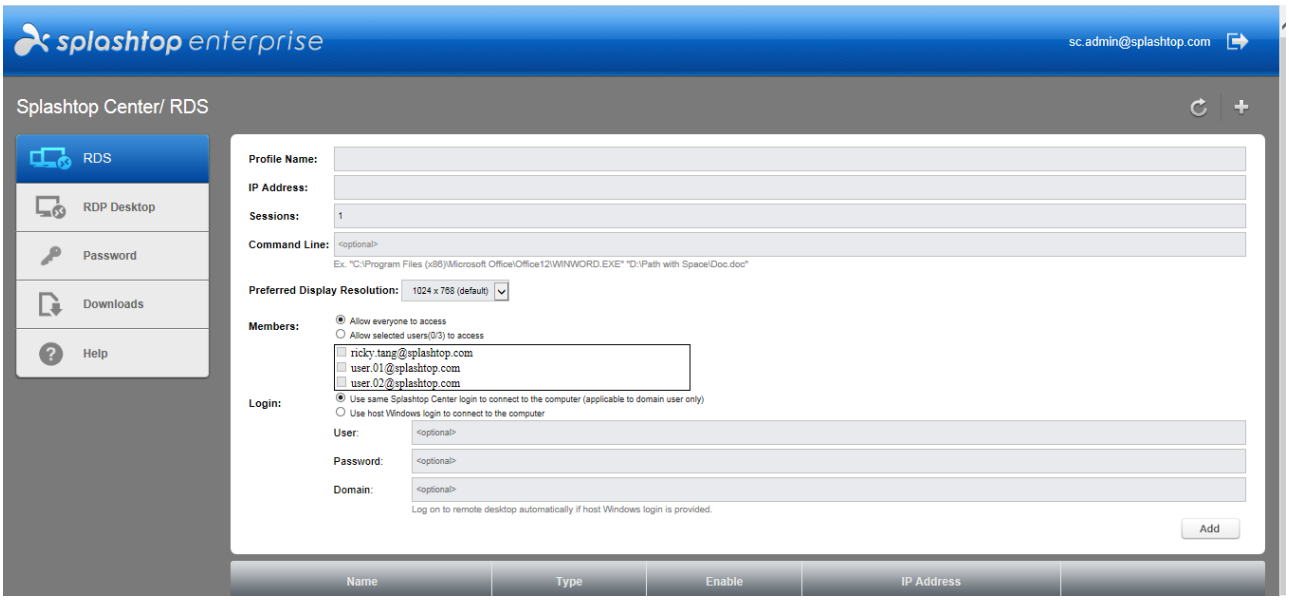
6.8.4.2. Splashtop Center setup

To set up the RDS remote desktop for use with Splashtop Enterprise, you will also have to access the **Splashtop Center Web portal** to configure the related settings. The URL of the **Splashtop Center Web portal** is the same as the IP address of Splashtop Center, as explained earlier in section 5.1, Accessing the Splashtop Center Web Portal.

In addition, please be reminded that ***ONLY*** IT Administrator accounts of Splashtop Center can set up the remote desktop computer(s) in the **RDS** tab.

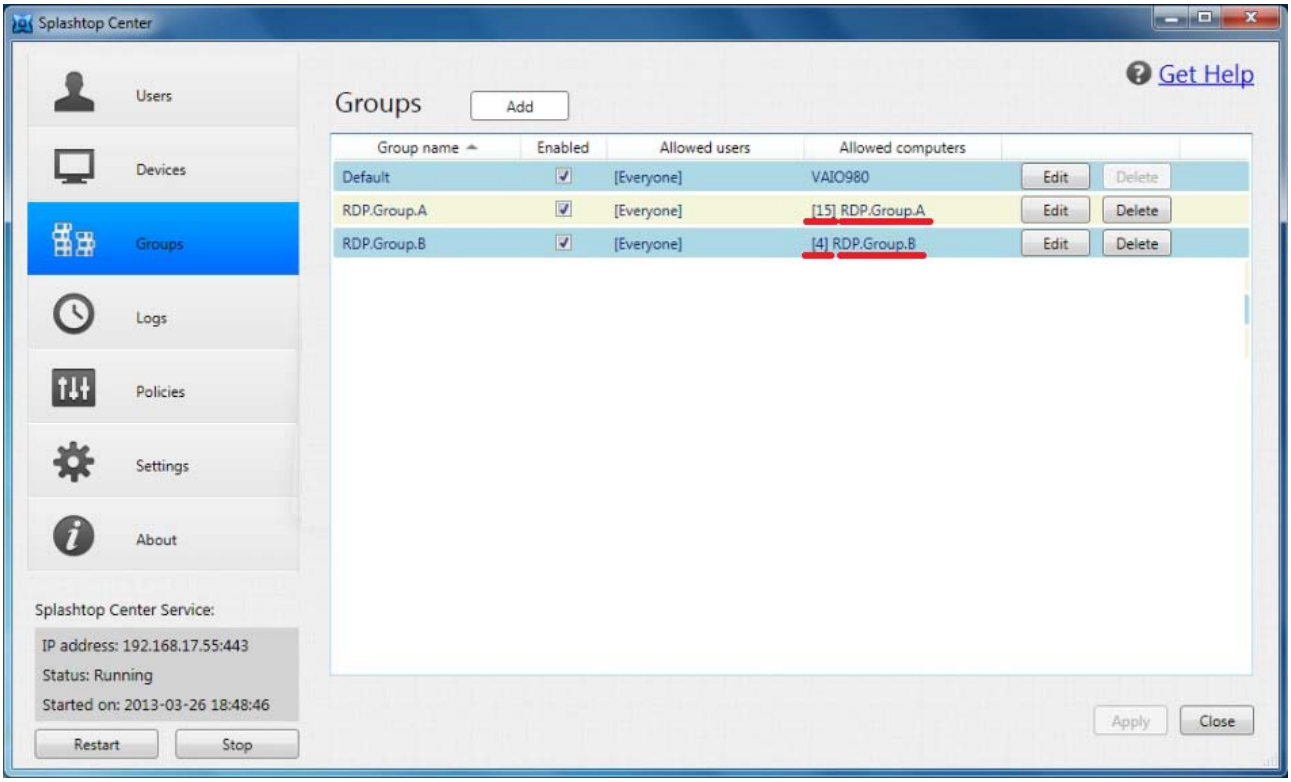
To add a group of multi-session RDS for remote desktop shared access into the **RDS** tab, click on the  button to open the *Add* dialog, as shown in the example below. Especially important is the **Use same Splashtop Center login to connect to the computer** checkbox, as mentioned earlier in section 5.5, RDS tab.

Please note that if the **Session** count is set to **1** as shown in the example below, it is not required to set up the Remote Desktop Session Host, and can therefore save you a few setup steps during the Windows RDP configuration.

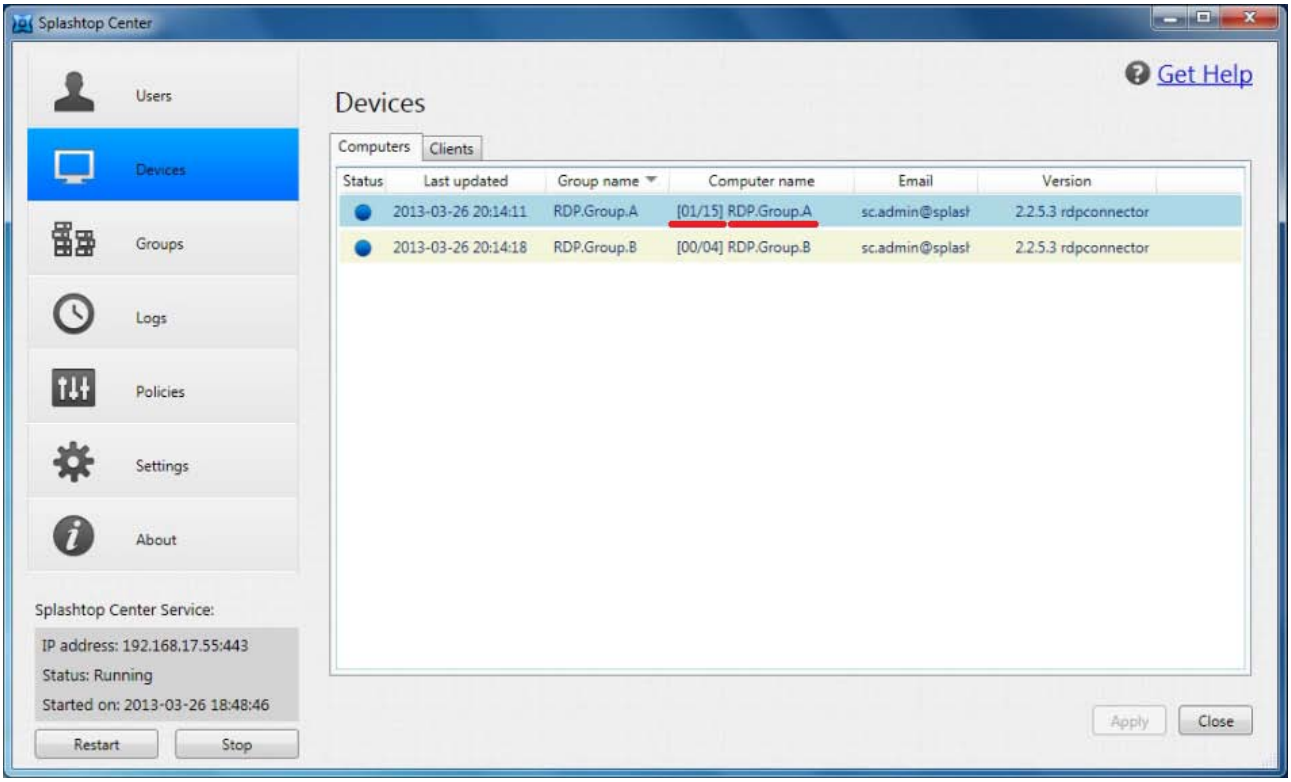


Once you have finished the settings to add a new RDS computer, it will be listed in the **RDS** tab of the **Web portal**.

In addition, the new items you just added via the **Web portal** (in this example, **RDP.Group.A** and **RDP.Group.B**) will be listed in the **Groups** tab of the Splashtop Center console, along with the regular Streamer groups that had been created directly using the Splashtop Center console. The name in the **Allowed computers** column for new groups (added via the **Web portal**) will be prefixed by the connectable (RDP) sessions information, in the format of "[total sessions] RDP Group Profile Name".



In addition, once a **Splashtop Enterprise app** is connected to a session of the RDP Group, the connection status of the Group will be shown in the format of "[connected sessions / total sessions] RDP Group Profile Name" in the **Devices/Computers** tab of the Splashtop Center console. In this case (see example illustration below), it is **[01/15] RDP.Group.A**, which indicates that among the 15 total allowed sessions, there is 1 RDP session currently being connected.



On the **Splashtop Enterprise app** side, that RDP remote desktop group will be shown in the computer list. The new group contains an auto-created virtual instance of a remote desktop computer, such that the RDP group can be in closer alignment with the Streamer group. In our example, the RDP remote desktop icon for the RDP group we added is now shown below as "**RDP.Group.A**" on the iPad screen.

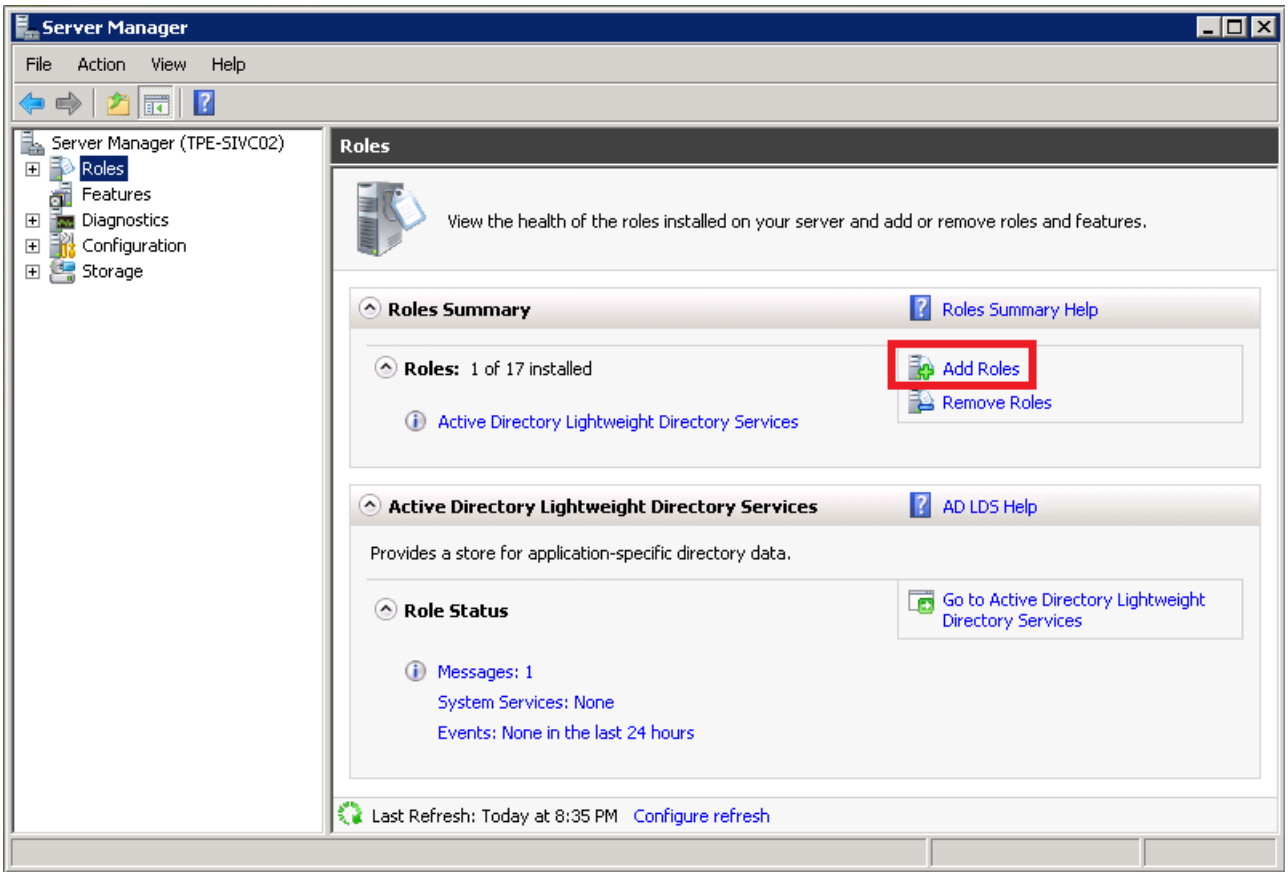
Now, if you tap the RDP remote desktop computer icon  in the computer list of the **Splashtop Enterprise app** (example shown above on the iPad), the RDP connection will be established with the RDS Server via the RDP protocol.

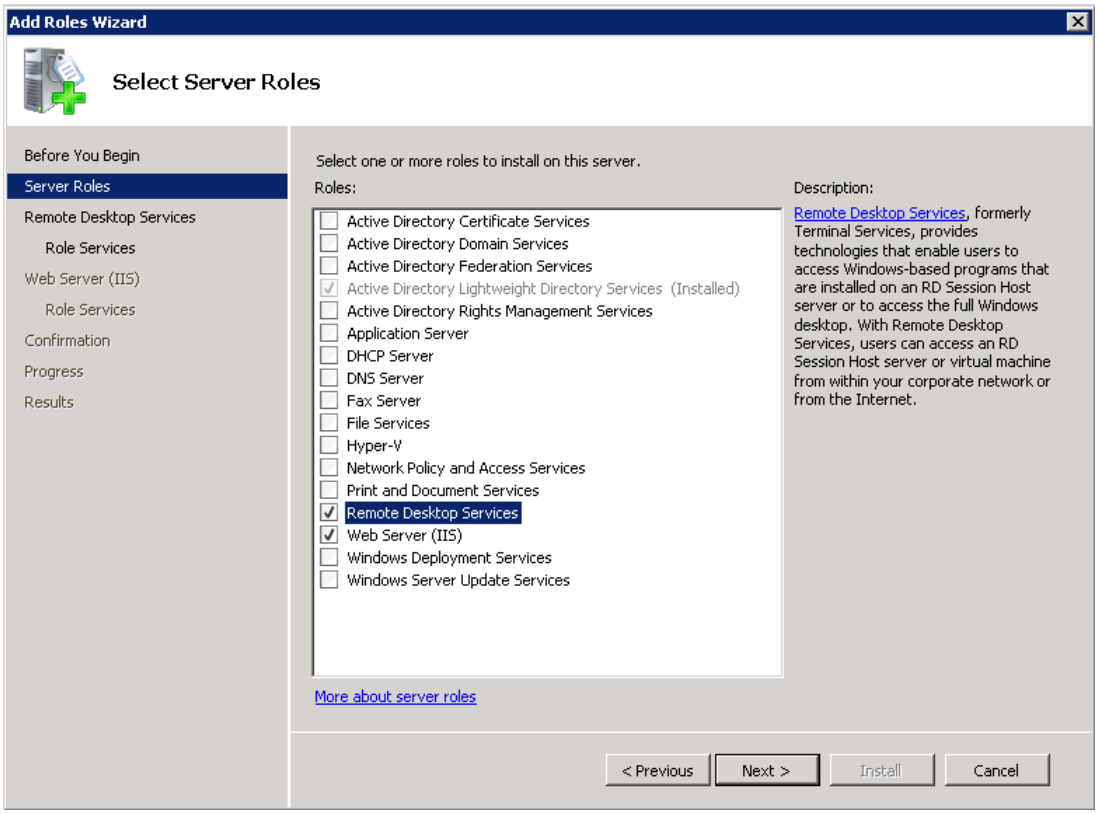
6.8.5. How to set up a remote application from Remote Desktop server with RD Session Host configured

6.8.5.1. Windows setup

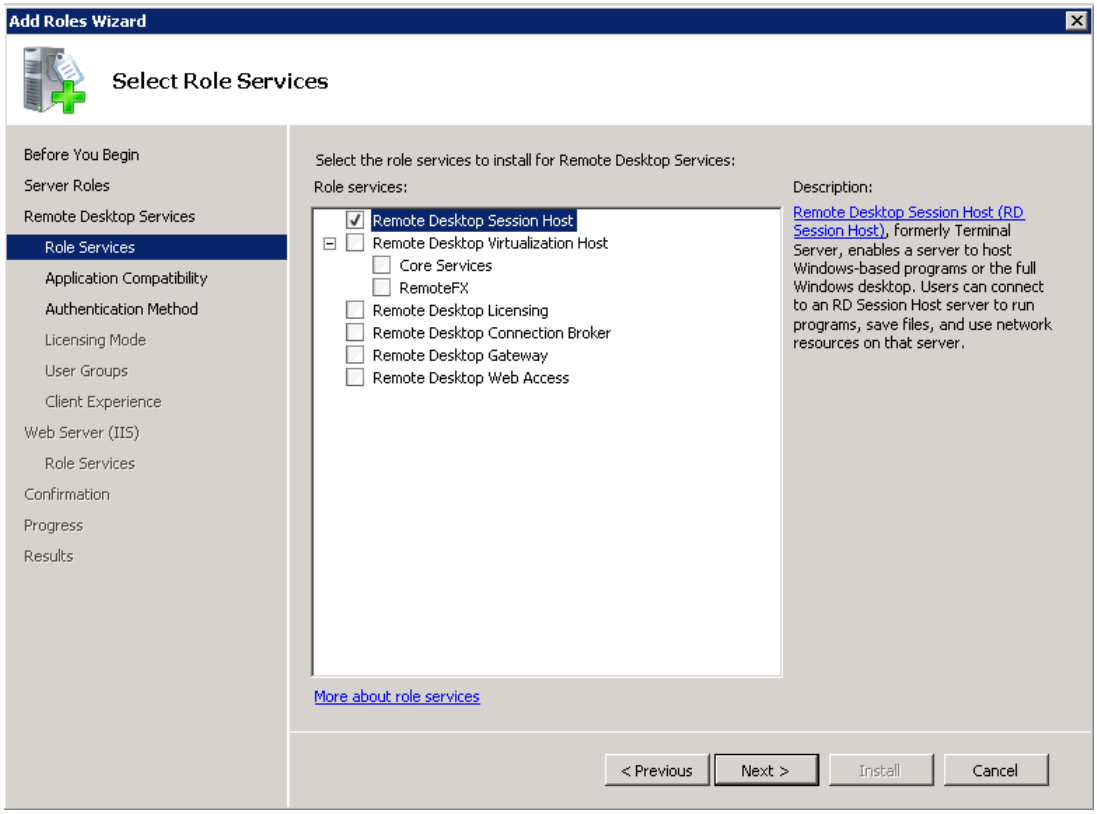
Please note that it is required that Windows Server 2008 R2 (or later version) be set up on the hosting server.

