ThinRDP Server

HTML5 Remote Desktop Client

Administrator's guide

Table of Contents

Mobile devices 63

Integrating ThinRDP 73

Advanced Settings 155

User's guide 203

1 About this document

On this help file you will find information about ThinRDP Server. This document is intended for administrators to set up and configure ThinRDP.
Check the "Getting started" section and follow the instructions to quickly install and configure ThinRDP Server.
Look into the "Advanced Settings" section to learn how you can better take advantage of the many features ThinRDP has to offer.

About us:

Cybele Software is a leading provider of software solutions that enable companies to extend their existing technology foundation by integrating with trend-setting technology innovations. Whether you want to improve the user interface for a mainframe application or need to enable remote Web access to Windows desktop applications, Cybele Software has a solution for you.
Since 2004, we have enabled companies to bridge the gap between cutting-edge technologies and proven client/server and mainframe systems. Our team of experienced developers strives to deliver flexible software solutions that increase the efficiency of and usability of legacy systems and data.

Cybele Software products are designed to provide the simplest implementation pathways possible, while ensuring the integrity and security of your existing environment. Our track record of delivering on these commitments is evidenced through our rapidly-expanding, global customer base.

You can find out more about our products and our company on our website at www.cybelesoft.com

2 Introduction

ThinRDP is a web application that allows users to **access** their **Windows Desktops remotely** from any device of their preference.

Why ThinRDP?

1. Users can have access to all of their remote programs, documents, files, and network resources from anywhere as if they were in front of the remote machine.

2. It doesn't matter which device they have. It can be an iPhone, iPad, Android tablet, ChromeBook or any other device with a HTLM5 compliant browser.

3. In a local area network (LAN), ThinRDP enables secure access to any PC through a single public IP address.

Technology details:

The application takes advantage of the **HTML5** technology and interoperates with almost every platform and browser.
ThinRDP does not require Flash, Java, ActiveX, Silverlight or any other setup on the end-user side and can be used from almost any device.

Furthermore, ThinRDP grants access to applications and desktops running on Windows Terminal Services. You can even remote into RDS / VDI platforms, such as session-based applications or virtual desktops.

Thanks to ThinRDP's cross-browser, cross-platform capability, Windows, Mac OS X, Linux, Android and iOS users can remote log in into Windows desktops and work with single applications through their favorite browser. The application supports Internet Explorer 9, Firefox, Chrome, Safari, and other HTML5 capable web browsers. IE8 and earlier versions may be enhanced with HTML5 features by the addition of the Chrome Frame plug-in.

See more:

Architecture

Security

Getting Started

Dynamic DNS and Certificate Sharing

Mobile Devices

Integrating ThinRDP

Advanced Settings

User's guide

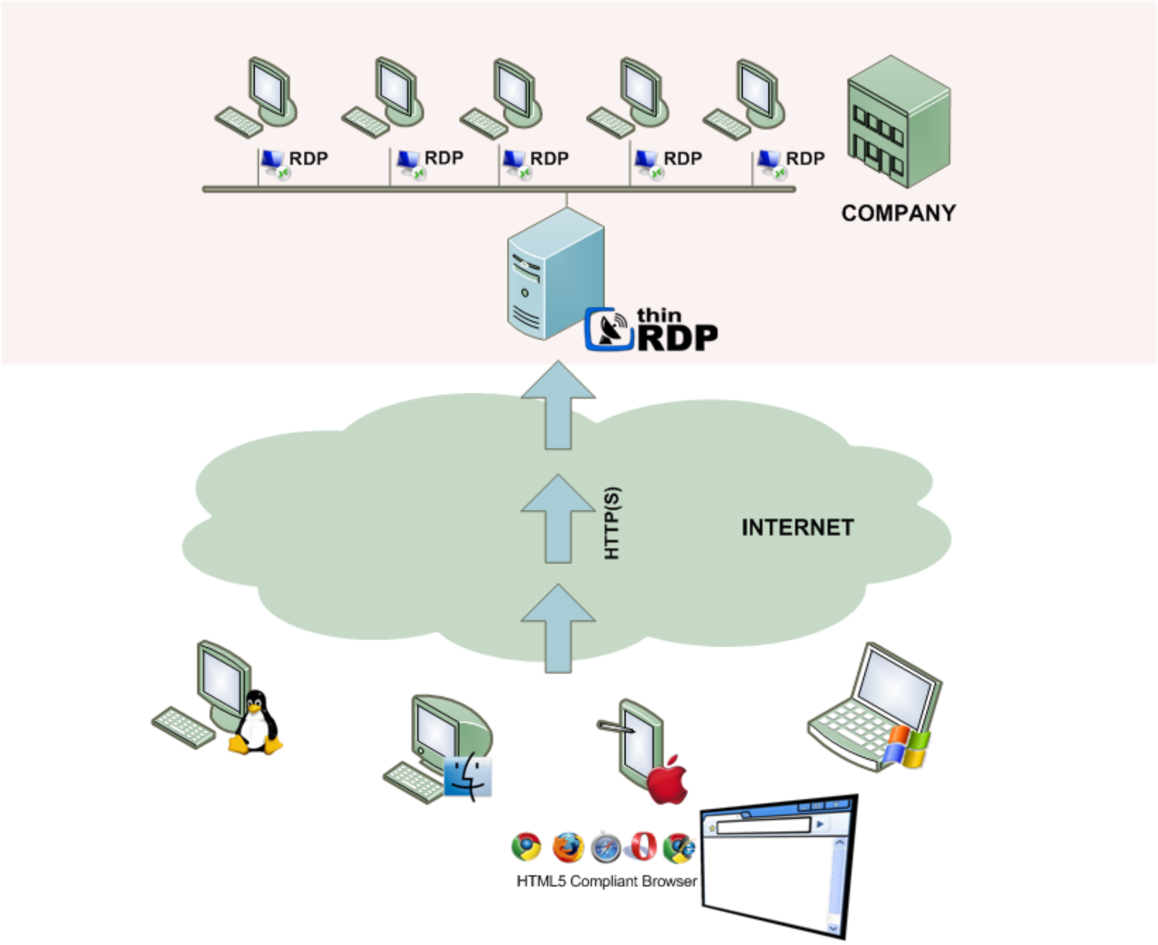
3 Architecture

ThinRDP is composed of:

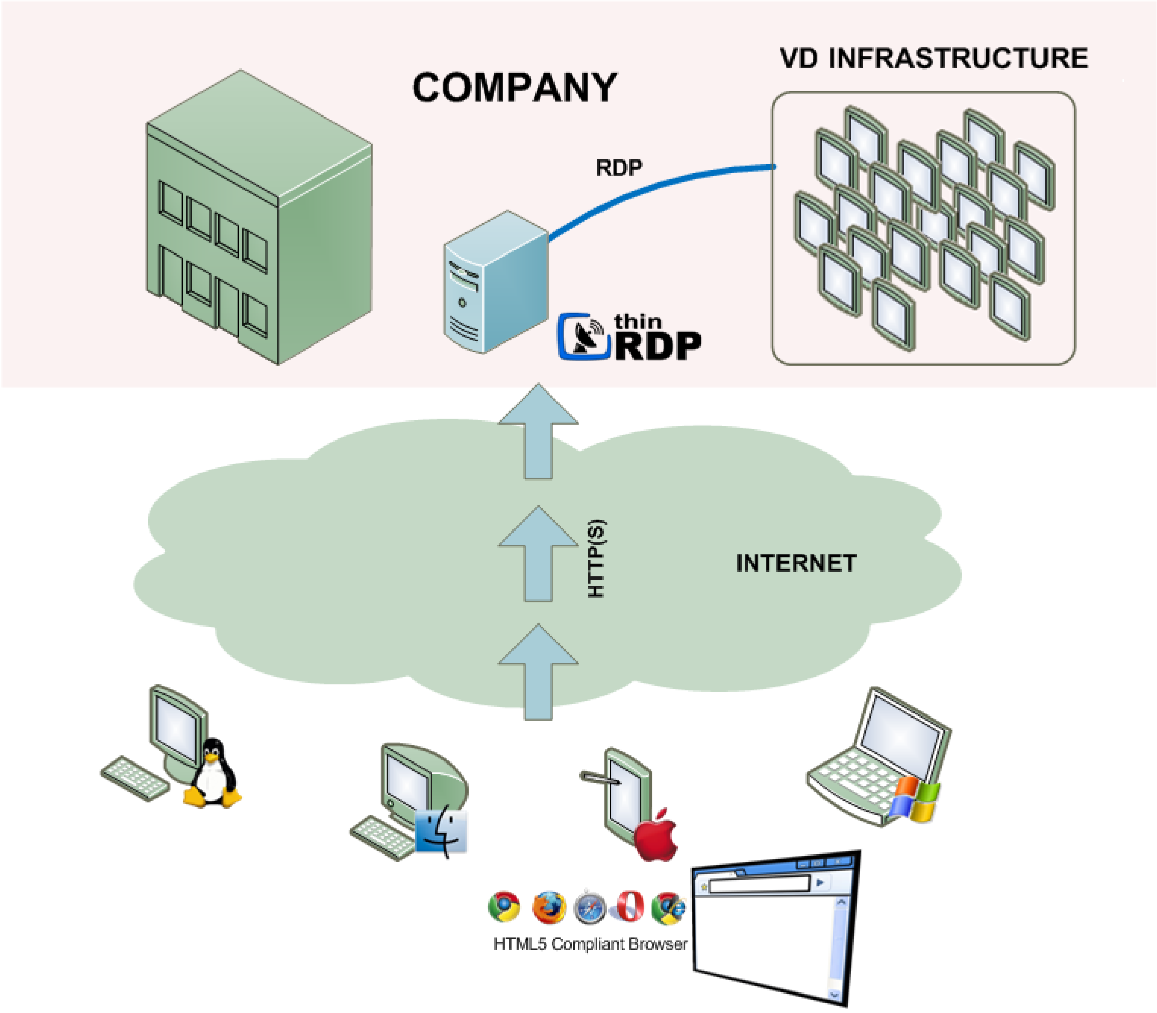
ThinRDP Windows Server:
ThinRDP Windows Server is a secure, high-performance HTTP / WebSockets server, which serves the web pages needed to run the ThinRDP Web Client on the web browser and, at the same time, acts as a gateway between the ThinRDP Web Client and the remote RDP server.

ThinRDP Web Client:
When the end-user accesses the ThinRDP main page and enters the appropriate connection parameters, the Web Client connects to the Server using Ajax and WebSockets (if available) to start the connection to the remote-end. Once the connection is established, ThinRDP Windows Server interprets RDP commands, optimizes them for the web, and sends the resulting data stream to the ThinRDP Web Client.

ThinRDP connecting to Windows PC's Desktops:



ThinRDP connecting to Virtual Desktops or Applications:



Requirements:

ThinRDP Web Client

- HTML5 Web Browser compliant

ThinRDP Windows Server

- Windows XP 32-bit / Windows XP 64-bit
- Windows Vista 32-bit / Windows Vista 64-bit
- Windows 7 32-bit / Windows 7 64-bit
- Windows Server 2008 32-bit / Windows Server 2008 64-bit

4 Security

Security and privacy are essential when accessing remote desktops through the Internet. ThinRDP Server provides a reliable, state-of-the-art security that keeps the exchanged information safe.

Secure connections

All the connections to ThinRDP from the browser are performed over HTTPS. ThinRDP provides you with the means to install your own 256-bit SSL certificate.

Authentication levels

ThinRDP allows you to set different authentication levels. You can choose a simple User/Password authentication and specify your own credentials, or Active Directory authentication, which will enable you to authenticate against Windows local or domain users.

Access Profiles:

The profile configuration gives you the possibility to restrict the access of different Active Directory users to different computers, thus strengthening the company's security scheme.
If you want to integrate ThinRDP authentication with external applications, read the External Authentication and Single-Sign-On topics.

5 Getting Started

Use this section to cover the fundamental aspects of ThinRDP in order to get started.

You will learn to create all the necessary configuration in a simple step by step guide so that you can start enjoying the benefits of ThinRDP in a matter of minutes:

1. Installing ThinRDP
2. Using ThinRDP for the first time
3. Customizing ThinRDP
4. Connecting after customization
5. Supported RDP shortcut keys

Find a more exhaustive reference of the available options here:

Advanced Settings

Managing the SSL Certificate

Dynamic DNS and Certificate Sharing

Mobile devices

Integrating ThinRDP

User's Guide

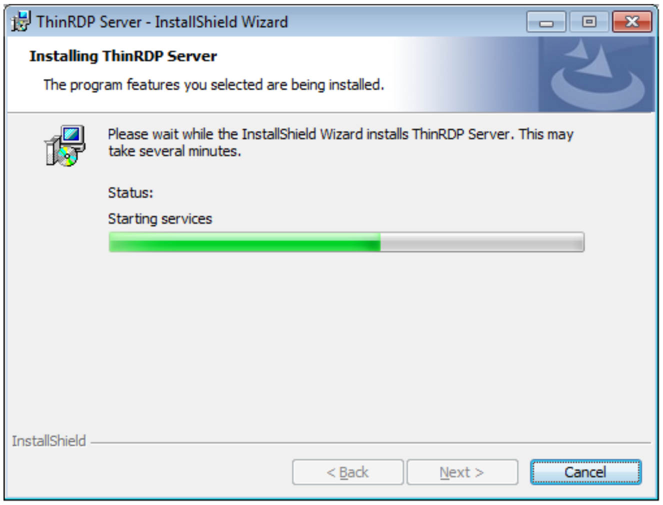
5.1 Installing ThinRDP

ThinRDP is simple to deploy. All you need to do is install it on a machine that will act as an access point.