Launch the **Server Manager**, go to **Server Roles**, and install **Remote Desktop Services** and **Web Server (IIS)**.

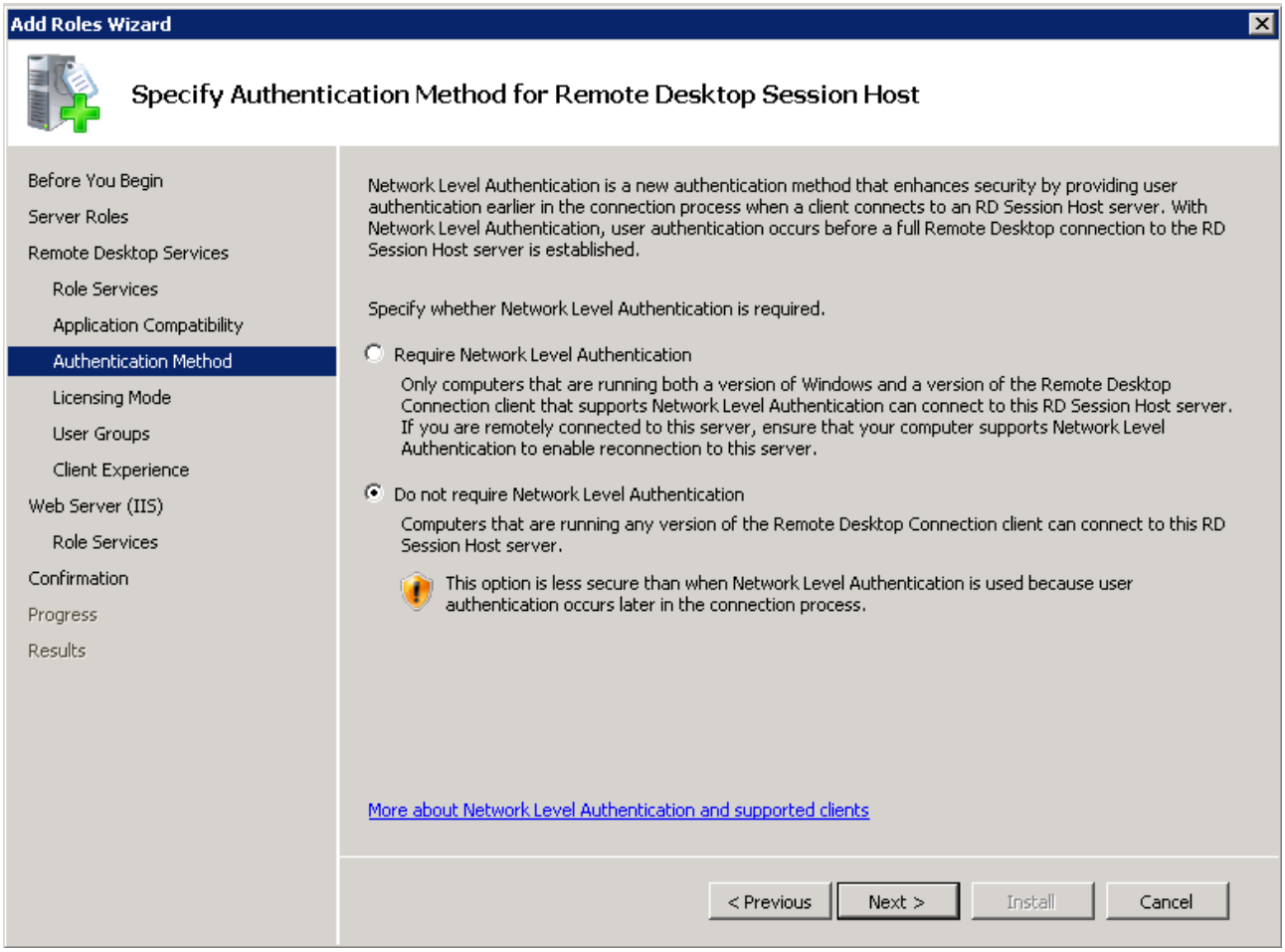




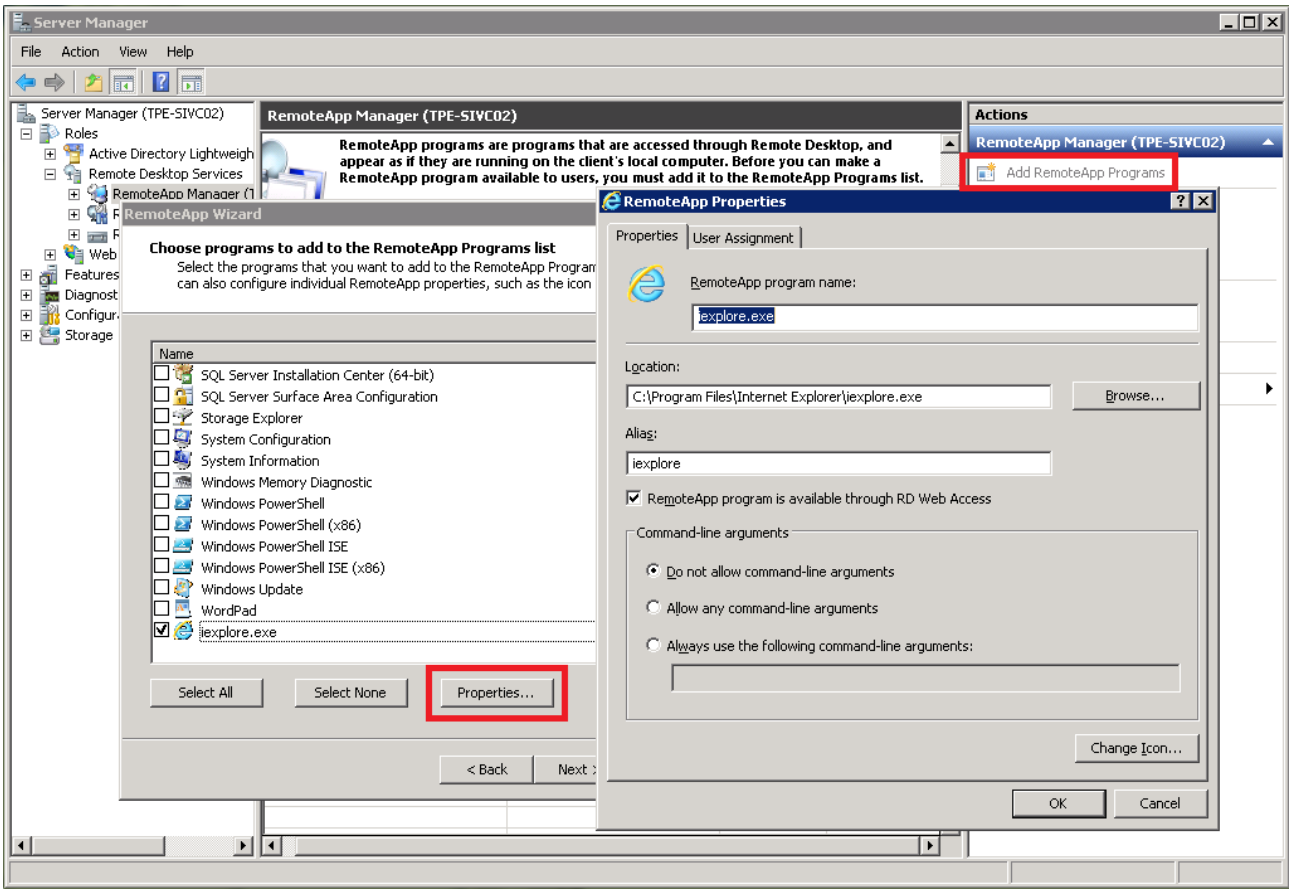
Then, install **Remote Desktop Session Host** for the role.



In addition, in the **Authentication Method** setting, we suggest that you select the **Do not require Network Level Authentication** option, to enable support for any version of Remote Desktop Connection client.

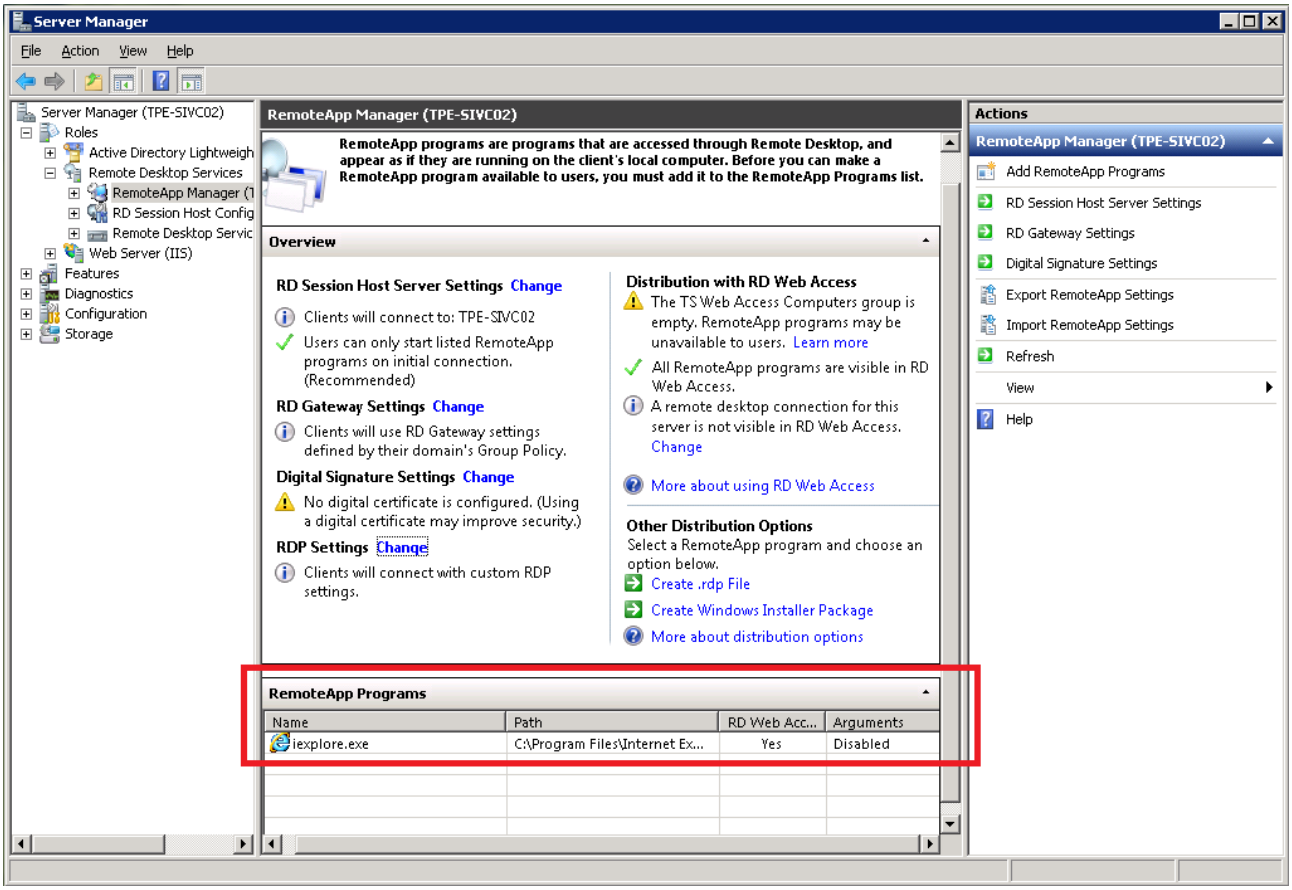


Now you can configure the Remote Application. Go to the **Actions** pane at the right side of the Server Manager window, select **RemoteApp Manager** in Remote Desktop Services, and click **Add RemoteApps Program**. Then, you can select from the list of programs, or select a different program by using the **Browse…** button.

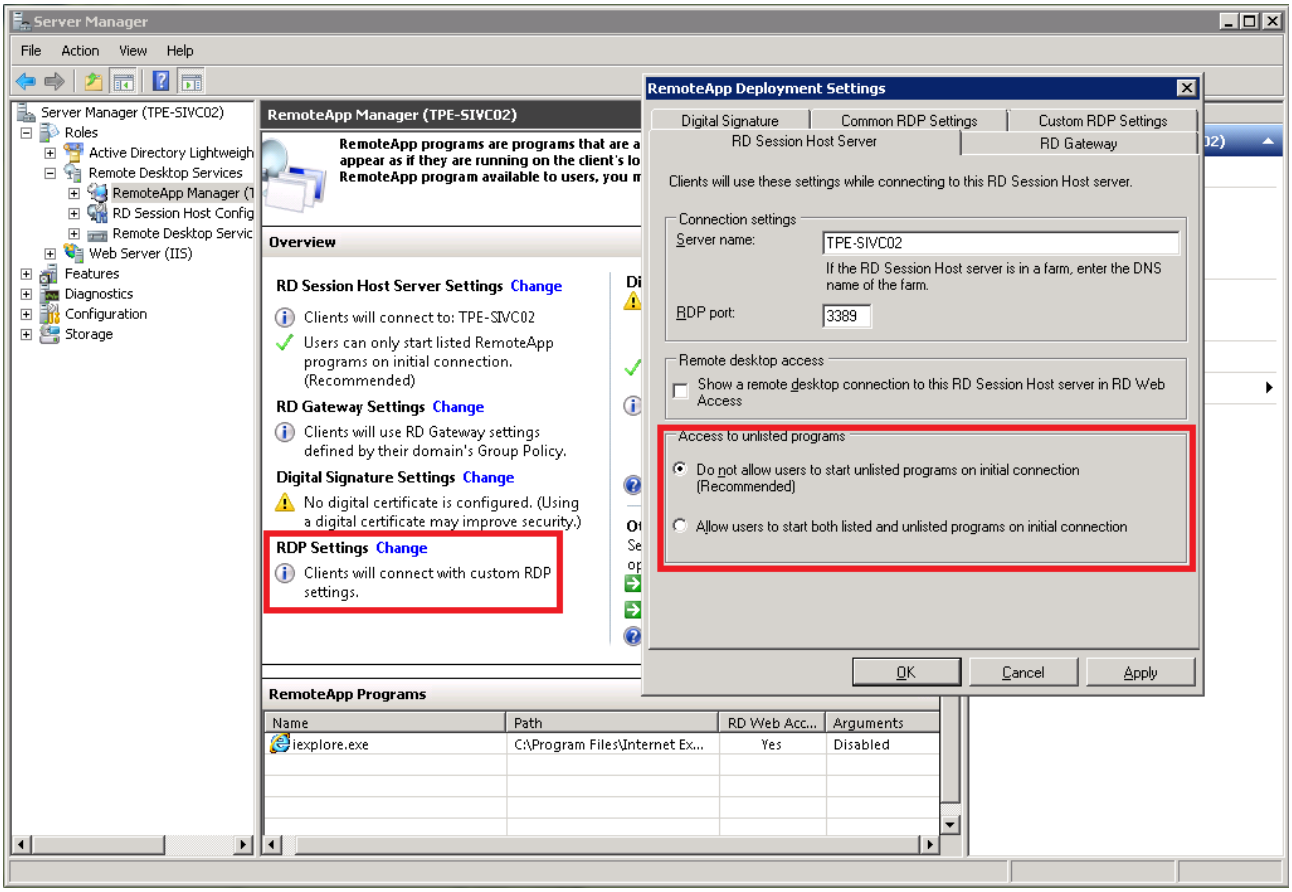


You can also assign command line arguments.

Once you have finished the settings to add the RemoteApp programs, you can find the names of those programs listed in the **RemoteApp Programs** list, as indicated in the example below.



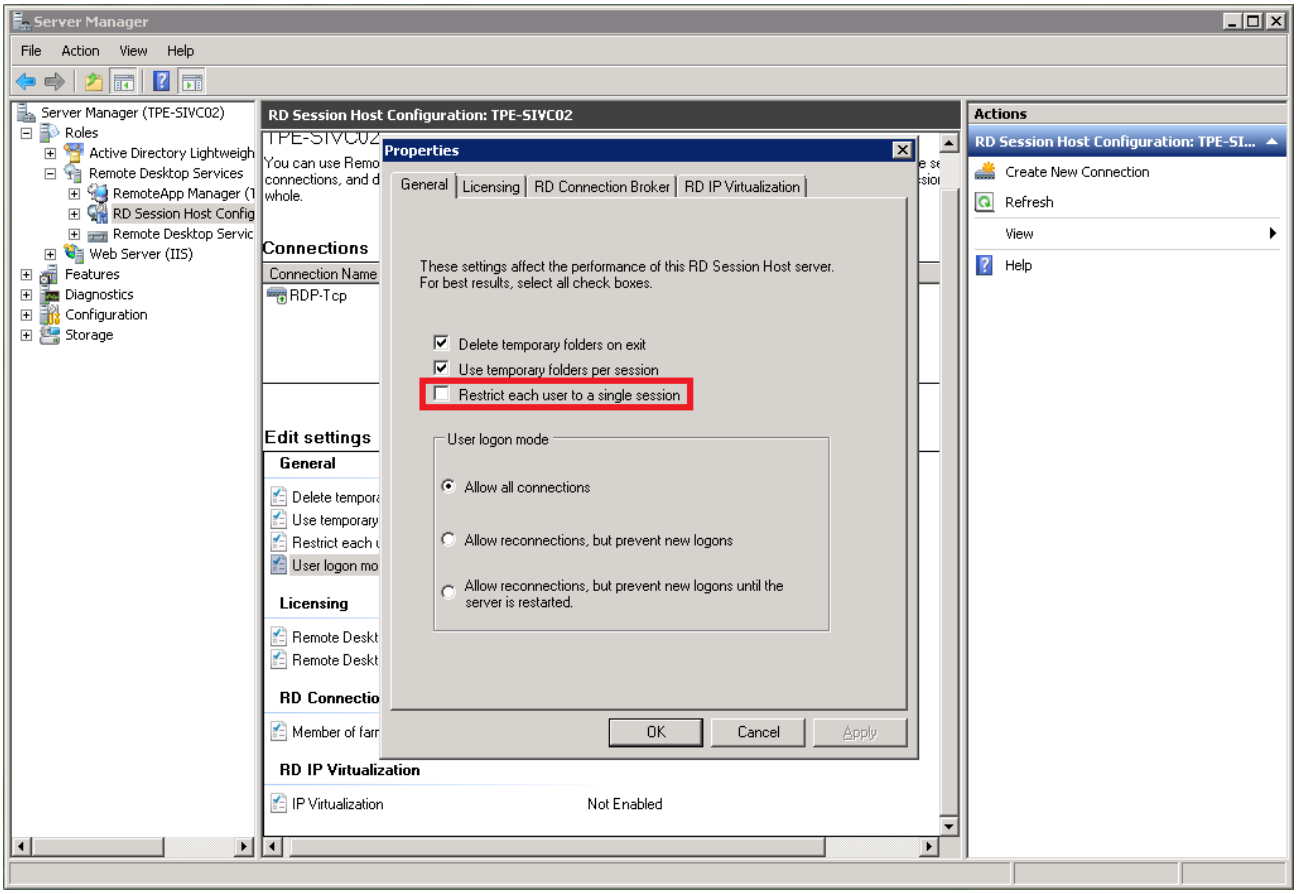
In addition, please note that if you do *not* want your users to start the unlisted programs upon initial connection, you must verify the **RDP Settings** to make sure the option has been selected, as indicated in the example below.



Next, in the **RemoteApp Deployment Settings** dialog, configure the **Remote Desktop** (RD) **Session Host server** to setup the access rights of programs.

At this point, you have a Remote Desktop server running with the appropriate remote application setup.

Finally, if you want to allow each user to log in with multiple sessions at the same time, this option can be turned "on" or "off" using the **Restrict each user to a single session** checkbox. This is found in the **General** tab of the **Properties** dialog box accessed from the **RD Session Host Configurations** section.



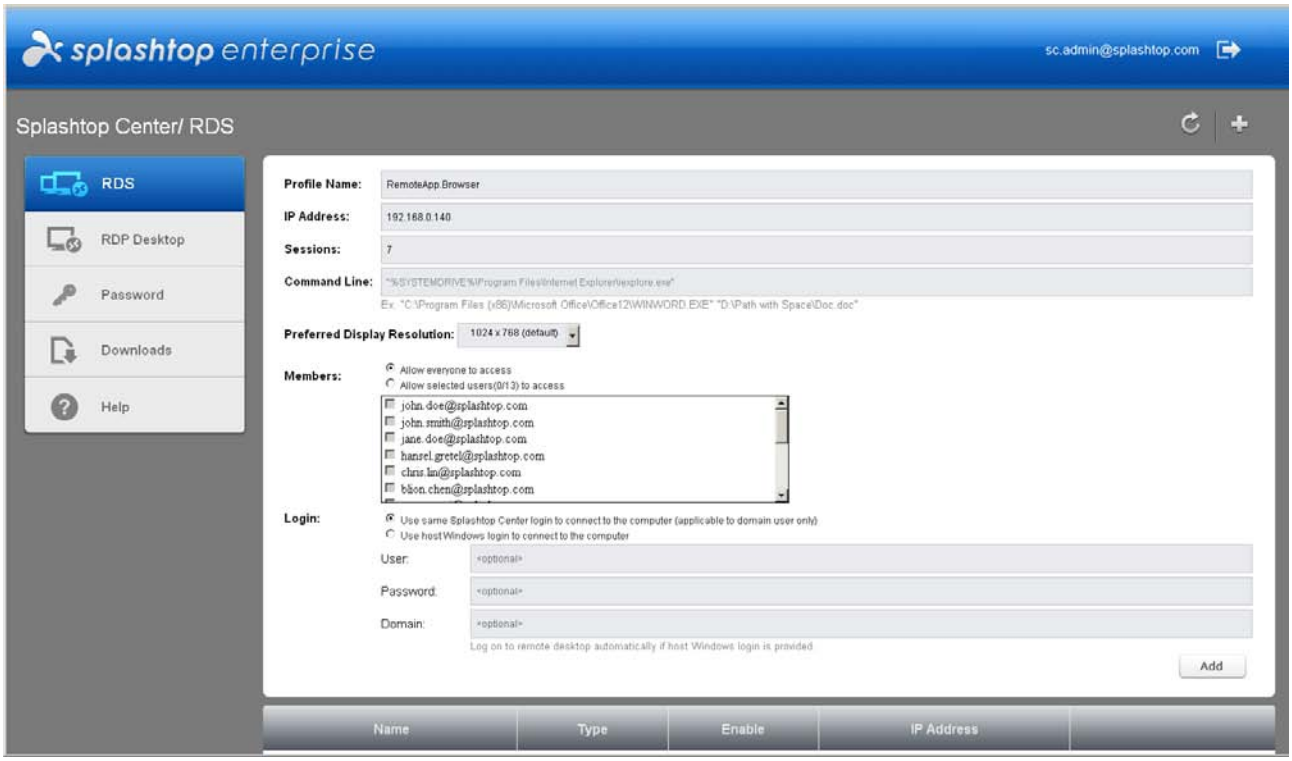
6.8.5.2. Splashtop Center setup

Likewise, to set up the RDS remote application for use with Splashtop Enterprise, you will also have to access the **Splashtop Center Web portal** to configure the related settings. The URL of the **Splashtop Center Web portal** is the same as the IP address of Splashtop Center, as explained earlier in section 5.1, Accessing the Splashtop Center Web Portal.

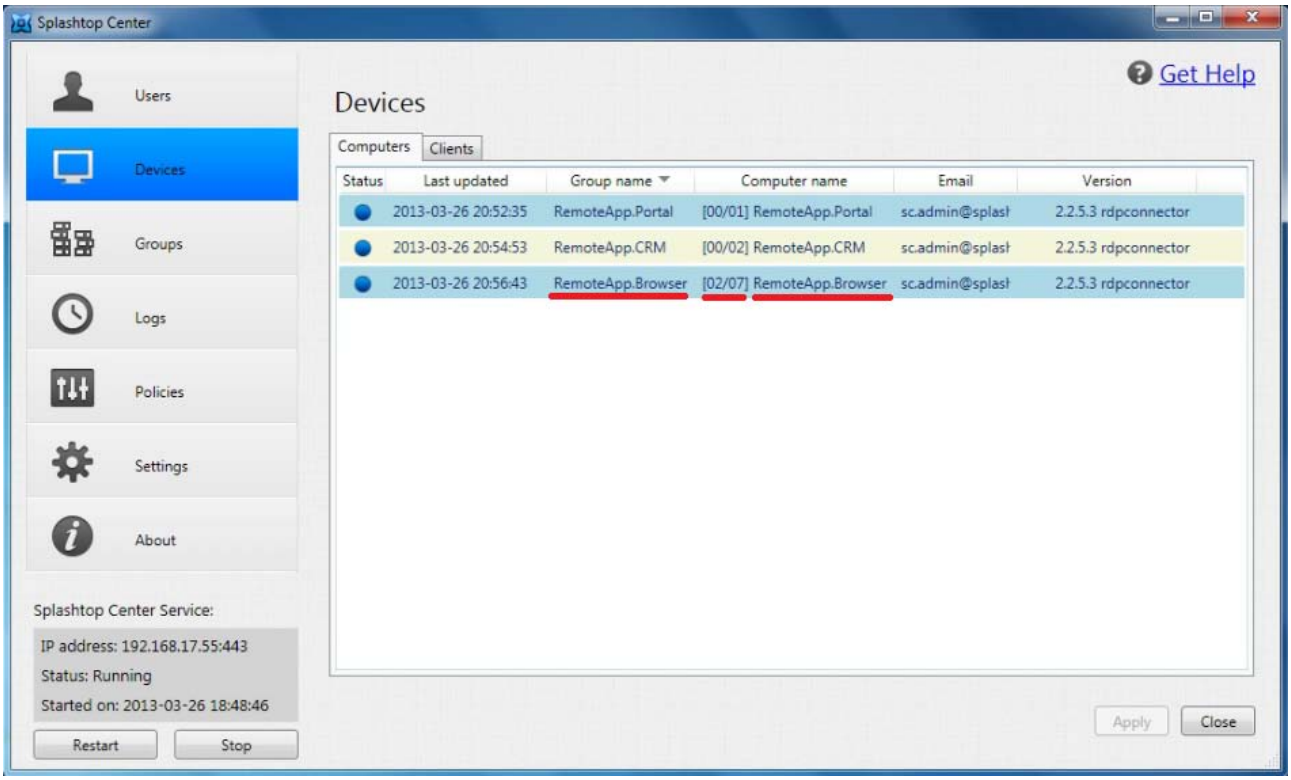
In addition, please be reminded that ***ONLY*** IT Administrator accounts of Splashtop Center can set up the remote application(s) in the **RDS** tab. Anyone logged in with a regular Splashtop Center user account will not have the **RDS** tab or the **RDP Desktop** tab available.

NOTE: Please be aware that only Microsoft Windows Server 2008 (**Terminal Services**), Windows Server 2008 RT2, and above support the capability to specify a program to start when connecting. Other Windows editions ***DO NOT*** support this feature.

To add a remote application into the **RDS** tab, click on the button to open the *Add* dialog, as shown in the example below. Especially important is the **Command Line** field, in which you must specify the file path of the program that you want to launch automatically. For example, if you are going to set up a specific browser for users to launch when starting a session, you can add it like this example:

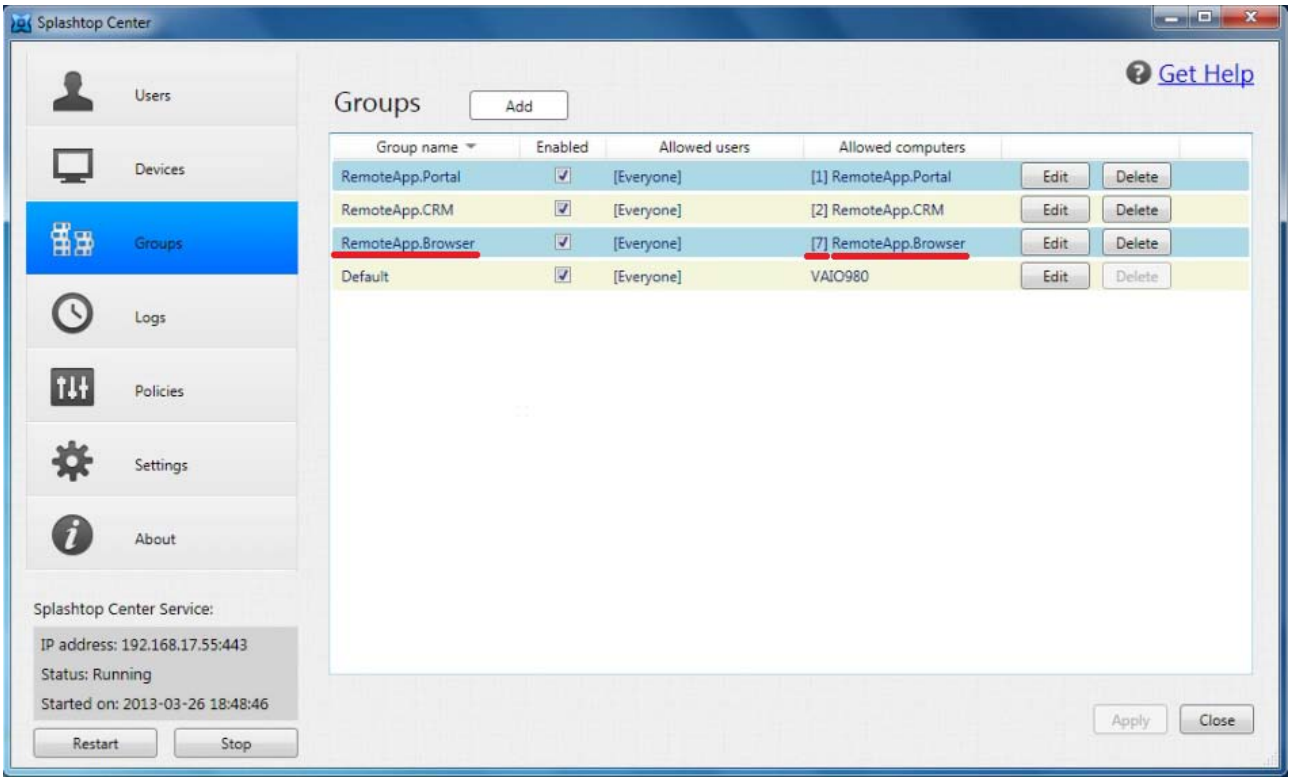


Once you have finished the settings to add the remote application group for shared access, the name of the newly created remote application **(RemoteApp.Browser)** will be listed in the **RDS** tab of the **Web portal**. It will also be shown in the **Devices/Computers** tab of the Splashtop Center console, as illustrated in the example below.

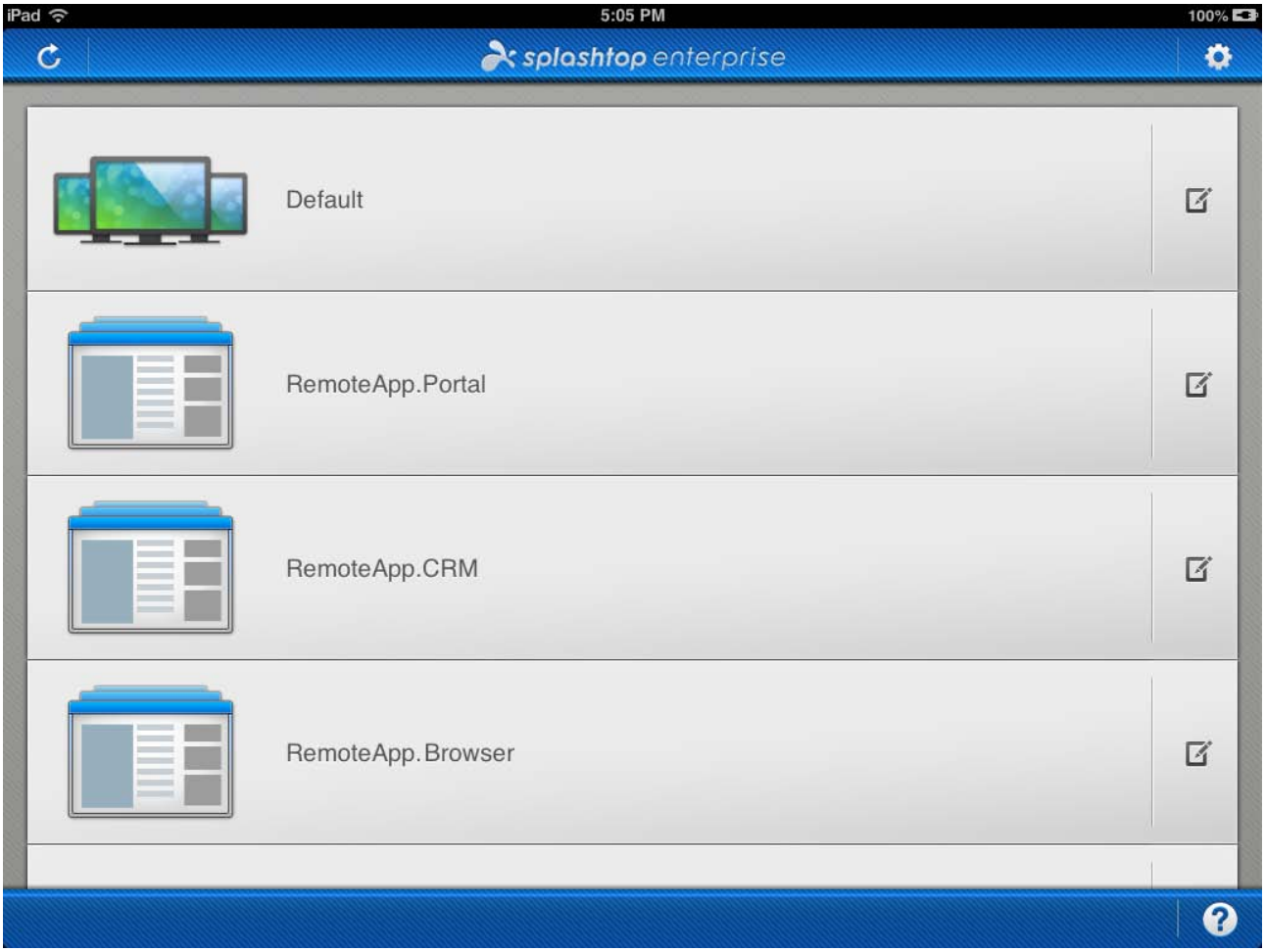


The Computer Name for the new remote application group (in this example, **RemoteApp.Browser**), which we just added in via the Splashtop Center Web portal, will be prefixed by the connectable (RDP) sessions information, in the format of "[connected sessions / total sessions] Remote application Profile Name". In this case (see example illustration above), it is "**[02/07] RemoteApp.Browser**", which indicates that among the 7 total allowed sessions, there are 2 RDP sessions currently being connected.