1. Download the installer from this link:

   http://www.cybelesoft.com/downloads/ThinRDPTSSetup.exe

2. Execute the installer on the target machine.



ThinRDP Server - InstallShield Wizard

Installing ThinRDP Server

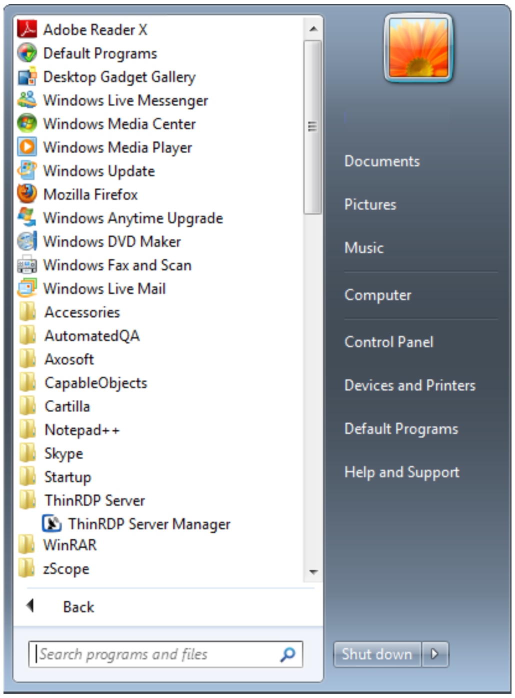
The program features you selected are being installed.

Please wait while the InstallShield Wizard installs ThinRDP Server. This may take several minutes.

Status:

Starting services

3. Look for the "*ThinRDP Server Manager"* in the Start Menu.



5.2 Using ThinRDP for the first time

Connecting to a remote desktop for the first time with ThinRDP is really easy:

Verify the communitcations settings

Once ThinRDP is installed and RDP in the remote machine is enabled, all you need is an HTML5 compatible browser: Google Chrome, Mozilla FireFox, Safari, Opera, Internet Explorer 9. Previous versions of Internet Explorer can be made compatible with HTML5 by installing Google Chrome Frame.

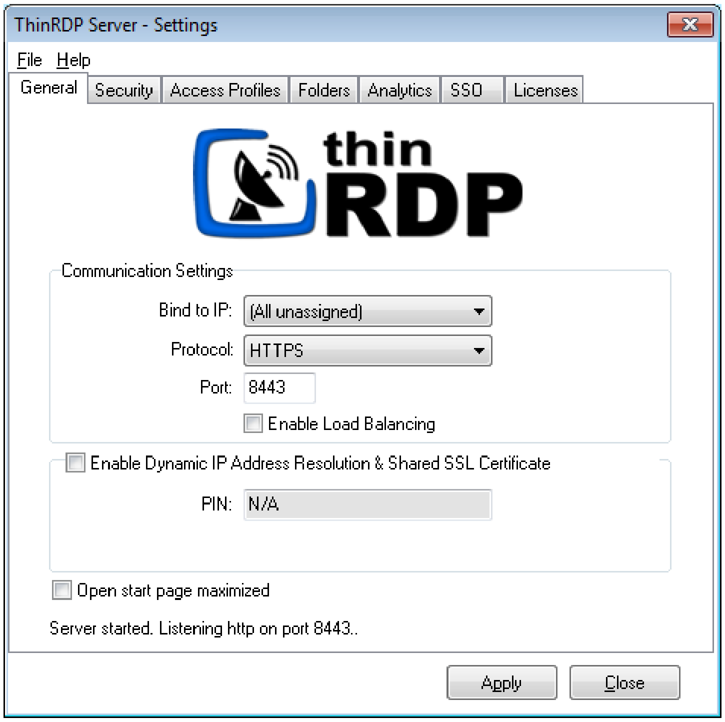
After all Connect to a desktop for the first time with ThinRDP.

5.2.1 Verifying the communication Settings

ThinRDP listens on port 8443 by default. If you are not using this port yet it won't be necessary to change the ThinRDP port.
Check whether ThinRDP is running looking at the status message of the "General" tab, located on the bottom of the window. It should say "Server started. Listening https on port...".

If you see the message "Could not bind socket. Address and port are already in use", it means that you will have to use another port since this one is already in use by another application.

1. Identify a port number that is not used yet in the computer where you have installed ThinRDP.



Communication Settings

Bind to IP: (All unassigned)

Protocol: HTTPS

Port: 8443

□ Enable Load Balancing

□ Enable Dynamic IP Address Resolution & Shared SSL Certificate

PIN: N/A

□ Open start page maximized

Server started. Listening http on port 8443..

2. Change the port number on the ThinRDP Manager General tab.

3. Press "Apply".

4. Verify whether ThinRDP is running in the status message of the "General" tab, located on the bottom of the window. It should say "Server started. Listening https on port...".

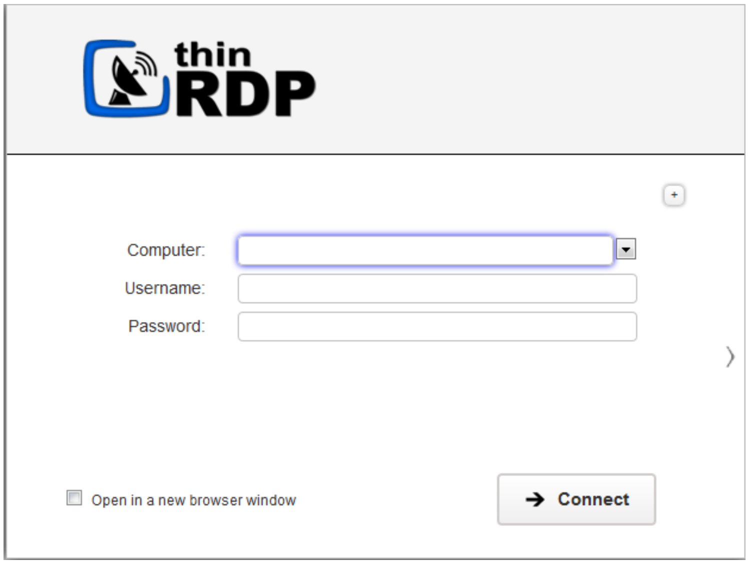
5.2.2 Connecting to a desktop

1. Open your preferred web browser.

2 . Type into the address bar https://127.0.0.1:8443/ . You can also change the 127.0.0.1 part with the server IP address or dns name where ThinRDP was installed.

3. Enter the remote desktop IP you want to connect to and type in also the user you will login with.

4. Enter the username and password to the remote machine.



5. Press Connect.

6. At this moment you are already connected remotely to the desktop. You should be seen it on your browser as if you were in front of the computer.

If you want to change the RDP connection settings, press the Options button (plus (+) sign on the right upper corner) and you will have the tabs Display, Program, Experience, Advanced and Resources available.