In addition, **Allowed Computers** for the new remote application group in the **Groups** tab of the Splashtop Center console will be prefixed by the connectable (RDP) sessions information, in the format of "[total sessions] Remote application Profile Name" as shown below.



On the **Splashtop Enterprise app** side, that remote application group will be shown in the computer list. The new group contains an auto-created virtual instance of a remote application group, such that it can be in closer alignment with the Streamer group. In our example on the iPad screen, the remote application icon for the new group we added is now shown below as "**RemoteApp.Browser**."



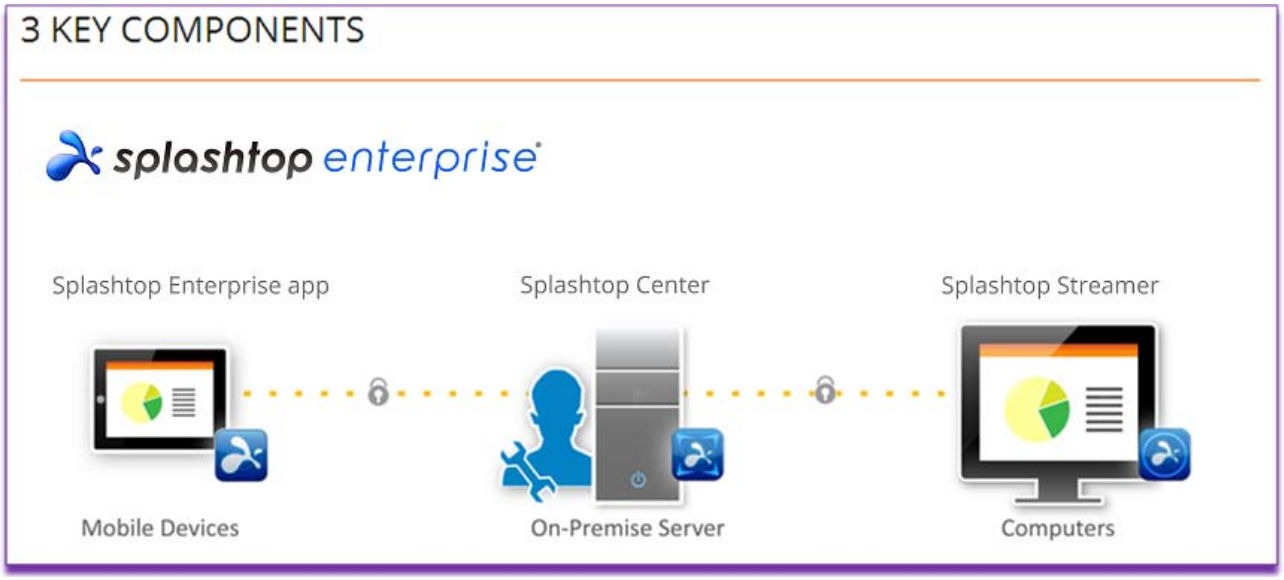
Now, if you select the remote application icon in the computer list of the **Splashtop Enterprise app**, the RDP connection will be established to the RDS Server via the RDP protocol, and will automatically launch the specified program when connecting.

7. Appendix

7.1. Splashtop Enterprise Architecture

This subject was touched upon in the Introduction, but here we offer more detail.

The Splashtop Enterprise solution is comprised of three specific components, each residing on different systems within an enterprise network. Together, they provide a secure remote access experience for mobile and remote users.



7.1.1. Splashtop Enterprise App

The Splashtop Enterprise App is a lightweight remote client that is installed on an employee's mobile device, such as a Apple iPad or iPhone, Google Android phone or tablet; Macs and Windows-based PCs, and laptops. Users initiate secure remote access requests from their mobile device to their enterprise desktop systems via the Splashtop Enterprise App software.

7.1.2. Splashtop Center

Splashtop Center, usually installed within the enterprise firewall (or DMZ) where possible, facilitates remote access sessions between the user's mobile device(called the "client device," running the Splashtop Enterprise App) and enterprise desktops (running the Splashtop Streamer software). An on-premise solution hosted on Windows-based servers running within the enterprise, Splashtop Center ensures the protection of sensitive data and improves regulatory compliance. For example, organizations specifically concerned with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance can be assured that Splashtop Enterprise is a remote access solution that helps organizations meet HIPAA guidelines for the privacy and security of health care information. More details about HIPAA in conjunction with Splashtop Center can be found in the Splashtop Enterprise *Security White Paper*.

When the mobile device running the Splashtop Enterprise App is on a different local area network, the Splashtop Center software also provides secure relay services to enable cross-firewall connections between the mobile device and the enterprise desktop running the Splashtop Streamer. All cross-firewall connections are secured using Secure Socket Layer (SSL) AES 256 encryption.

Seamless integration with existing Active Directory user directories helps IT Administrators simplify the process of local user authentication and ensure that only authorized users can establish remote Splashtop Enterprise sessions.

NOTE: Other installation options were mentioned in section 3.1 (for example, if your company has no DMZ).

7.1.3. Splashtop Streamer

The Splashtop Streamer software is installed on each Windows PC or Mac from which the user will access or control applications and data from their mobile device. The IT Administrator will send "Invitation E-Mail" to the user, containing a hyperlink and instructions for the user to download and install the Streamer to his or her computer. Therefore, users will normally install the Streamer themselves. To enable mobile users to access more than one desktop computer, IT Administrators can configure a group of computers — each with Splashtop Streamer installed — as a shared resource pool from within the Splashtop Center management console.

7.2. Readiness / Installation Checklist

Here is a handy checklist to help you verify that you have performed all the steps needed, from beginning to end, in order to install Splashtop Center and set up shared resources for your employees to use.

#	Required Items
1	IT Administrator: Install Splashtop Center and activate the Splashtop Center License.
2	IT Administrator: Prepare one IP address and one TCP port for the Splashtop Center. On-premise Gateway and Relay port is port 443 (default). Set up port forwarding between public IP and private IP if you need external access.
3	IT Administrator: Set up the Gateway User Account and Password.
4	Employees: Streamer installation Install Splashtop Streamer on desktop or laptop. Fill in the Splashtop Center field, Gateway user Email (ID), and Password for Streamer. (May also need to allow Streamer through the desktop/laptop firewall.)
5	Employees: Client installation Install Splashtop Enterprise app on an iPad or other client device. Fill in the Splashtop Center field, Gateway user Email (ID), and Password on the client app.

#	Optional Items
6	IT Administrator: Prepare one domain name and set up internal DNS (and external DNS for the IP address if you need external access).
7	IT Administrator: Set up the Administrator's ID and Password for the Groups feature. Assign the user to Admin Authority.
8	IT Administrator: Import trusted or self-signed SSL certificate in Splashtop Center.
9	Employees: Import self-signed SSL certificate in mobile device and computer.
10	IT Administrator: Add Active Directory users.
11	IT Administrator: Check Enable Device Activation option, create activation codes, and send activation codes to each user. Employees: Activate user devices by activation codes.

7.3. SSL Certificate Import / Export

Splashtop Center is not considered secure if there is no SSL certificate. Therefore, a self-signed SSL certificate is pre-bundled with Splashtop Center by default. So, if you choose not to import your own SSL certificate, then the default SSL certificate will be used instead.

For security enhancements, it is recommended that you generate a self-signed SSL certificate using the function provided by Splashtop Center (**Settings** > **Security** > **Generate**), if not importing one. This was explained earlier in section 4.8.2.

7.3.1. Installing the SSL Certificate

In Step 1 of each of the five sub-sections below, an example of an actual URL might look like:
https://s4b-splashtop.com:443/sslcert
where 443 is a port number, and **sslcert** is the name of a certificate.

7.3.1.1. On an Android tablet or Android phone (4.0):

1. Enter https://your_Splashtop_Center_URL:port/sslcert into the Browser app.
2. A Security warning dialog prompt will open. Select **Continue** to proceed.
3. Insert the file name for the certificate.
4. If no lock screen PIN or password has been set on your tablet, a message will open and ask you to set it. Press **OK**.
5. Set a Pattern, Pin, or Password lock screen. After setting it, the certificate is installed onto your tablet.

7.3.1.2. From your Nexus 7 tablet's internal storage:

1. Get the certificate onto your computer from https://your_Splashtop_Center_URL:port/sslcert via the browser.
2. Connect the tablet to the computer, and copy the certificate or key store from your computer to the root of internal storage.
3. Tap **Settings** 》 **Personal** 》 **Security** 》 **Credential storage** 》 **Install from storage**, then select the filename of the certificate.
4. Enter the key store password if prompted, and then tap **OK**.

7.3.1.3. On an iPad or iPhone:

1. Launch https://your_Splashtop_Center_URL:port/sslcert from the Safari app.
2. When you see the **Cannot Verify Server Identity** dialog prompt, proceed with **Continue**.
3. Select **Install** to trust the self-signed certificate to the iPad device.

7.3.1.4. On a Mac PC or Notebook:

1. Get the certificate onto your computer from https://your_Splashtop_Center_URL:port/sslcert via the Safari browser.
2. Double click the certificate in the Downloads, and **Keychain Access** will open.
3. Choose **Always Trust**.

7.3.1.5. In Windows

1. Launch https://your_Splashtop_Center_URL:port/sslcert in Internet Explorer and download the **sslcert.cert** file.
2. Run the command **mmc.exe** from the Windows 7 Start, Search bar.
3. If prompted by UAC (User Account Control) to allow the MMC to make changes to this computer, click **Yes**. It will bring up a blank MMC console.
4. From the **File** menu, select **Add/Remove Snap-in…**.
5. In the **Add or Remove Snap-ins** window, choose the **Certificates** snap-in, then click the **Add >** button. It will bring up the **Certificates snap-in** window.
6. In the **Certificates snap-in** window, select **Computer account**, then click the **Next >** button. This will bring up the **Select Computer** window.
7. In the **Select Computer** window, select **Local computer: (the computer this console is running on)**, then click the **Finish** button. This will bring you back to the **Add or Remove Snap-ins** dialog.
8. In the **Add or Remove Snap-ins** window, click the **OK** button.
9. In the MMC console, select **Trusted Root Certification Authorities**.
10. In the **Action** menu, select **All Tasks**, then select **Import…**. It will bring up a **Certificate Import Wizard** window.
11. In the **Certificate Import Wizard** window, click the **Next >** button. It will bring up **File to Import**.
12. In the **Certificate Import Wizard** window, click the **Browse…** button to select the **sslcert.cer** file which you downloaded in step 1, and then click the **Next >** button. It will bring up **Certificate Store**.
13. In the **Certificate Import Wizard** window, select **Place all certificates in the following store** then **Certificate store: Trusted Root Certification Authorities**. Click the **Next >** button, click the **Finish** button, and then click **OK** to finish the Certificate Import Wizard.
14. **Exit** the MMC console. A "**Save console settings to Console1?**" message will display. No need to save the console, so click the **No** button.

After completing these steps, you would need to **uninstall and reinstall Splashtop Streamer** if you should ever want to log in to Splashtop Center without an SSL certificate.

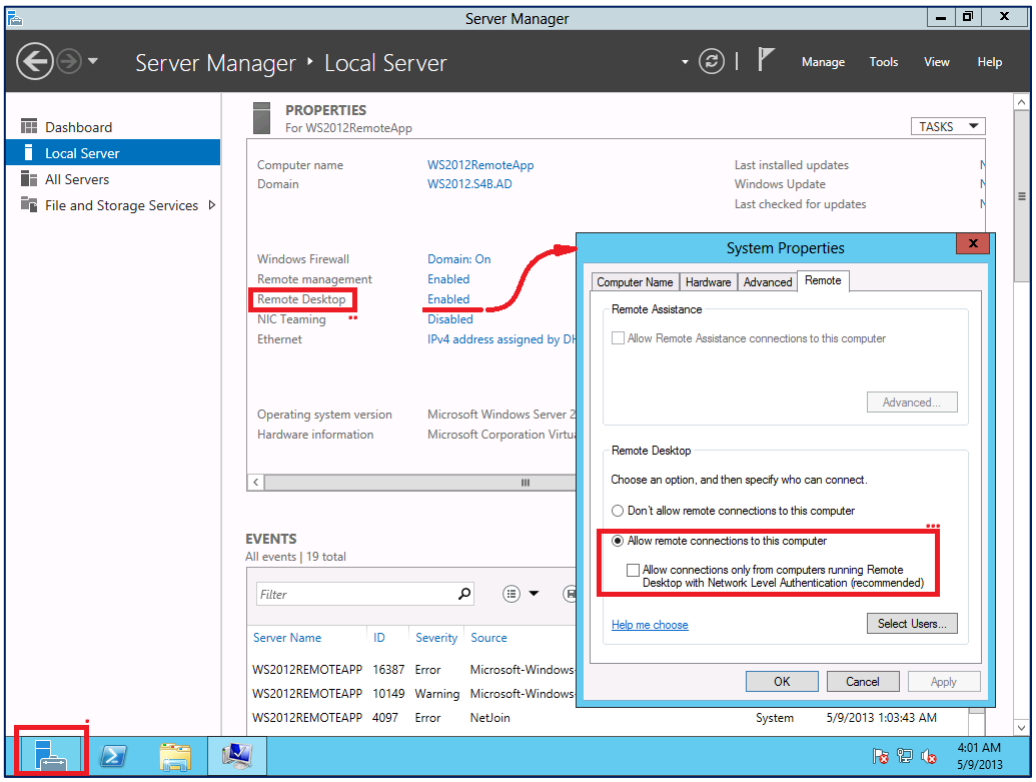
7.4. Setting Up RDP and RDS in Microsoft Windows Server 2012

Earlier in this Guide, Section 6.8 focused on setting up RDP Connector in Microsoft Windows **Server 2008 R2**. In this addendum, we offer some tips to IT personnel concerning how to set up Microsoft Remote Desktop (RDP) and Remote Desktop Services (RDS) in Microsoft Windows **Server 2012**.

This addendum separately describes (1) how to enable the Remote Desktop function in Windows Server 2012, and (2) how to add roles and features in Server Manager of Windows Server 2012, for configuring the Remote Desktop Services on session-based desktop deployment, and RemoteApp program publishing.

7.4.1. How to Enable Remote Desktop in Windows Server 2012

In Microsoft Windows Server 2012, the IT Administrator can simply enable the Remote Desktop function from the **Server Manager**.

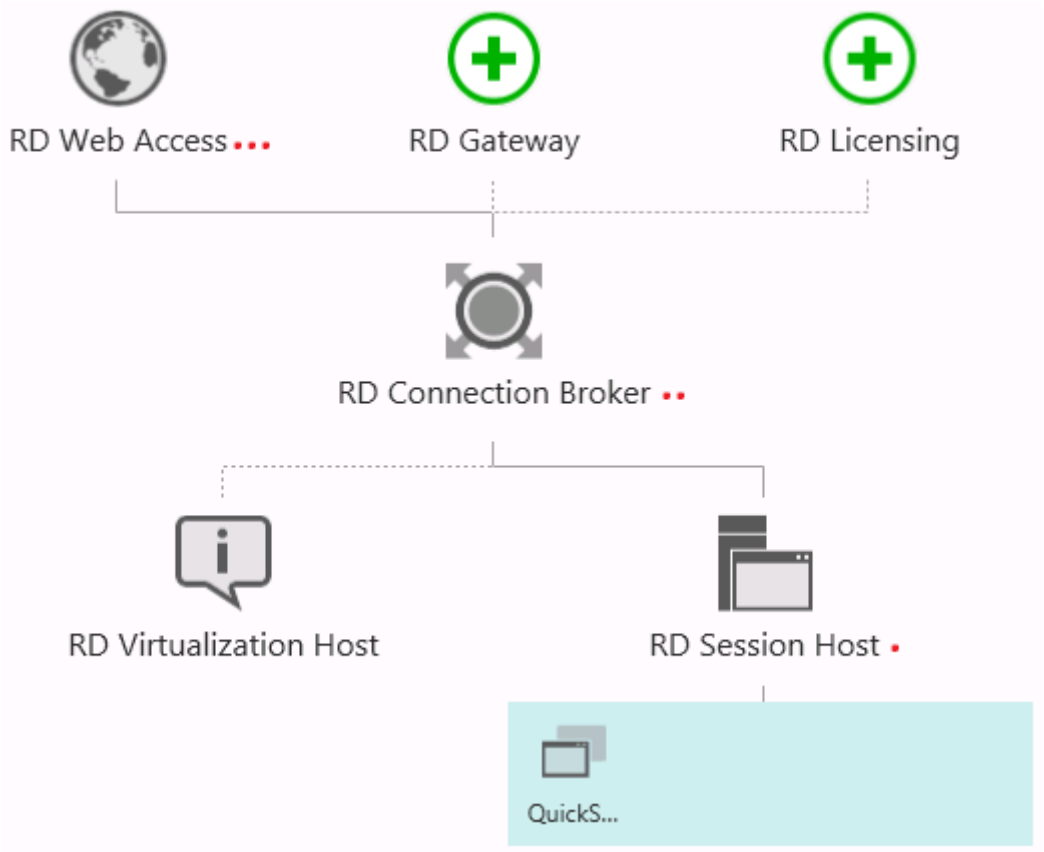


In Microsoft Windows Server 2012, to provide multi-session remote desktop services, and to publish RemoteApp programs, the server(s) settings are configured using the **Remote Desktop Services** feature. As with Microsoft Windows Server 2008 R2, Remote Desktop Session Host (**RDSH**) settings are included into the Remote Desktop Services, in Windows Server 2012.

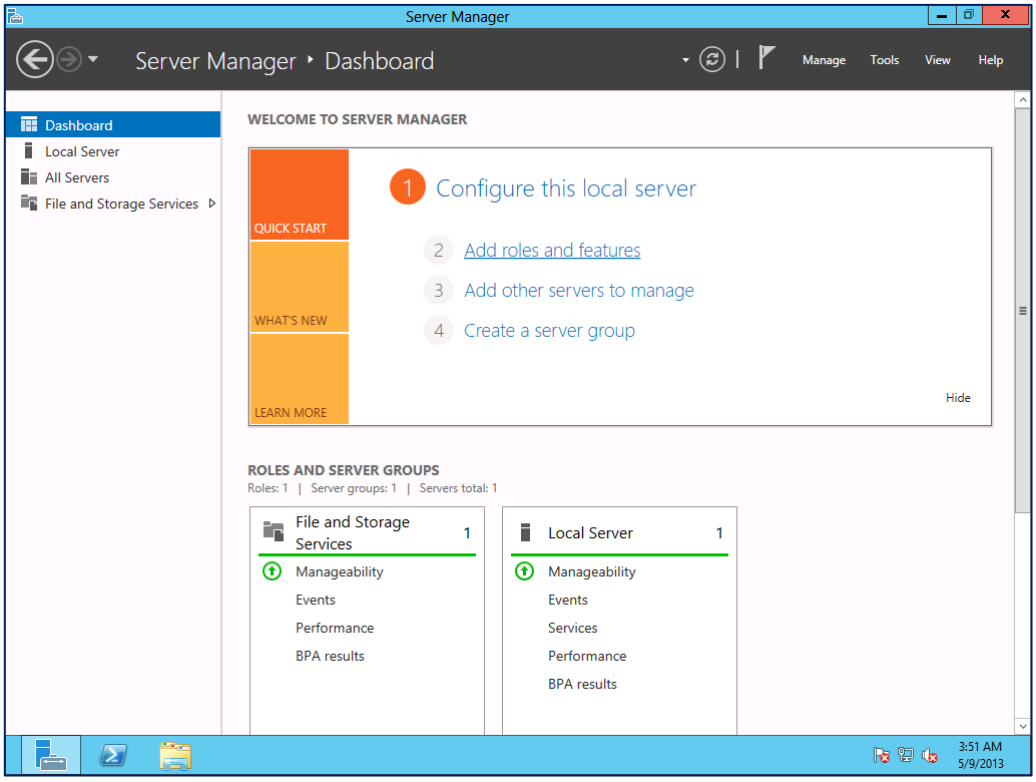
7.4.2. How to Configure Remote Desktop Services

Remote Desktop Services — Components

- The three basic components of Remote Desktop Services in Windows Server 2012 are:
  - **RD Session Host**
  - **RD Connection Broker**
  - **RD Web Access**

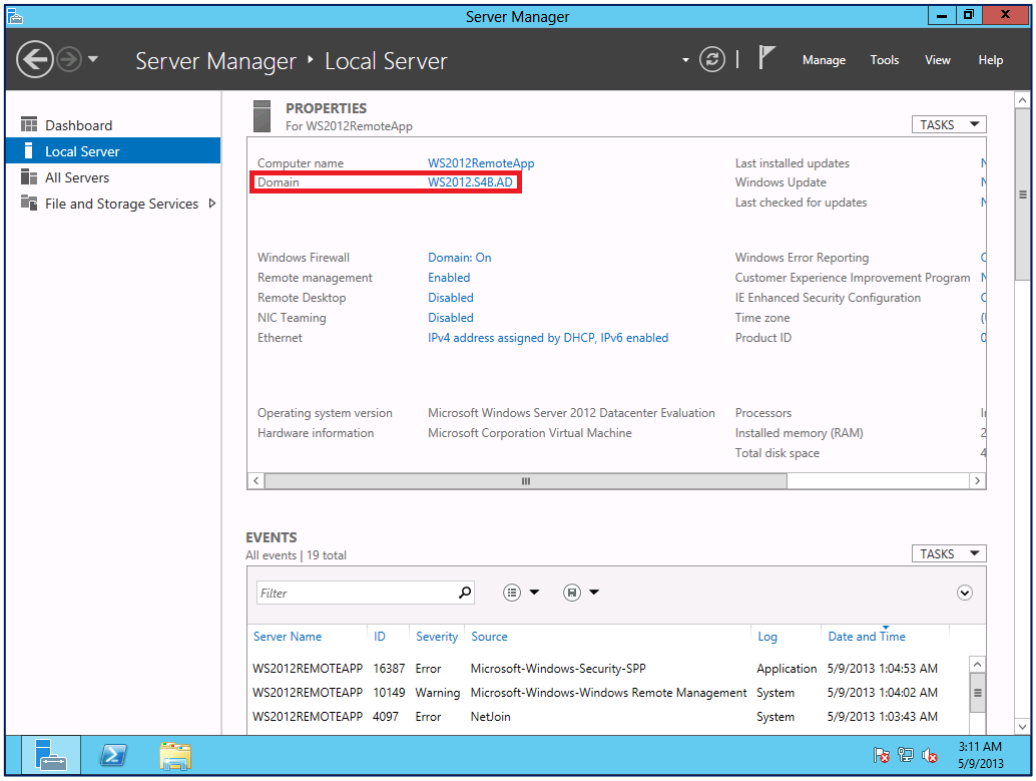


To install any local server role or feature/service, the IT Administrator can start from the **Dashboard** to **Add roles and features**, shown below.



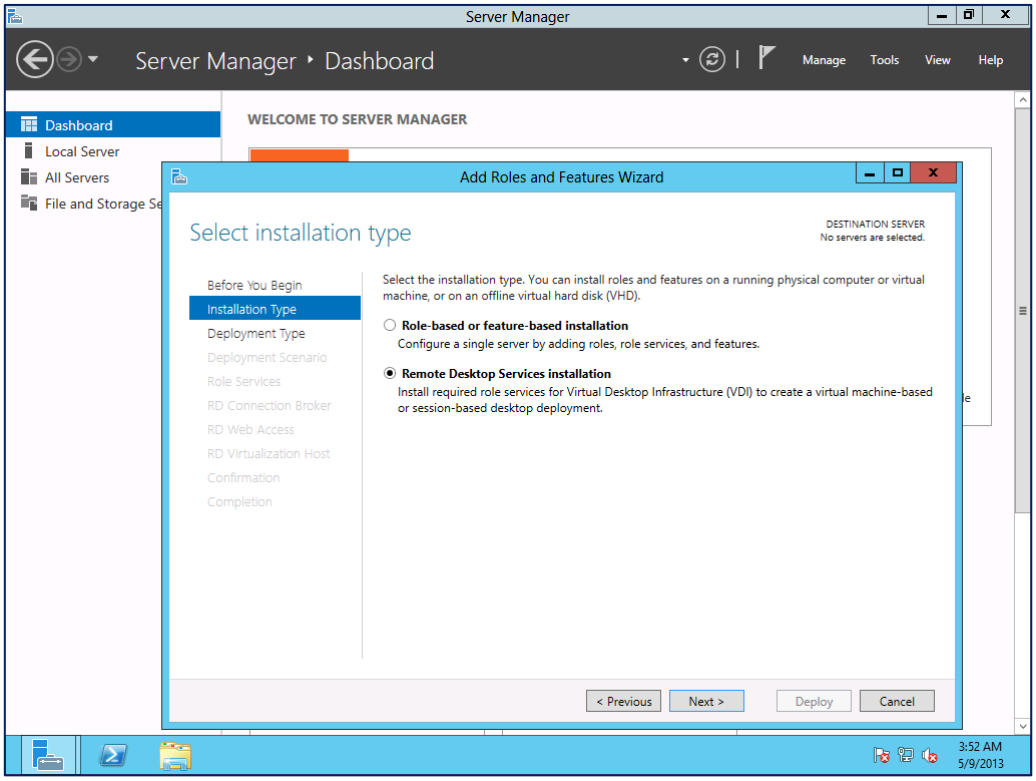
7.4.2.1. Joining the Server to an Active Directory Domain

To set up the Remote Desktop Services in Windows Server 2012, the server must first join an AD Domain (Active Directory Domain), to add Remote Desktop Services role service and features.

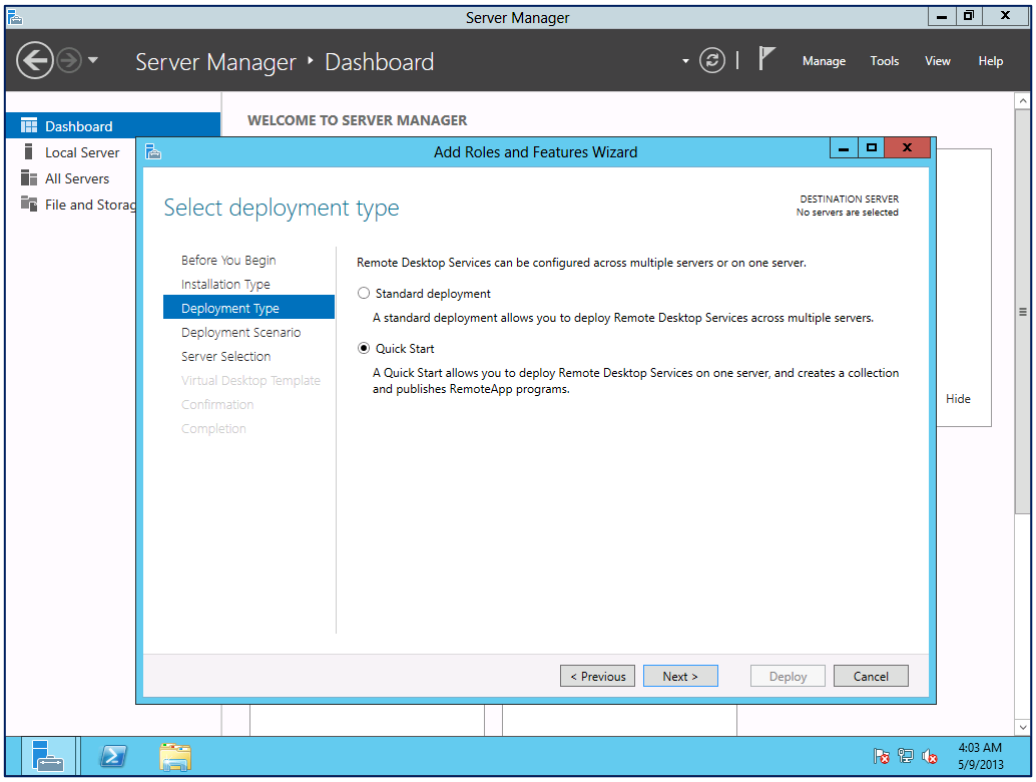


7.4.2.2. Remote Desktop Services Installation

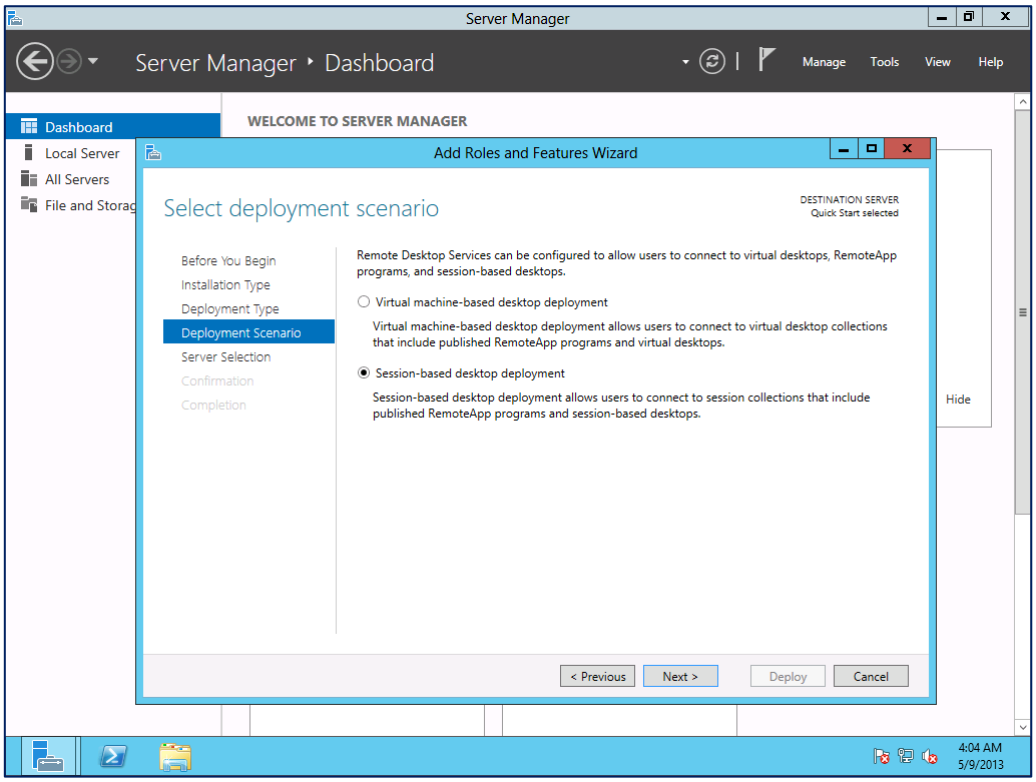
To set up the Remote Desktop Services, the IT Administrator can use the **Add Roles and Features** wizard to select **Remote Desktop Services installation** as shown below.



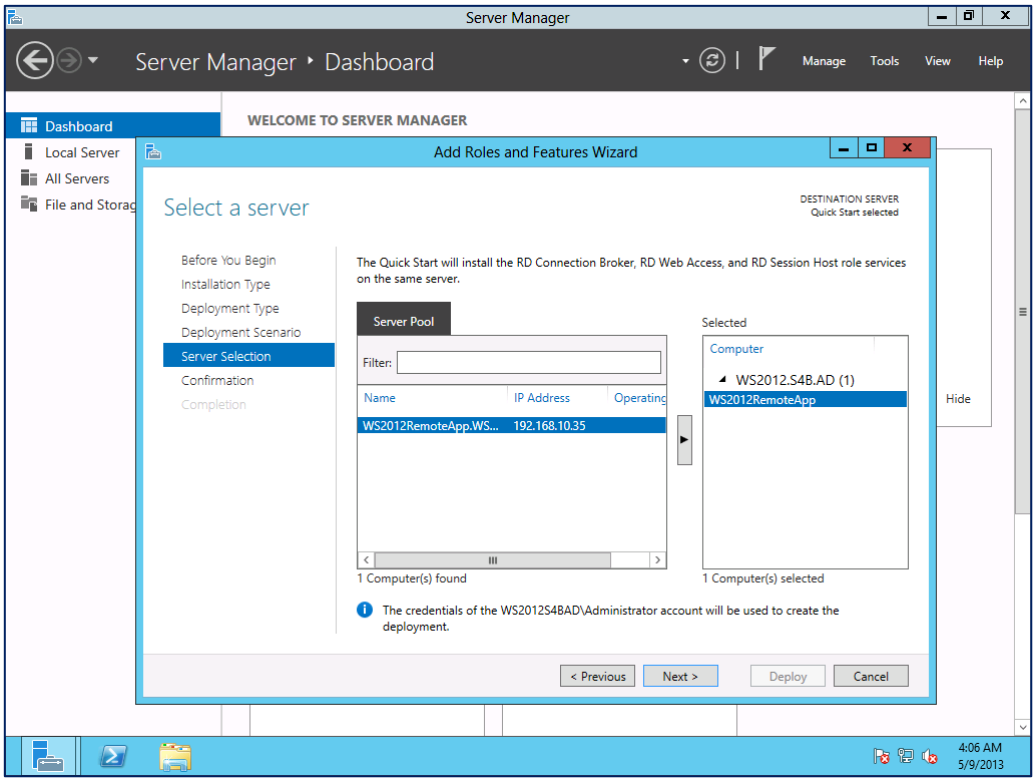
The IT Administrator can choose to have a **Quick Start** to deploy the Remote Desktop Services on the server, and to create Session Collections, and to publish the RemoteApp programs.



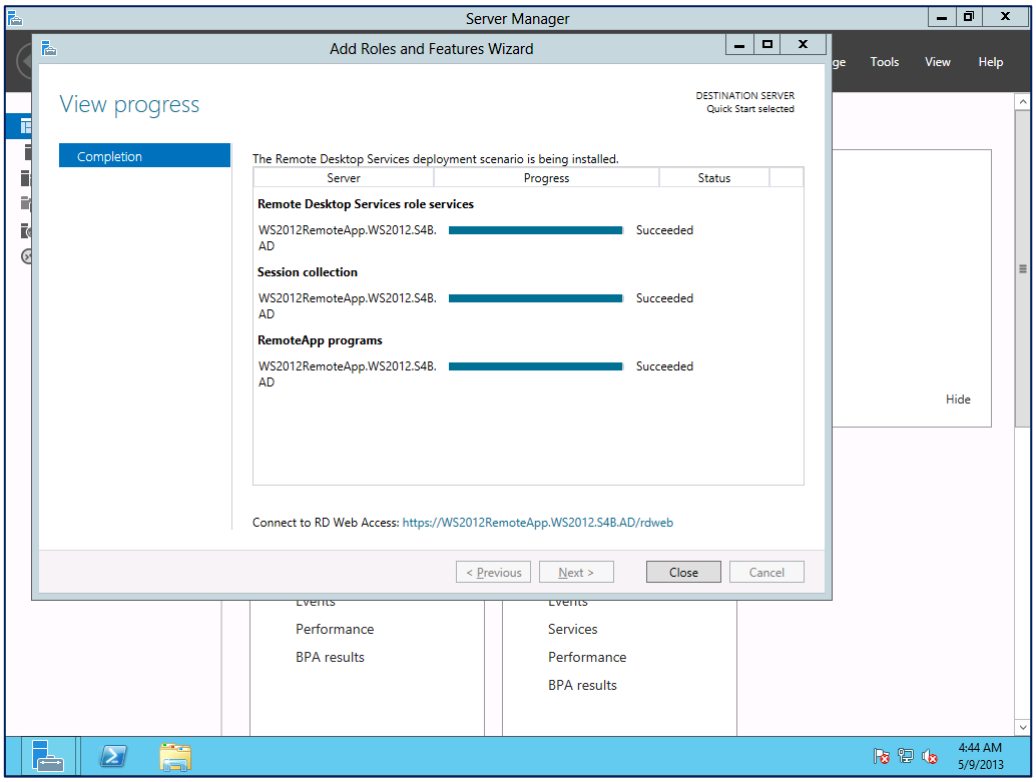
Select **Session-based desktop deployment** to be the **Deployment Scenario** as shown below.