To set up different options and make ThinRDP suit better your needs, read the Customizing ThinRDP topic.

5.3 Customizing ThinRDP

Once you have installed ThinRDP and have connected for the first time, you can customize it to your specific needs:

1. Set the security level

2. Test internal access

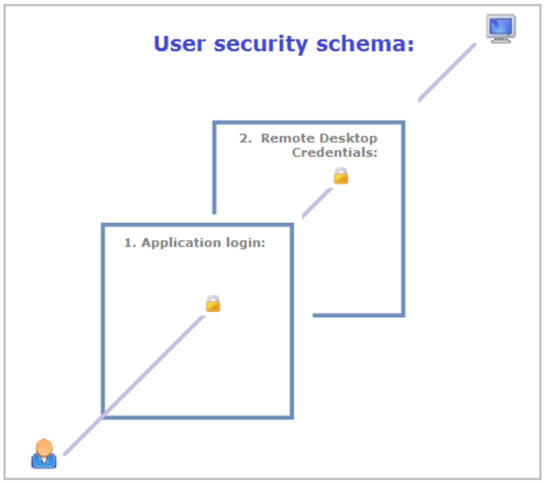
3. Configure internet access

4. Enable Remote Sound

5. Map Remote Disk Drives

5.3.1 Setting the access security level

The application administrator can set two user access security levels.



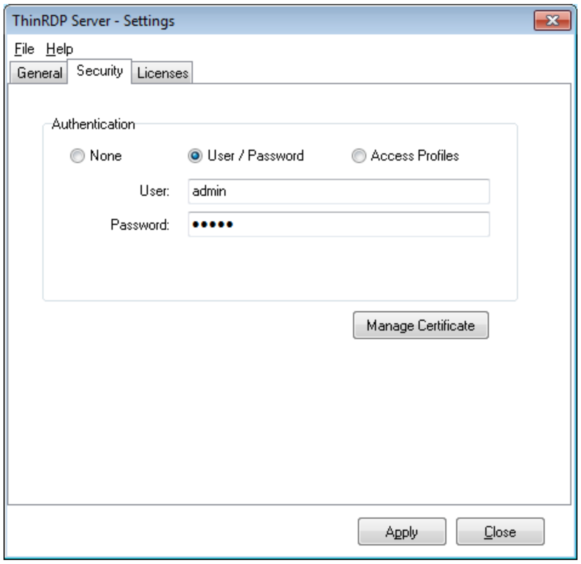
1. Application Login:

The first level provides access to users into the ThinRDP application.
You can set three different authentication modes to access the application: None, Username/Password and Access Profiles.

2. Remote Desktop Credentials:

Once logged into the application, the users will have to provide the remote desktop credentials.
You can only set default options for this security level when using Access Profiles.

In order to set up the application access security control, go to the "Security" tab in the ThinRDP Server Manager:



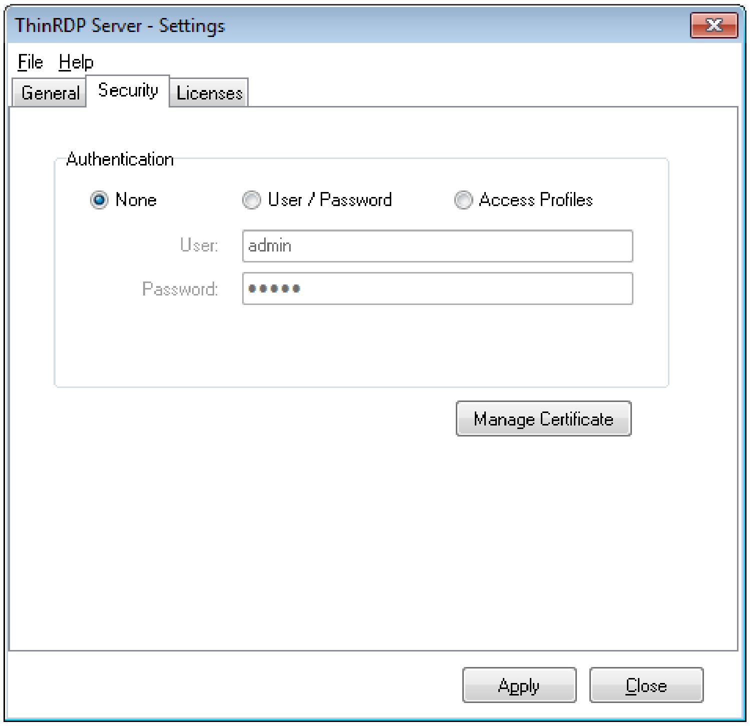
Authentication
○ None ● User / Password ○ Access Profiles
User: admin
Password: •••••

5.3.1.1 No login required

When you first install ThinRDP, the authentication will be set to "None", in other words it will have no login required.

When you set the security to None, it means that everyone will have access into the ThinRDP application without identifying themselves and so the first security level will be disabled.

This option is only recommended for local use.



Authentication

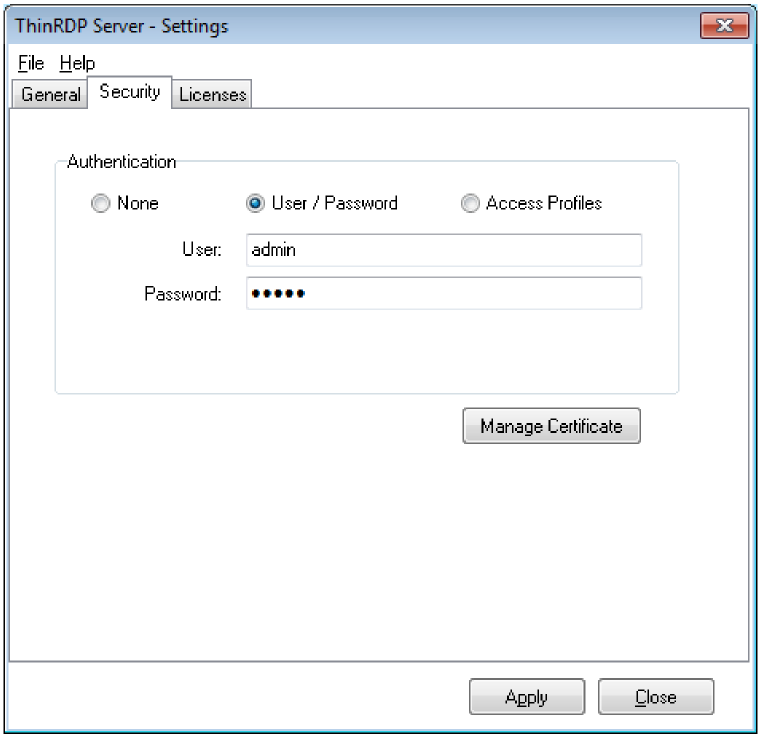
● None ○ User / Password ○ Access Profiles

User: admin

Password: •••••

5.3.1.2 User / Password

When you choose this kind of access security level, you will be able to create a single user name and password. This way, all users will have to use the same credentials (user name and password) to get into the application.