Select a server from **Server Pool** to install, and then **Server Manager** will start to complete the installation.

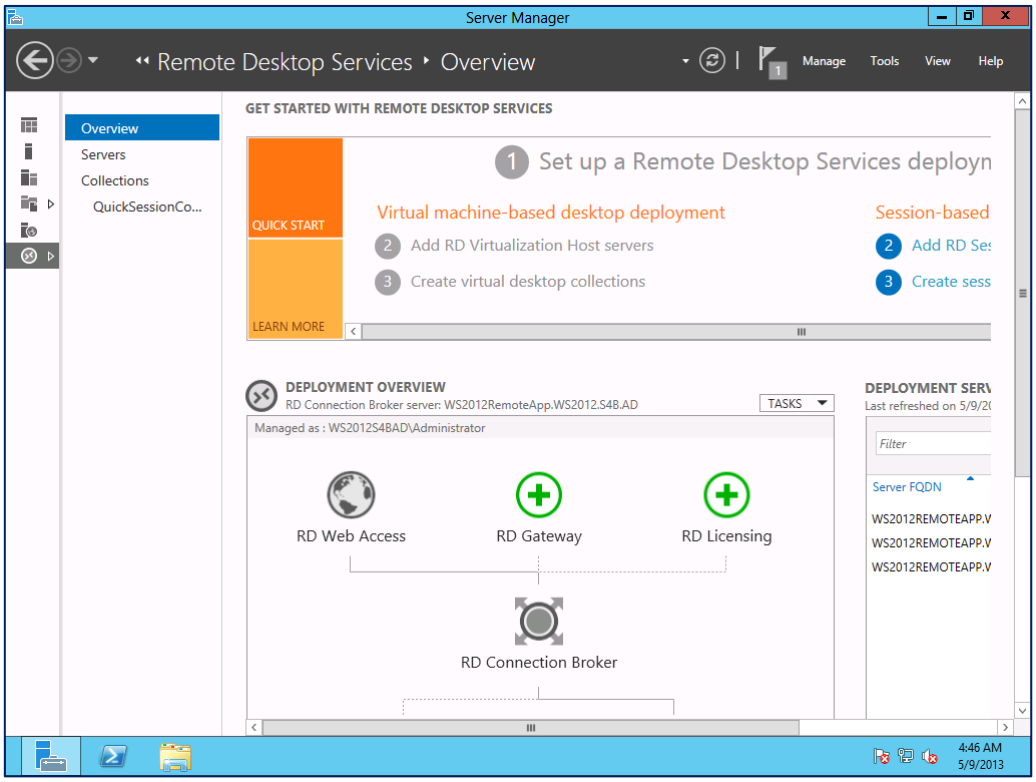


After the restart, the progress/completion status of all three quick deployment services will display.



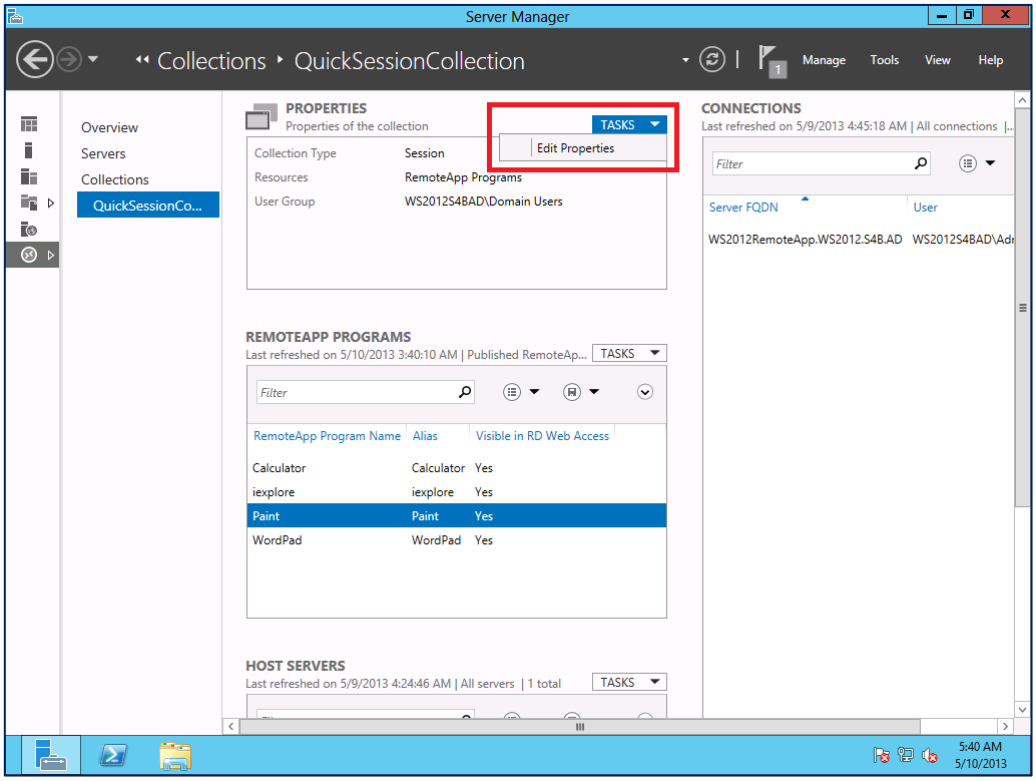
7.4.2.3. Overview of Remote Desktop Services

After the **Remote Desktop Services** have been completely installed, you can find its tab in **Server Manager.** Within the **Remote Desktop Services** tab, the IT Administrator can do **Add RD Session Host servers** and **Create session collections** to deploy.



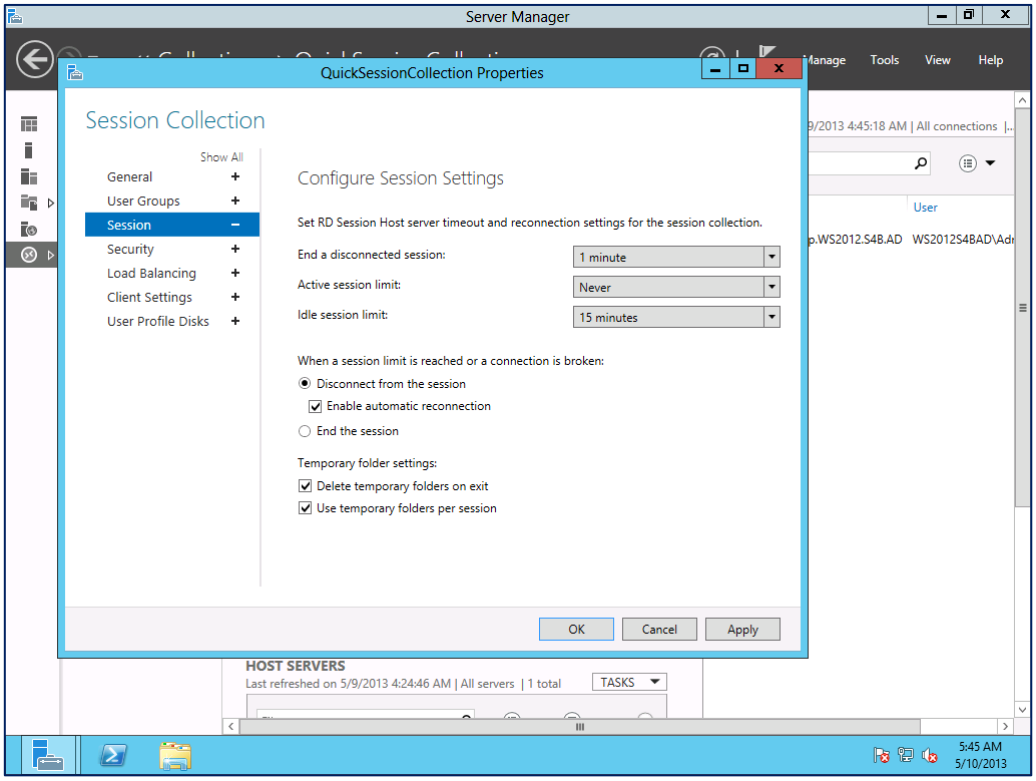
7.4.2.4. Properties Settings of a Session Collection

The IT Administrator can specify the **PROPERTIES** and **REMOTEAPP PROGRAMS** settings of a session collection.

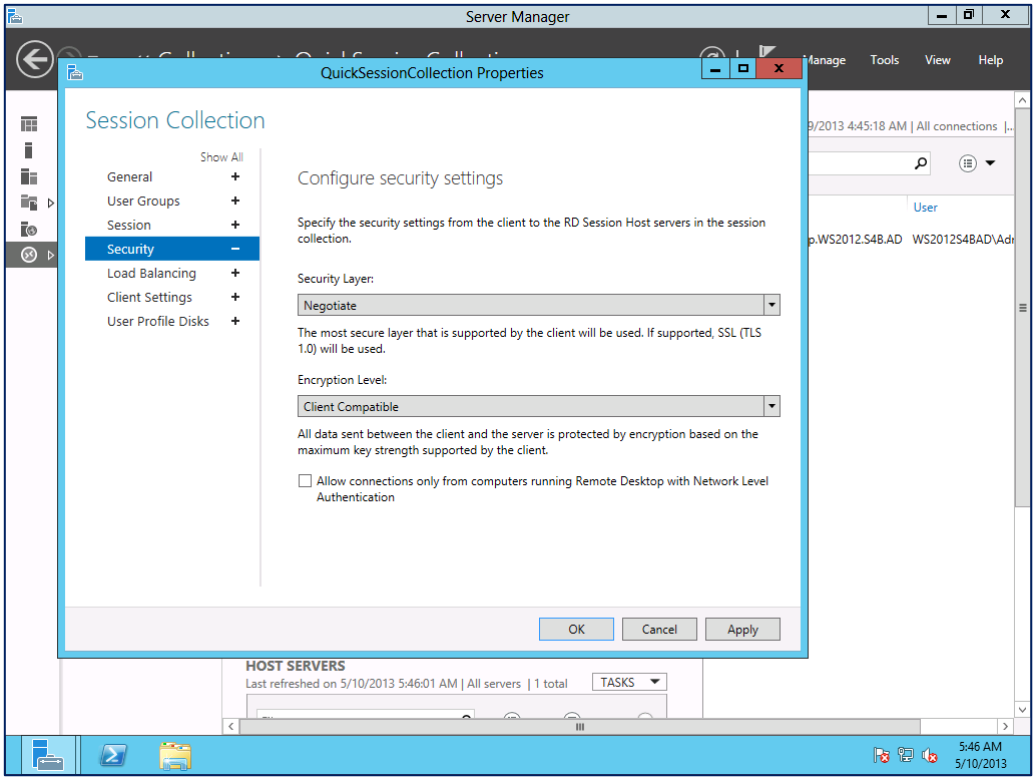


There are seven settings available for a Session Collection, and some suggested options and configuration are listed below as a reference. The example settings we have illustrated below are: **Session**, **Security**, and **Load Balancing**.

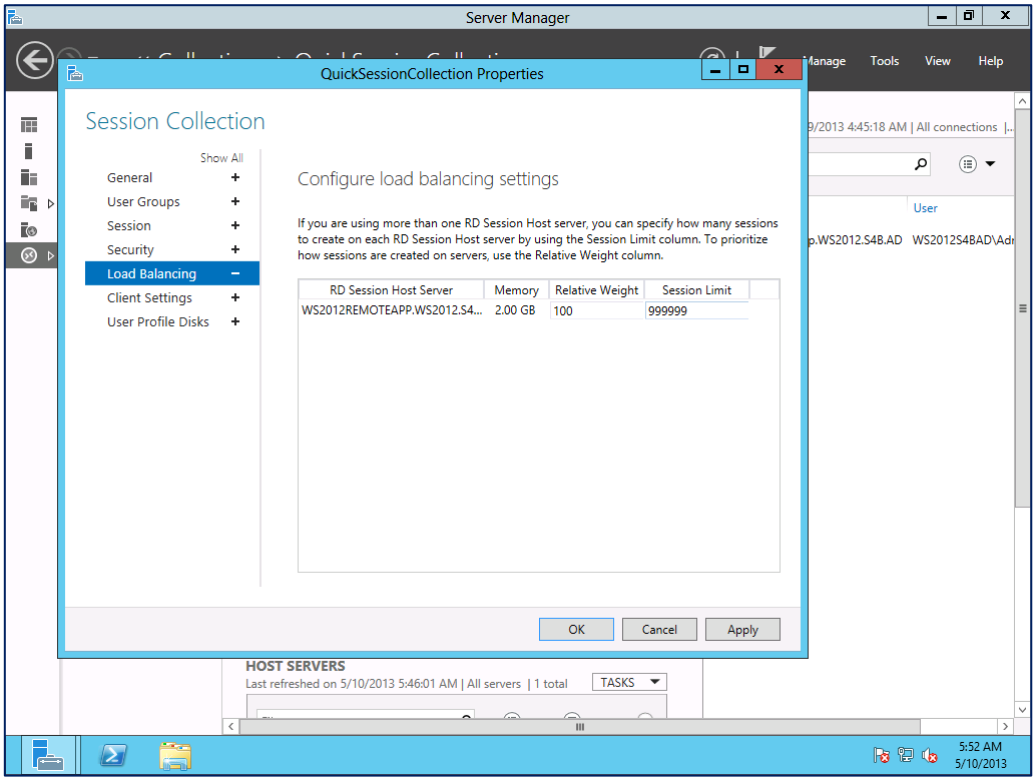
Session:



Security:

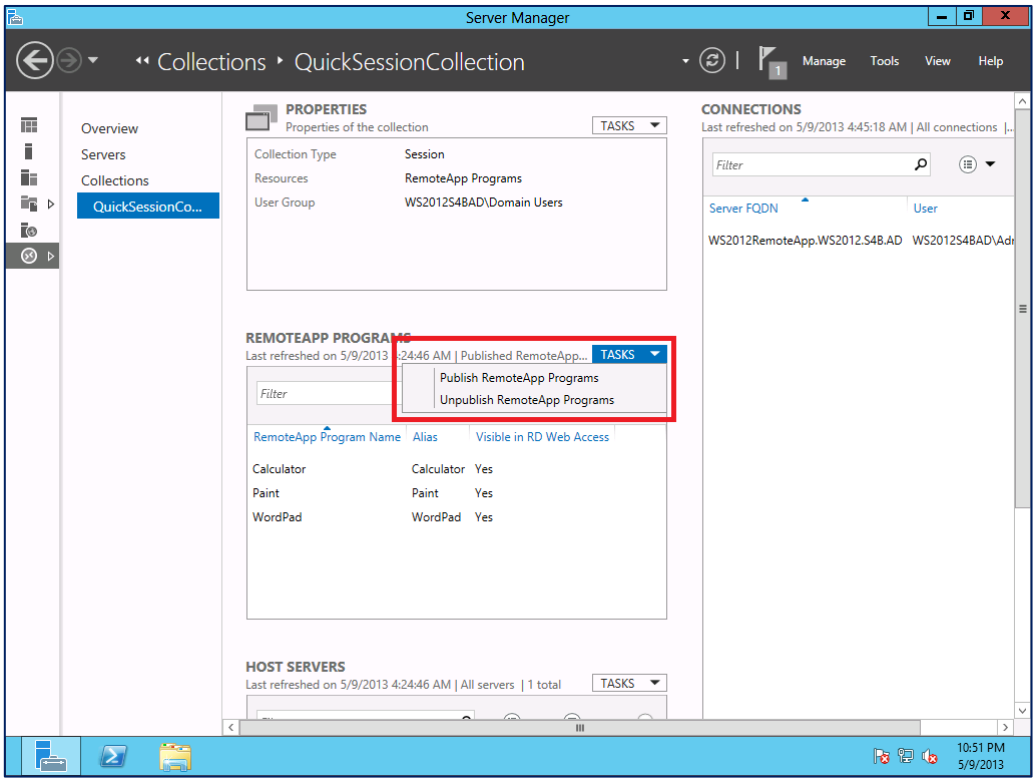


Load Balancing:

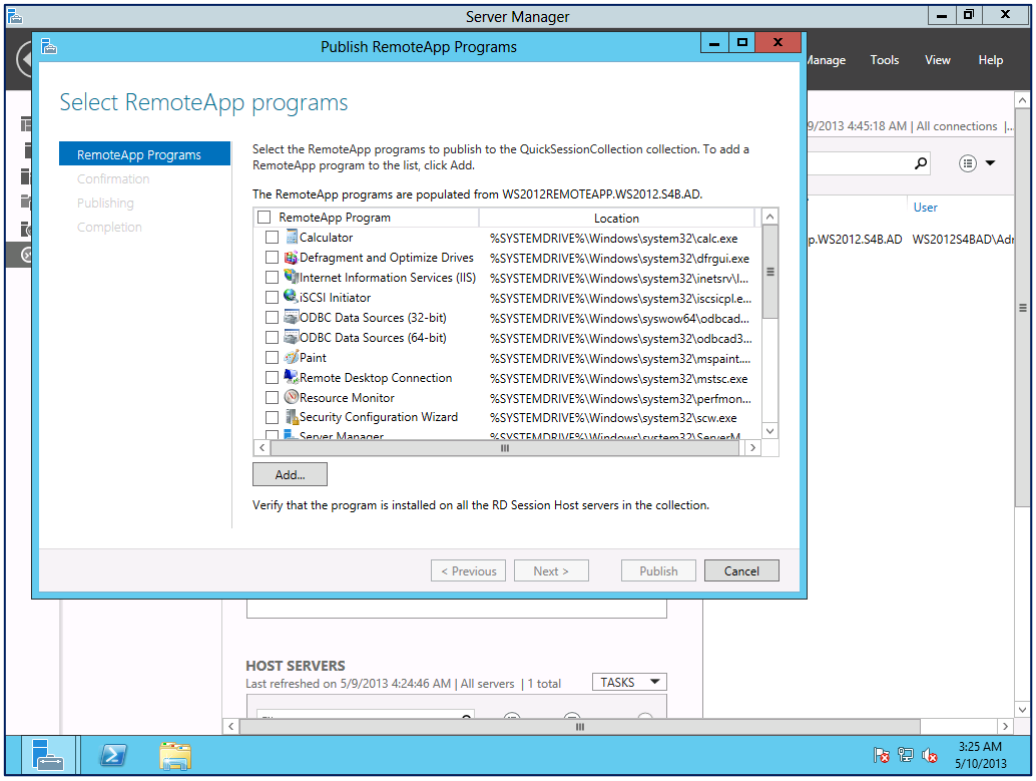


7.4.2.5. Publishing RemoteApp Programs

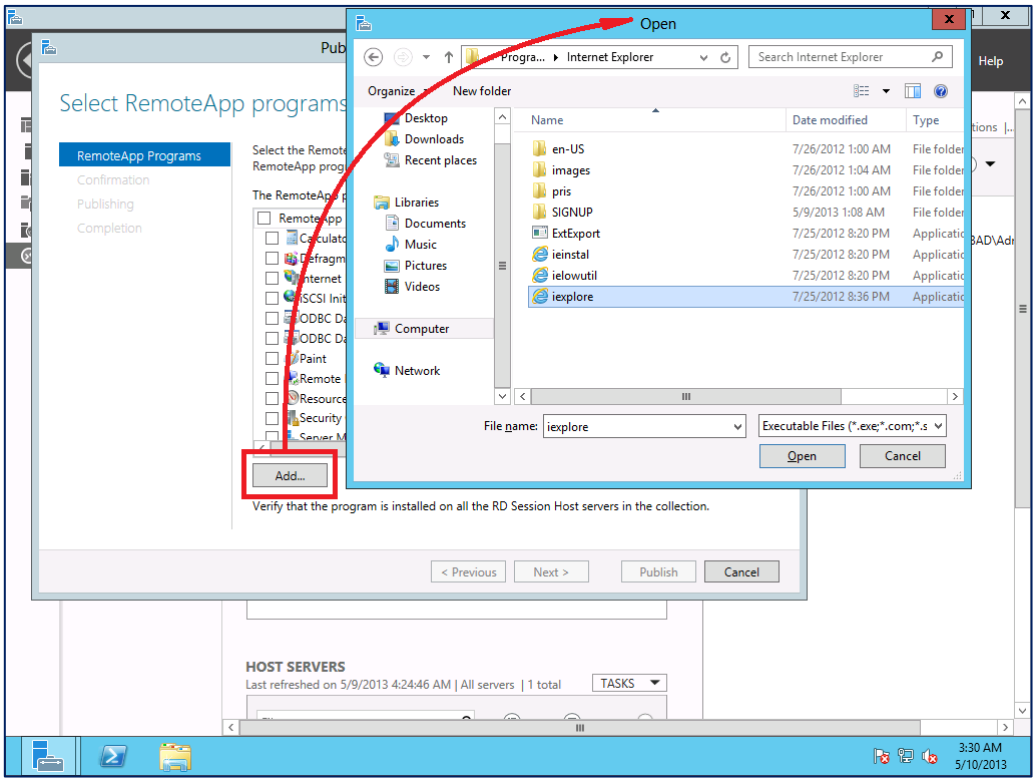
In the pre-set session **QuickSessionCollection**, the IT Administrator can publish the local programs/applications to remote clients (**Publish RemoteApp Programs**), or unpublish them (**Unpublish RemoteApp Programs**). In the example illustration below, we already set the **Calculator**, **Paint**, and **WordPad** programs previously.



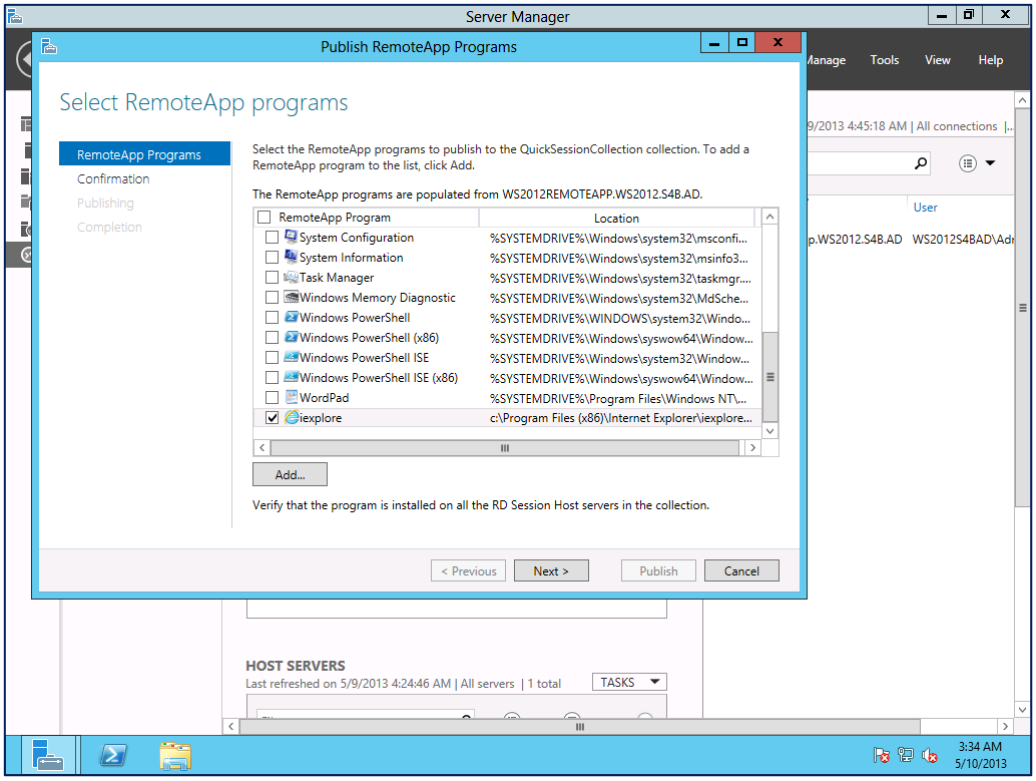
Those programs that are populated in the local server will be listed in the **RemoteApp Program** list:



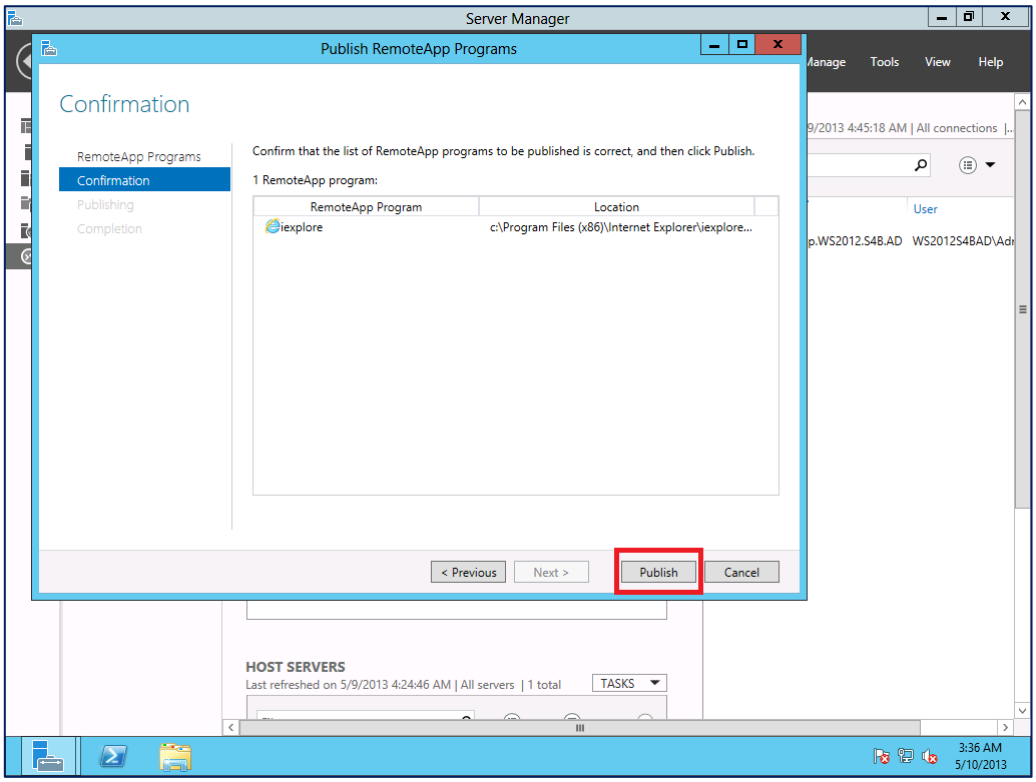
The illustrations below show, for example, how to publish the Internet Explore (**iexplore.exe**) program from the local server to the remote clients. Since IE Explore is not listed in the **RemoteApp Program** list, we selected **Add…** to determine its file path.



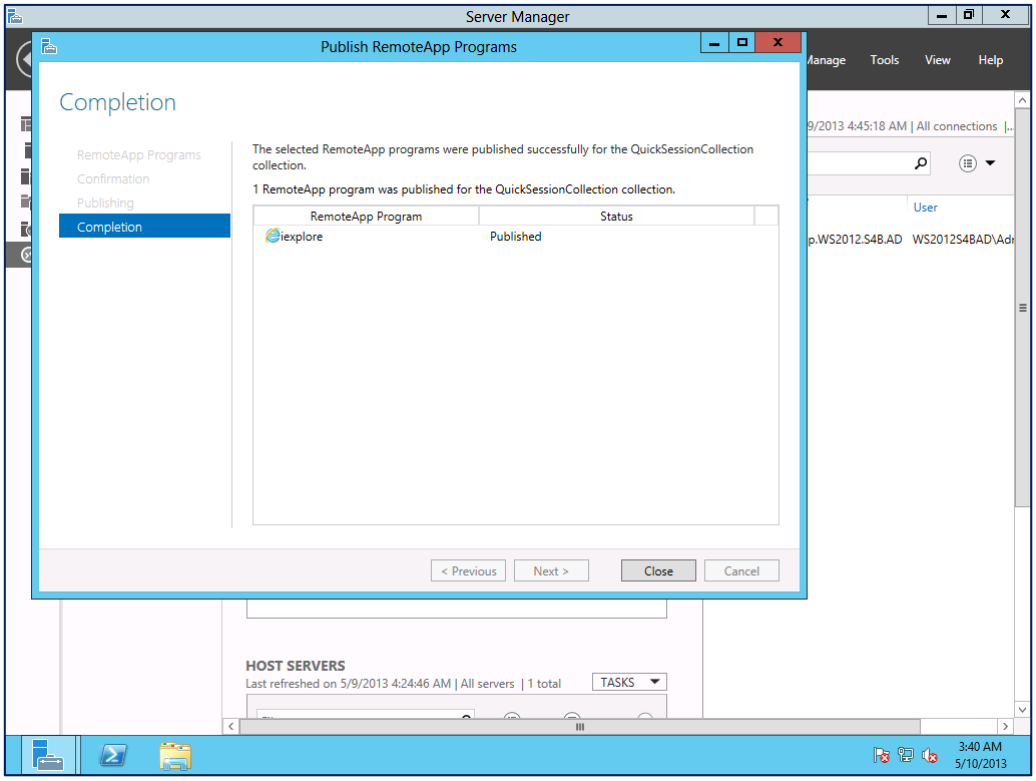
After **iexplore** has been added to the list successfully, then we can check its checkbox, and click **Add…**.



After clicking **Add…**, the selected RemoteApp programs will be listed in a *Confirmation* box. You can then click **Publish** to publish them for access by the Splashtop Center users.



The *Completion* box will then appear and show the status as **Published** to verify that the process is completed and successful.



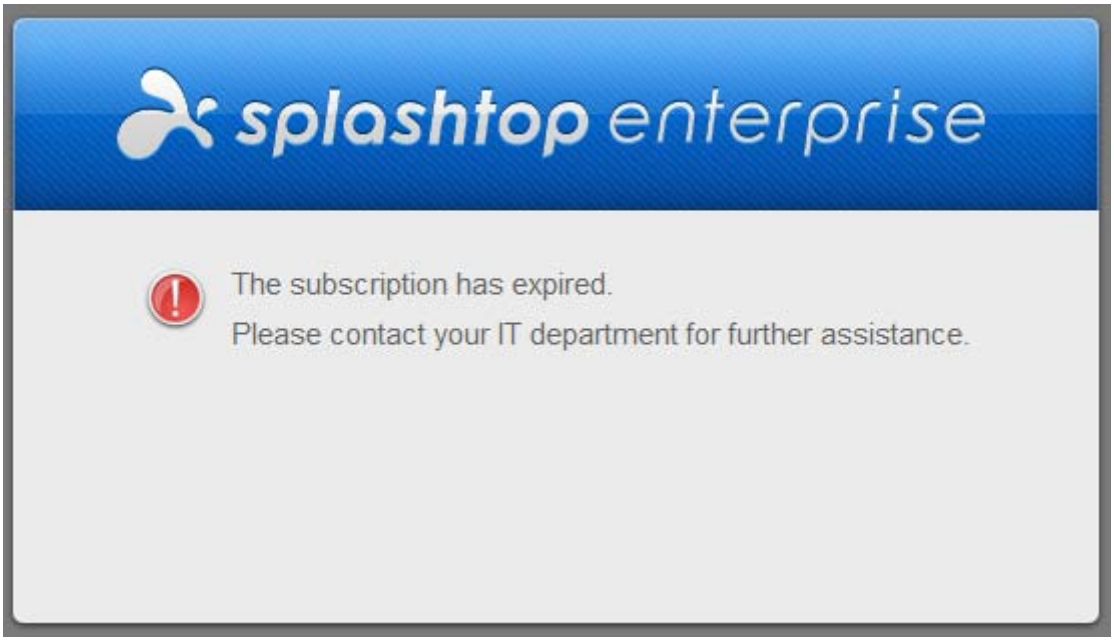
7.5. If Your License Expires

If your Splashtop Center license should happen to expire someday, the behavior will be such that:

- Once Splashtop Center has detected license expiration, it will automatically display the License tab of Settings. The license Status will be shown as "Product Expired." At this point, all other tabs/pages of Splashtop Center will be disabled and cannot be accessed.

- All Streamers and clients will return the message: "The subscription has expired. Please contact your IT department for further assistance."

- You will no longer be able to log in. If any users try to access the online customer portal at the **Splashtop Center Web portal**, it re-directs to a web page displaying a similar message:



7.6. Definitions

7.6.1. Users

In this document, the term "Users" refers to the employees at your company whom you, the IT Administrator, have authorized to use mobile devices to access computers in your company remotely via Splashtop Enterprise. The term "user" is different from the term "IT Administrator" in that the IT Administrator has the power to perform *any* actions in Splashtop Enterprise/Splashtop Center. This Guide is designed for use by the IT Administrator (server/desktop/network administrators), not for general users.

- **Gateway User**
  A Splashtop Center user account that only exists on the Splashtop Center gateway module, which the IT Administrator has added using the Users tab in Settings. This is the typical account for Splashtop Center, unless you use Active Directory.
- **Domain User**
  An Active Directory (AD) user which is managed by the IT Administrator. IT Administrators can integrate these already-existing AD users into Splashtop Center.

A "user" counts as one "Seat" as explained on the next page.

7.6.2. SSL and TLS

The TLS (Transport Layer Security) protocol, and the SSL (Secure Sockets Layer) protocol, are encryptions which are used for providing more secure communication. TLS and SSL authentication relies on client functionality that is built in to some Microsoft Windows operating systems. If a client or server is running an operating system that does not support TLS/SSL, it cannot use TLS/SSL authentication. In addition, for authentication to occur, there must be TCP/IP connectivity between the client and the target server.
In Splashtop Center, **TLS** and **SSL** are choices in the **Encryption** field of the **Email** tab (within the Settings tab).