○ None ● User / Password ○ Access Profiles

User: admin

Password: •••••

To set up this authentication mode, follow these steps below:

1. Choose the authentication level by selecting "User/Password" and specify your own credentials.

2. The default credentials are user "admin" and password "admin". We suggest you to change at least this default password.

3. Press "Apply" when you are done.

4. When you access the application via web browser, provide this user name and password to get into the ThinRDP Server.

5.3.1.3 Access Profiles

This option enables you to tailor access profiles and let users seamlessly and safely connect their desktop, applications and weblinks, using the current company's security policy.

You should use "Access Profiles" if you need to:

a. Restrict the application access with Active Directory Authentication.

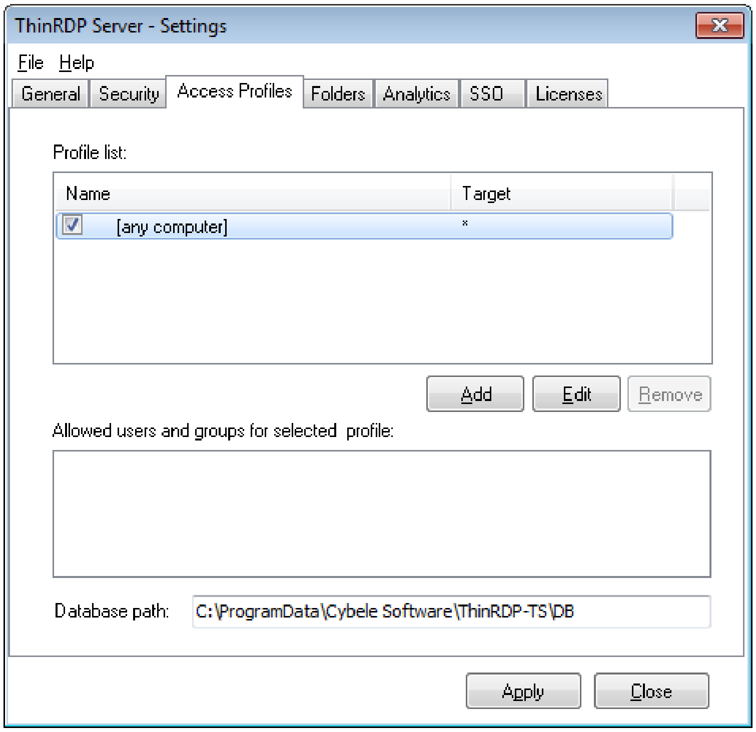
b. Specify different access levels for different users and groups of users.

c. Make the users' experience faster by configuring predetermined RDP preferences for each profile.

d. Unify authentications in a *Single Sign-on* schema.

e. Allow external application to manage ThinRDP users and machine permissions through the use of a Web Service.

In order to use the "Access Profiles", you should set this option as the authentication mode on ThinRDP Manager's "Security" tab.
This will enable the "Access Profiles" tab, as shown below.



Name	Target
☑ [any computer]	*

Database path: C:\ProgramData\Cybele Software\ThinRDP-TS\DB

The following topics will teach you how to manage RDP profile and Weblink profiles, from this Access Profiles window.

5.3.1.3.1 RDP Profiles

An RDP profile is a profile that safely connects users to their desktop and applications. Learn on the next topics how to:

[Create an RDP Profile](#)

[Edit an RDP Profile](#)

[Disable an RDP Profile](#)

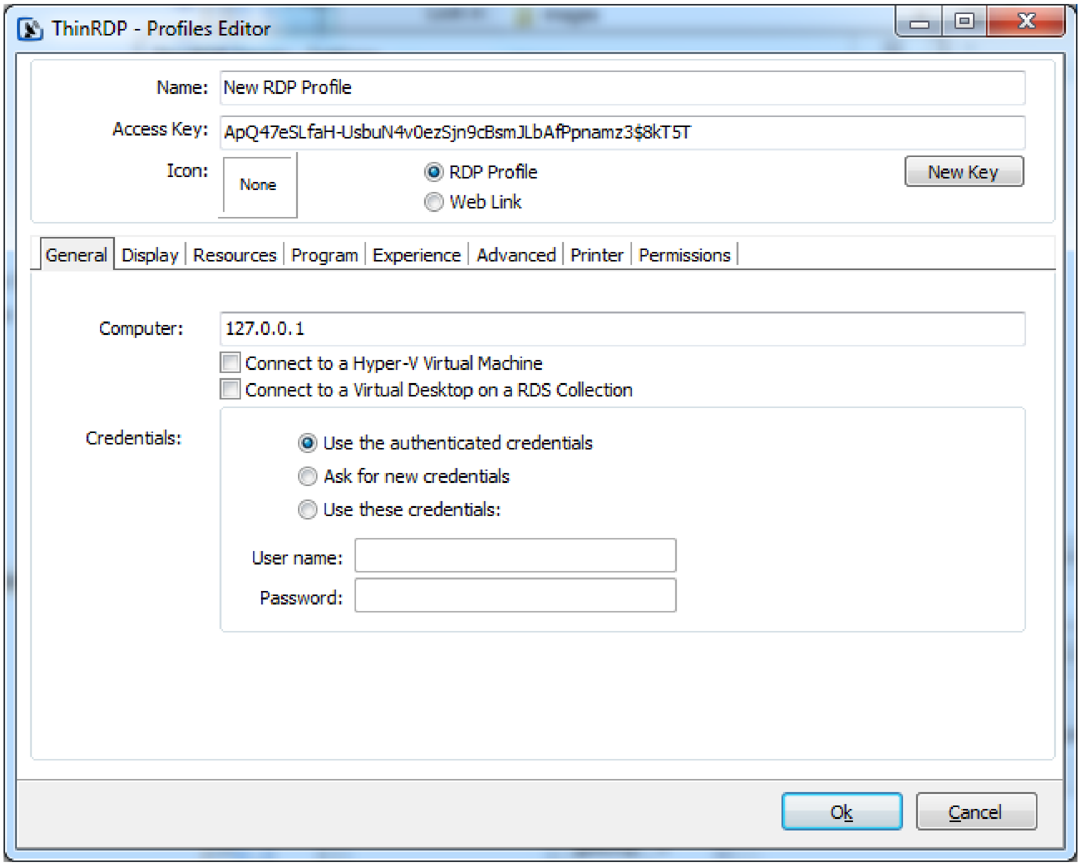
[Remove an RDP Profile](#)

[Get to know the "any computer" profile](#)

5.3.1.3.1.1 Creating a profile

1. Go to ThinRDP Manager's "Access Profile" tab. If it is not there, read the topic [Access Profiles](#) first.

2. Press "Add" to create a new profile and the following window will be presented:



ThinRDP - Profiles Editor

Name: New RDP Profile

Access Key: ApQ47eSLfaH-UsbuN4v0ezSjn9cBsmJLbAfPpnamz3$8kT5T

Icon: None

● RDP Profile

○ Web Link

Computer: 127.0.0.1

□ Connect to a Hyper-V Virtual Machine

□ Connect to a Virtual Desktop on a RDS Collection

Credentials:

● Use the authenticated credentials

○ Ask for new credentials

○ Use these credentials:

User name:

Password:

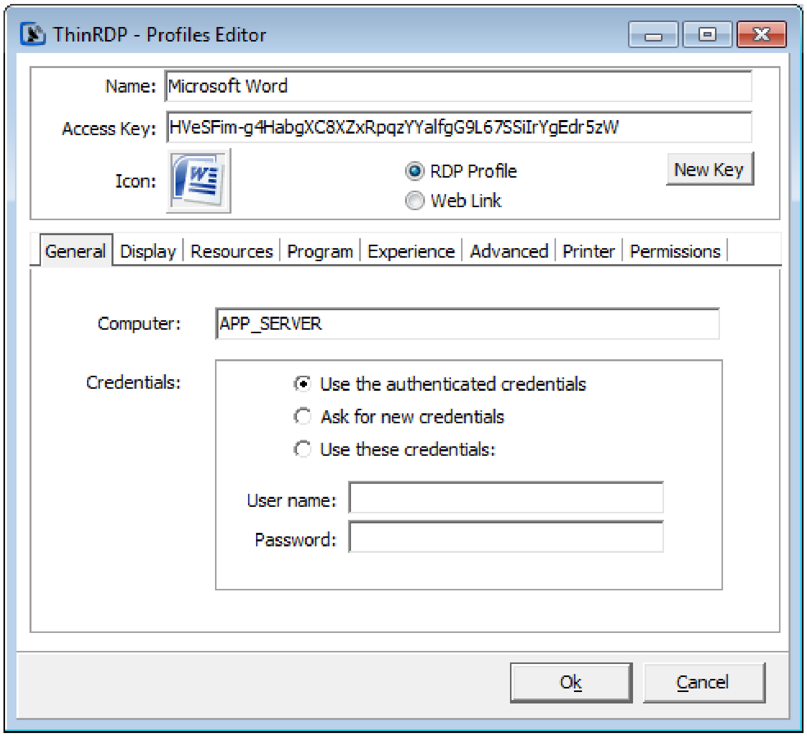
3. In order to understand better how to configure this new profile, read the next topic ([Edit a profile](#)) from step 3 on.

5.3.1.3.1.2 Editing a profile

Configuring a profile properly will allow you to take advantage of this feature and create the access scheme that suits better the company's needs.
Remember that each profile defines a single computer's desktop or application access, except for the "[any computer]" profile that gives access to all computers.

1. Go to ThinRDP Manager's "Access Profile" tab. If it is not there, read the topic Access Profiles first.

2. Press "Edit" to configure the profile and the following window will be presented:



ThinRDP - Profiles Editor

Name: Microsoft Word

Access Key: HVeSFim-g4HabgXC8XZxRpqzYYalfgG9L67SSiIrYgEdr5zW

Icon:

● RDP Profile
○ Web Link

Computer: APP_SERVER

Credentials:
● Use the authenticated credentials
○ Ask for new credentials
○ Use these credentials:

User name:

Password:

3. First of all, type in a descriptive name for the profile in the "Name" field.

4. Specify the computer this profile will connect to. Enter the internal IP or computer name on the field Computer.

5. Set the credentials to log into the remote machine:

Use the authenticated credentials	Sets a *Single sign-on* schema. The application credentials will be used to log in automatically on the remote desktop.
Ask for new credentials	Prompt the user for new credentials to access the remote desktop.
Use these credentials	If the credentials informed here are correct, this option will connect the user automatically to the remote desktop on selecting the profile, or after authenticating on ThinRDP, if this is the only profile the user have.

6. Go to the permissions tab and set up the permission preferences as follow:

Allow anonymous access	Use this option, if you want this profile to be available for everyone. This means that everybody accessing ThinRDP will see this profile. Checking this option will disable the user selection.
Group or users accesss	To use specific users for this profile, uncheck "Allow anonymous access", press "Add" and choose the users and groups from the local domain. This means that only users that authenticate with their correct Windows username and password will be able to use this profile.

7. You may want to configure other settings for the RDP connection. If so, check out the available options on Display, Program, Experience, Advanced and Printer.

8. When you are done with the previous steps, press OK.

5.3.1.3.1.3 Disabling a profile

Disabling a profile will make it unavailable to all users.
If you disable a profile and later on decide to use it again, all of its settings will be kept on.

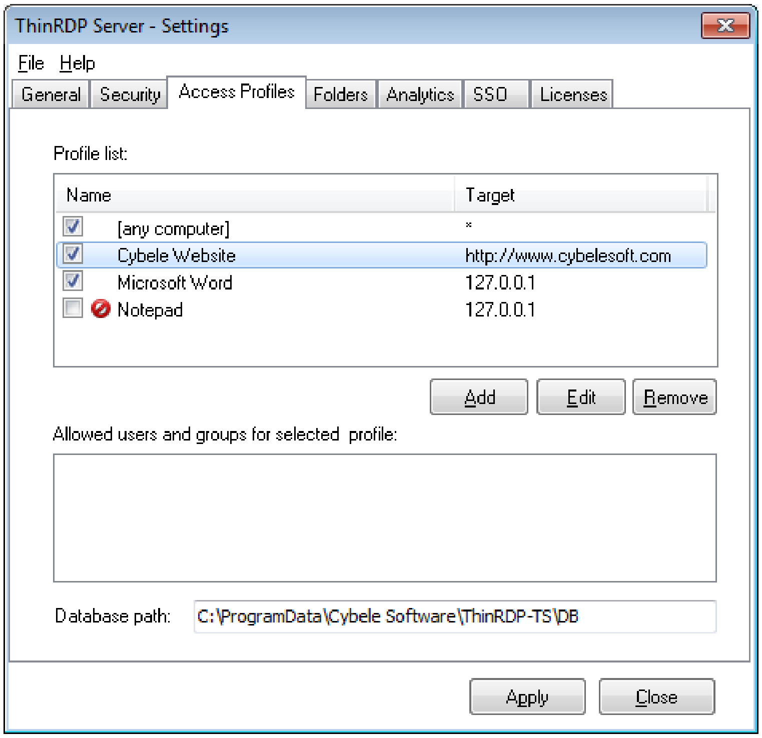
1. Go to ThinRDP Manager's "Access Profile" tab. If it is not there, read the topic Access Profiles first.