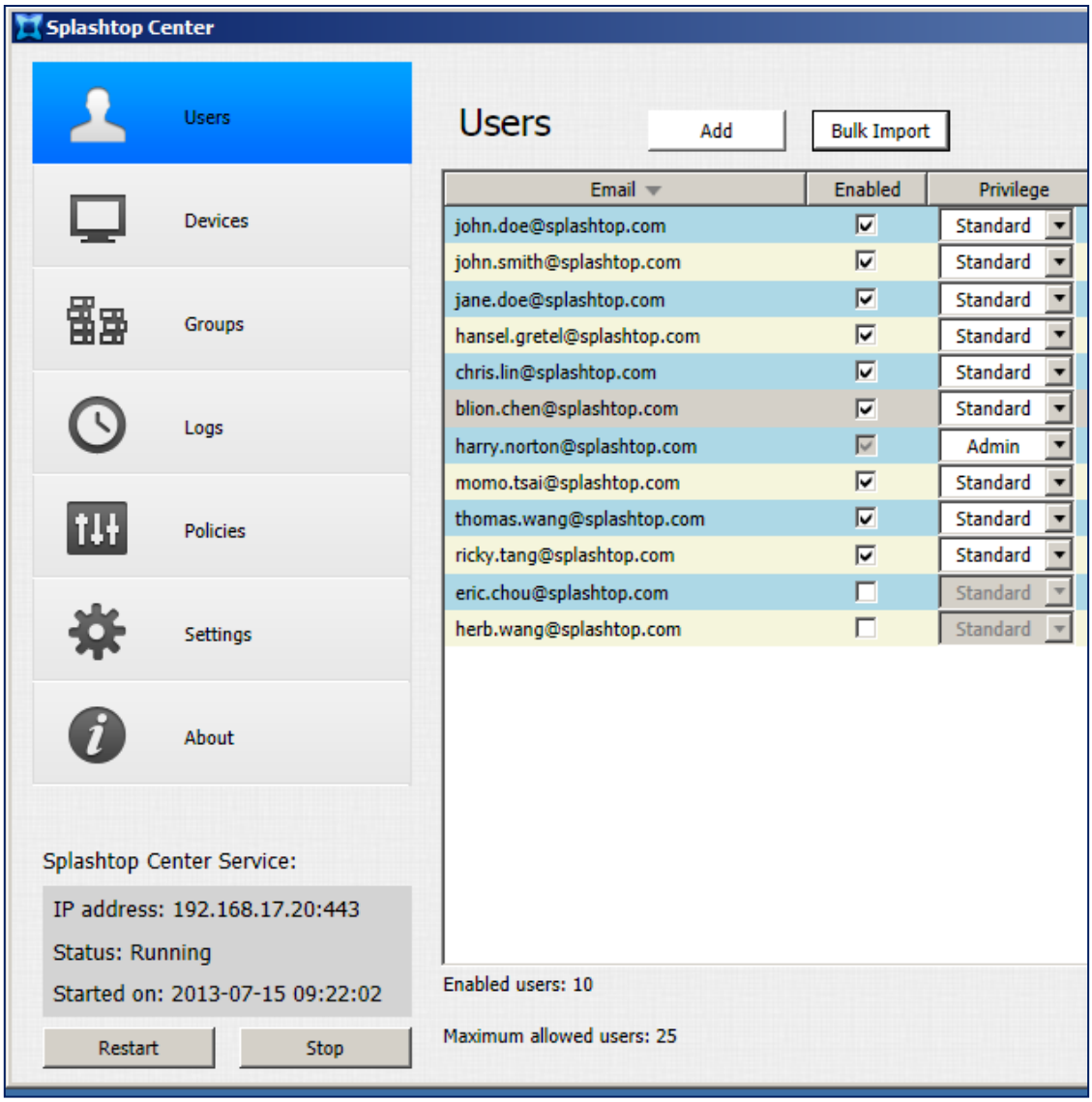
7.6.3. NTLM

In a Windows network, NTLM (**NT L**AN **M**anager) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users, with the ability for a server to authenticate to the client. NTLM uses an encrypted "challenge/response protocol" to authenticate a user, and is widely used in situations where a domain controller is not available or is unreachable. For example, if the server is not joined to a domain, or the user is remotely authenticating over the web.

7.6.4. Seats

Each License Key has a maximum number of Seats associated with it, according to what you have purchased. Each user who is in an **Enabled** status counts as one Seat. You cannot exceed the maximum number of enabled Seats defined in your License agreement. To help you manage this, you can easily enable or disable a user by checking or un-checking the checkbox in the **Enabled** column of the **Users** tab. (The checkbox for the *Administrator* is grayed out because it can never be disabled.)

In the example below, this customer is allowed a maximum of 25 users. There are 12 users listed, but the last 2 are disabled. Therefore, there are only 10 Seats being used here. Fifteen are still available.



In the case that your License Key allows unlimited Seats, the "Maximum Allowed Users" notification shown above will not display.

Normally, each user is entitled to make up to two concurrent Streamer connections/logins — that is, allowed to remote-connect to two different computers running the Streamer at the same time.

So, for example, if your license states that "Maximum Allowed Users" is 25, then your "Maximum Allowed Computers" would be 50.

Although the theoretical "good faith" limit is two concurrent Streamer connections per user, by the same token, Splashtop does not forcefully restrict the exact count for Streamers per user, as long as the total concurrent Streamer logins does not exceed the total Streamer logins allowed (according to the number of Splashtop Center "Seats" you have purchased).

Using the example of 25 Seats, 2 Streamers per Seat, and therefore a maximum of 50 computer connections allowed: Let's say it is 3 AM, and only two of the users are currently using Splashtop Center. Theoretically, each of the two users can log in to 25 computers/Streamers, and this would be allowed because it would not exceed the maximum limit of 50 computers.

Disabling Users to "Free Up" Seats

As mentioned earlier, you can easily enable or disable a user by checking or un-checking the checkbox in the **Enabled** column of the **Users** tab. If you are already at your "Maximum Allowed Users" limit, but you want to add and enable a new user, one solution is to disable one of the existing users. This will "free up" a Seat so you can Enable a different user, and still not exceed your maximum allowed users.

When you add users individually, they will automatically have a status of **Enabled**. However, when you add multiple users via Bulk Import, either Gateway users or Domain (Active Directory) users, they will have a status of **Disabled** by default. After the users have been successfully added, you can manually choose which ones to enable in the **Users** tab initially, which is useful if you are nearing your Seat limit.

NOTE: When you update or restore your License, there is no interruption to your Splashtop Center service, and any remote connections in session at that time will not be affected. Therefore, if you update/restore your License someday, and Splashtop Center detects that there are not enough available Seats at that moment, it will automatically disable users (as a way of continuing service so it will not need to be interrupted). A message will pop up, to notify you of the number of auto-disabled users, and the names of each user.

8. Index

A

About tab
- Splashtop Center ... 120
- Splashtop Streamer ... 43

Activation Code ... 28, 55, 56, 57, 65, 99, 102, 143, 145, 195
- Generating additional codes ... 102

Activation, License Key ... 142
- Offline ... 118
- Online ... 118

Active Directory users ... 58, 59, 67

Adding a new policy
- Security tab ... 95

Adding a remote application ... 132

Adding groups ... 79, 146
- Computers tab ... 82, 148
- Users tab ... 80, 147

Adding users individually ... 53

Adding users with Bulk Import
- Domain (Active Directory) ... 67
- Gateway ... 61

Adding virtual desktop using RDS tab ... 127

Allow everyone to access option ... 81, 132

Allow password to be saved on clients (Policy Settings) ... 90

Application, remote
- Adding apps using the RDS tab ... 132
- Setting up a remote application from RD server with RD Host configured ... 181

Assign License button ... 116

Automatically send email to users for account/password setup and device authentication option (Email tab) ... 56, 107, 108, 110, 143

B

Backup tab ... 114, 142
- **Restore all settings from file** button ... 115
- **Save all settings to file** button ... 114

Bandwidth and Scalability (RDP Connector ... 164

Bulk Import (Users tab)
- Activation code ... 65
- CSV file for import ... 61, 67
- Domain AD users ... 67
- Exporting/saving log messages ... 64
- Gateway users ... 61
- User policy ... 65

C

Changing Password (Gateway users) ... 123

Changing ports (Splashtop Center) ... 140

Clear button (Email tab) ... 109

Clients tab (Devices) ... 76

Computers tab (Devices) ... 74

Configurable Shortcuts and Gamepad icon (on Toolbar of Client app) ... 35

Connection
- How to make a remote connection ... 32
- Options on Client device Toolbar ... 34

Copy all to clipboard button ... 57

Copyright information ... 6

CSG, information ... 35

Customer Portal ... 121
- Login ... 122

D

Deactivating a client device 76, 144
Default (Groups tab) 79
Default Policy, defined 88
Definitions of terms 216
Deleting a group 149
Deleting a policy 97
Deployment
in a private network 49
in the DMZ 47
Physical vs. Virtual 49
Devices tab 74
Clients tab 76
Computers tab 74
Disable Device Activation 145
Disabling users automatically during License update 119, 218
Disconnecting a remote connection (from the Client device) 36
DMZ (de-militarized zone) deployment 47
Domain (Active Directory) users 53, 58, 59, 68
Domain Name, Switching (Bulk Import) 69
Download tab of Web portal 124

E

Edit Email Templates button 110
Edit List (MAC address filtering for Policies) 90, 96
Editing a group 150
Editing an existing policy 96
Email tab (Settings tab) 107, 141
Email Template window 110
Enable auto launch option 41
Enable blank screen option 42
Enable Device Activation 55, 99, 145
Enable remote access from external network (Policy Settings) 93
Enable Schedule for Streamer Update checkbox (Software Update) 113
Enabling and Disabling Users 51, 52, 218
Encryption field (Email tab) 108, 216
EULA for Splashtop Streamer 38
Expired license/subscription 215
Exporting/saving log messages of Bulk Import users 64

F

Force SSL on Local LAN connections (Security tab) 105
Force Streamer Update button (Software Update) 111

G

Gateway user passwords 123
Gateway users 53
General tab (Settings tab) 98, 140, 145
Gestures (Hints screen) 33
Get Help button in Splashtop Center 50
Glossary 216
Groups tab 79, 151
Default group 79

H

Hardware Requirements, Splashtop Center 14
Help screens on Client device 36
Help tab of Web portal 139
Hibernation/Sleep mode 153, 156
Hide Streamer UI from non-Admin users option (Policy Settings) 93
High Availability
Splashtop Server unexpectedly off-line 162
Typical usage 162
Hints screen
Gestures on mobile device 33

Toolbar icons on mobile device 34
http protocol vs. **https** (port 80) 141

I

Importing users with Bulk Import
Domain (Active Directory) 68
Gateway users 61
Installing
Splashtop Center 19
Splashtop Enterprise Client App 26
Splashtop Streamer 37
Virtual Display driver 157
Insufficient disk space 24
Internet Firewall
for a private network 49
for DMZ 48
Intranet Firewall (for HTTPS) 48
Invitation Email 56, 107, 110
if not enabled 57
iSCSI disk partition 162

K

Keyboard
Opening on Client device during remote connection 34

L

License expired 215
License Key 142
Maximum number of activations 117
Offline activation 118
Online activation 118
Trial account 20
License Manager 118
License tab (Settings)
Assign License button 116
Release License button 116
Log files showing remote connection status/history
Saving to CSV format 85
Logs tab 84
Export button 85
Show Session Log field 85

M

MAC Address filtering (Policy Settings) 90
Manage Group dialog box 150
Maximum Allowed Users 217
Maximum frame rate (Policy Settings) 94
Microsoft NET Framework 24
Mode Switching (Policy Settings) 92
Modify button (Software Update) 111

N

Network Requirements 16
NTLM authentication 216

O

Offline activation (License Key) 118
Off-line Splashtop Center Server unexpectedly 162
Online activation (License Key) 118
Others tab in Policy Settings 94
Overview 7, 192

P

Password field in Email tab (of Settings tab) 109
Password for Gateway users, changing 123
Password tab of Web portal 123
PFX file format (SSL Certificate) 106

Physical vs. Virtual deployment 49
Policies
Allow password to be saved on clients 96
Bulk Import (Users tab)
Exporting/saving log messages 64
Default Policy defined 88
Enable remote access from external network 93
MAC Address filtering 90
Maximum frame rate 94
Mode Switching 92
Security tab 89
Session idle timeout 93
Port Error message 24
Port field (Email tab) 108
Port number, changing 42, 140
Preferred Display Resolution
RDP Desktop) 136
RDS Server 129
Preset Password option 55
Private network deployment 48

R

RDP Connector 163
Adding remote application using RDS tab 132
Adding virtual desktop using RDS tab 126
Network Level Authentication 168
OS compatibility 164
RDP Desktop tab 169
showing correlation with Devices 171
RDS tab 126, 177, 188
Scalability 164
Set up remote application from RD Server with RD Session Host configured 181
Set up remote desktop for RDP-enabled computer 165
Set up remote desktop from RD Server with RD Session Host configured 173
RDP Desktop 135
Adding RDP-enabled computer 170
Fields in Add dialog, defined 135
RDP Desktop tab of Web portal 135
RDS tab of Web portal 127
Re-installing Splashtop Center 142
Release License button 116
Remote Desktop
Authentication Method 176
Configuring on Server 2012 200
Enabling on Server 2012 199
RD Session Host 173
Services, joining Active Directory Domain 202
Setting up a remote application 132, 181
Turning on RDP Remote Desktop 165, 167
Remote Desktop Services, defined 126
RemoteApp Program
Publishing 210
Settings 207
Request Additional Activation Codes function 102
Require Streamer blank screen when connected (Policy Settings) 93
Require Streamer Windows login credential when connecting option (Policy Settings) 90
Resolution settings (on Client device computer list) 32
Restarting Splashtop Center 50
Restore all settings from file button (Backup tab) 115
Restore to Default button
Email templates 110
Policy 89

S

Save all settings to file button (Backup tab) 114
Seats
Defined 217
Disabling and Enabling 218

in combination with logged-in Streamers 218
Secure Relay/Secured Socket Layer (SSL) 13
Security tab (Settings tab) 103
Security tab for Add/Edit Policy 89
Sender/From field (Email tab) 108
Server field (Email tab) 108
Session idle timeout (Policy Settings) 93
Settings tab 98
in Splashtop Center console window 98
Backup tab 114
Restore all settings from file button 115
Save all settings to file button 114
Email tab 107
General tab 98
in Splashtop Streamer dialog box 41
License tab 116
Security tab 103
Export button 105
Force SSL on Local LAN connections 105
Generate button 104
Import button 103
Remove button 105
Software Update tab 111
Enable Schedule for Streamer Update checkbox 113
Force Streamer Update button 112
Modify button 111
Shared access to group of computers 80
Show Activation Status option 102
Show Session Log field 85
Sleep/Hibernation mode 153, 156
Software Update tab
Enable Schedule for Streamer Update checkbox 113
Force Streamer Update button 111
Software Update tab (Settings tab) 111
Splashtop Center
About tab 120
Adding a new policy 95
Adding groups 79
Computers tab 82
Users tab 80
Adding users 51
Bandwidth Requirements 16
Checklist for setup 194
Clients tab 76
Computers tab 74
Defined 8, 12, 193
Deleting a policy 97
Deployment as physical vs. virtual 49
Deployment in the DMZ 47
Devices tab 74
Downloading trial version 19
Editing an existing policy 96
Enabling and Disabling users 51, 52
Features 9
Get Help button 50
Groups tab 79, 151
Hardware/Software Requirements 14
Installing 19
Trouble-shooting 24
Internet Firewall
for a private network 49
for DMZ 48
Intranet Firewall for HTTPS 48
License expired 215
License Key 20
Logs tab 84
Export 85
Show Session Log field 85
Making a remote connection 32
Policies tab 88
Default Policy defined 88
Port number, changing 140
Private network deployment 48
RDP and RDS on Server 2012 199
RDP Desktop 135
Re-installing 142

Restarting 50
Scalability 16
Server unexpectedly off-line 162
Settings tab 98
Backup tab 114
Email tab 107
General tab 98
License tab 116
Security tab 103
Software Update tab 111
SSL Certificate 196
Stopping 50
Upgrading 23
URL for Web portal 121
Users tab 51
Web portal 121
Splashtop Center URL field
in app for mobile device 143
in Email tab 110, 141
in Status tab of Streamer 140
Splashtop Enterprise
Defined 7, 8, 192
FAQ and online support 18
Installing the Client App (on mobile device) 26
Wake-on-LAN (WoL) 152
Mac 154
Virtual Display driver 157
Windows 153
Web site 11
Splashtop Enterprise App
Activating 29
Client (Mobile Device) Requirements 15
Defined 192
Installing 26
Settings/Options on iPad 30
Splashtop Streamer
About tab 43
Advanced tab 42, 43
Defined 8, 193
Enable auto launch 41
Enable blank screen 42
End User License Agreement 38
Hide Streamer UI from non-Admin users 93
Installing 37
Trouble-shooting 45
Port number, changing 42
Require Streamer blank screen when connected 93
Require Streamer Windows login credential when connecting 90
Requirements for Windows and Mac 17
Security tab 42
Settings tab 41
SRServer.exe 44
Status tab 39, 140
System power options 41
Terminal Services 44
User Account Control (UAC) 46
Splashtop Whiteboard icon (on Toolbar of Client app) 35
SRServer.exe
Splashtop Streamer 44
SSL (Secure Socket Layer)
Defined 216
Encryption field of Email tab 108
SSL Certificate 103
Converting a certificate to PFX format 106
SSL Certificate, installing 196
from Nexus 7 tablet internal storage 197
on Android tablet or Android phone 196
on iPad or iPhone 197
on Mac PC or notebook 197
SSL Encryption
Force SSL on local LAN connections 13
Status tab
Splashtop Streamer 39
Stay in Splashtop Center mode only (Policies) 92
Stopping Splashtop Center 50

Streamer 92
System power options..... 41
System Requirements 14

T

Templates for automatic Email..... 110
Restore to Default..... 110
Terminal Services
Splashtop Streamer 44
Terms defined (Glossary) 216
Terms of Service 38, 120
TLS (Transport Layer Security)
Defined 216
Encryption field of Email tab 108
Toolbar
Configurable Shortcuts and Gamepad icon..... 35
Hints screen, icons identified..... 34
Opening on Client device during remote connection..... 34
Splashtop Whiteboard icon 35
Trial account setup for Splashtop Center..... 19

U

Updating to a newer version of Splashtop Streamer..... 112
Upgrading Splashtop Center..... 23
URL for Web portal (Customer Portal) 121
User Account Control (UAC)..... 46, 198
User field in Email tab (SMTP account)..... 109
Users
Active Directory users 58, 59
Adding Domain users 58, 59
Adding Gateway users..... 53
Defined 216
Tab in console window..... 51
Users List (Bulk Import, Domain Users)..... 70
Users tab..... 51

V

Verify button (Email tab) 109
Version number of Splashtop Center (About tab).....120
Version number of Splashtop Streamer (About tab) 43
View Details (Policy).....96
Virtual desktop, RDS tab 126
Virtual Display driver 157
Virtual vs. Physical deployment 49
Virtual witness disk.....162

W

Wake-on-LAN (WoL) 152
App and Streamer on different sub-nets.....159, 160
App and Streamer on same sub-net.....158
Mac 154
On-line Streamer and Off-line Streamer on same sub-net
.....160
Splashtop Center and Streamer on same sub-net.....159
Virtual Display driver 157
Windows 153
Web pages for Splashtop Enterprise 11, 120
Web portal 121
Download tab.....124
Help tab.....139
How to determine URL for access 121
Logging in as different User Types.....122
Password tab 123
RDP Desktop tab.....135, 169
RDS tab.....127
Windows Server 2012
Setting up RDP and RDS 199
Witness disk.....162

Z

ZenDesk, Downloading Splashtop Center and getting trial account License Key 19, 22