2. Select the profile you want do disable.

3. Mark the check-box located beside the profile name.

4. Observe that a forbidden image will be shown on the profile line.

5. Press "Apply" to save the changes.



Profile list:

Name	Target
☑ [any computer]	*
☑ Cybele Website	http://www.cybelesoft.com
☑ Microsoft Word	127.0.0.1
□ 🚫 Notepad	127.0.0.1

Allowed users and groups for selected profile:

Database path: C:\ProgramData\Cybele Software\ThinRDP-TS\DB

5.3.1.3.1.4 Removing a Profile

Remember that once you remove a profile you won't be able to recover it.

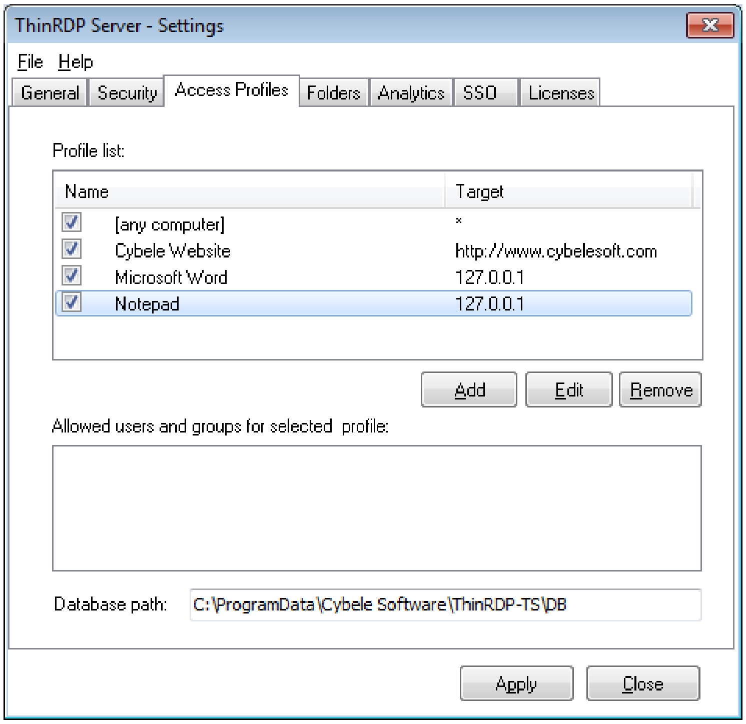
1. Go to ThinRDP Manager's "Access Profile" tab. If it is not there, read the topic Access Profiles first.

2. Select the profile you want to remove.

3. Press the "Remove" button.

4. Press "Yes" on the confirmation message.

5. Press "Apply" to save the changes.



Profile list:

	Name	Target
☑	[any computer]	*
☑	Cybele Website	http://www.cybelesoft.com
☑	Microsoft Word	127.0.0.1
☑	Notepad	127.0.0.1

Allowed users and groups for selected profile:

Database path: C:\ProgramData\Cybele Software\ThinRDP-TS\DB

5.3.1.3.1.5 The "[any computer]" profile

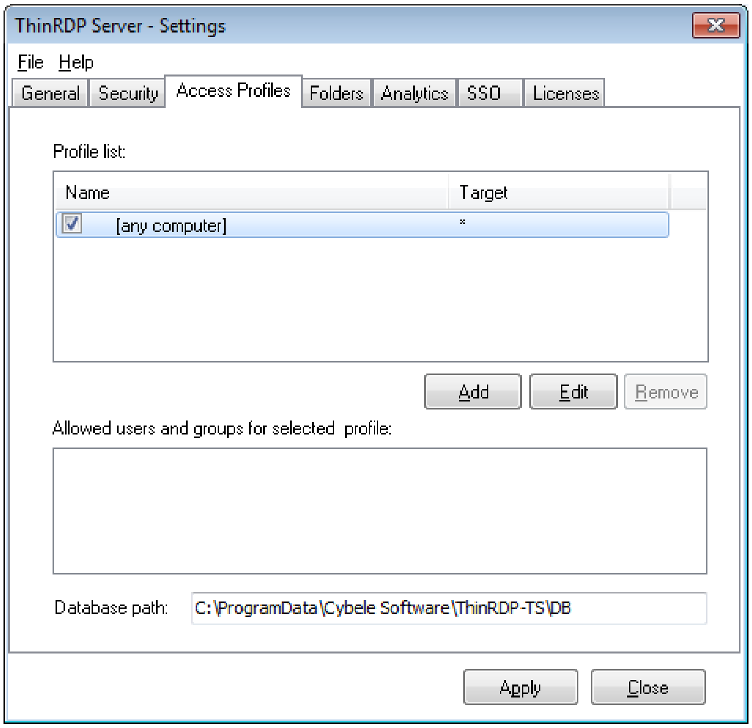
The "[any computer]" profile is the default profile for ThinRDP.

It has two special behaviors:

a. Allows access to all computers.
b. Let users choose freely their own settings at the connection moment.

Initially this profile comes with the "Allow anonymous access" option set.
If you want to grant this profile to a limited set of users and groups, follow these steps:

1. Select the [any computer] profile.
2. Observe that the "Remove" option is still disabled. That's because this profile can not be removed.
3. Click on the "Edit" option.



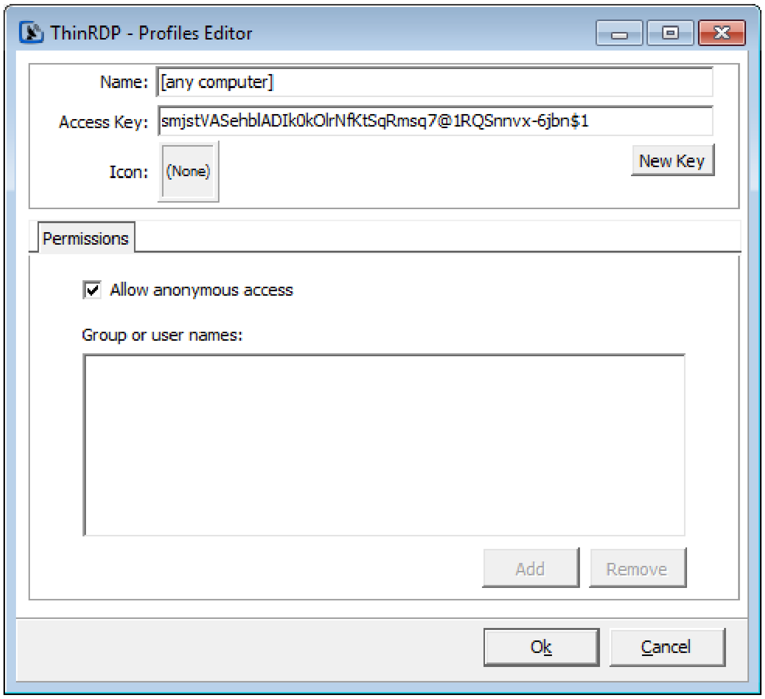
Profile list:

Name	Target
☑ [any computer]	*

Allowed users and groups for selected profile:

Database path: C:\ProgramData\Cybele Software\ThinRDP-TS\DB

4. Uncheck the "Allow anonymous access".
5. Click on Add to select the users who will be granted with the "[any computer]" profile.



Name: [any computer]

Access Key: smjstVASehblADIk0kOlrNfKtSqRmsq7@1RQSnnvx-6jbn$1

Icon: (None)

☑ Allow anonymous access

5.3.1.3.2 Weblink Profiles

A Weblink profile is a profile that gives the users access to informed URL. These profiles will be presented along with the RDP profiles within the Web Interface.
Read the next topics and learn how to:

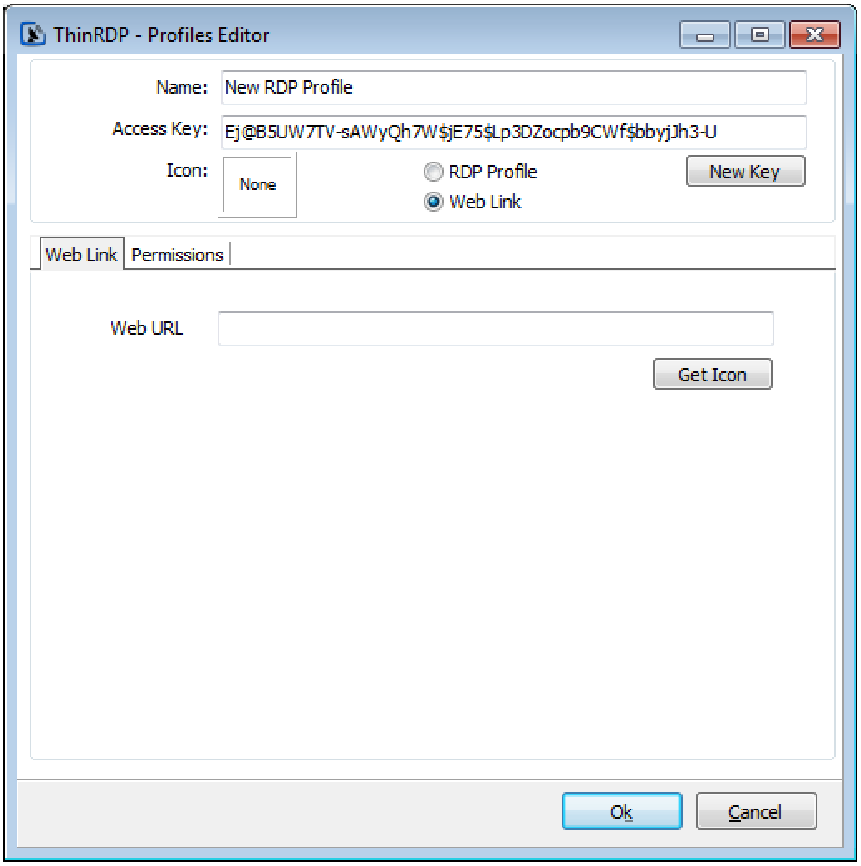
- Create an Weblink Profile
- Edit an Weblink Profile
- Disable an Weblink Profile
- Remove an Weblink Profile

5.3.1.3.2.1 Creating a profile

1. Go to ThinRDP Manager's "Access Profile" tab. If it is not there, read the topic Access Profiles first.

2. Press "Add" to create a new profile.

3. Select the option "Web link" and the screen below will be presented.



ThinRDP - Profiles Editor

Name: New RDP Profile

Access Key: Ej@B5UW7TV-sAWyQh7W$jE75$Lp3DZocpb9CWf$bbyjJh3-U

Icon: None

○ RDP Profile
● Web Link

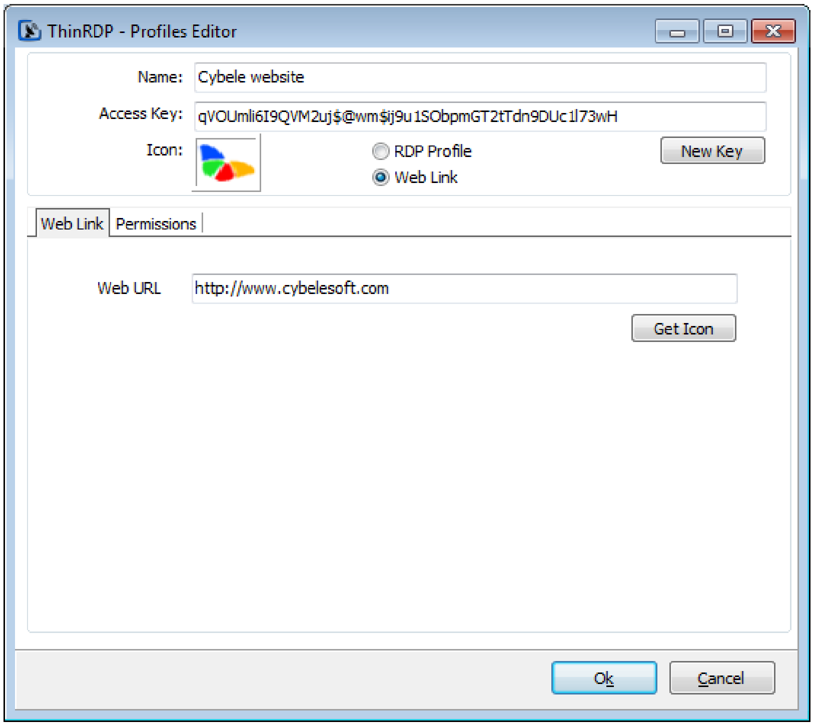
Web URL:

3. In order to understand better how to configure this new profile, read the next topic (Edit a profile).

5.3.1.3.2.2 Editing a profile

1. Go to ThinRDP Manager's "Access Profile" tab. If it is not there, read the topic Access Profiles first.

2. Select the profile you want to modify and press "Edit" to configure the profile.



Name: Cybele website

Access Key: qVOUmli6I9QVM2uj$@wm$ij9u1SObpmGT2tTdn9DUc1l73wH

Icon:

○ RDP Profile

● Web Link

Web URL http://www.cybelesoft.com

3. First of all, type in a descriptive name for the profile in the "Name" field.

4. Specify the "Web URL" you want the profile to connect to.

5. Go to the permissions tab and set up the permission preferences as follow:

Allow anonymous access	Use this option, if you want this profile to be available for everyone. This means that everybody accessing ThinRDP will see this profile. Checking this option will disable the user selection.
Group or users accesss	To use specific users for this profile, uncheck "Allow anonymous access", press "Add" and choose the users and groups from the local domain. This means that only users that authenticate with their correct Windows username and password will be able to use this profile.

6. When you are done with the previous steps, press OK.

5.3.1.3.2.3 Disabling a profile

Disabling a profile will make it unavailable to all users.
If you disable a profile and later on decide to use it again, all of its settings will be kept on.

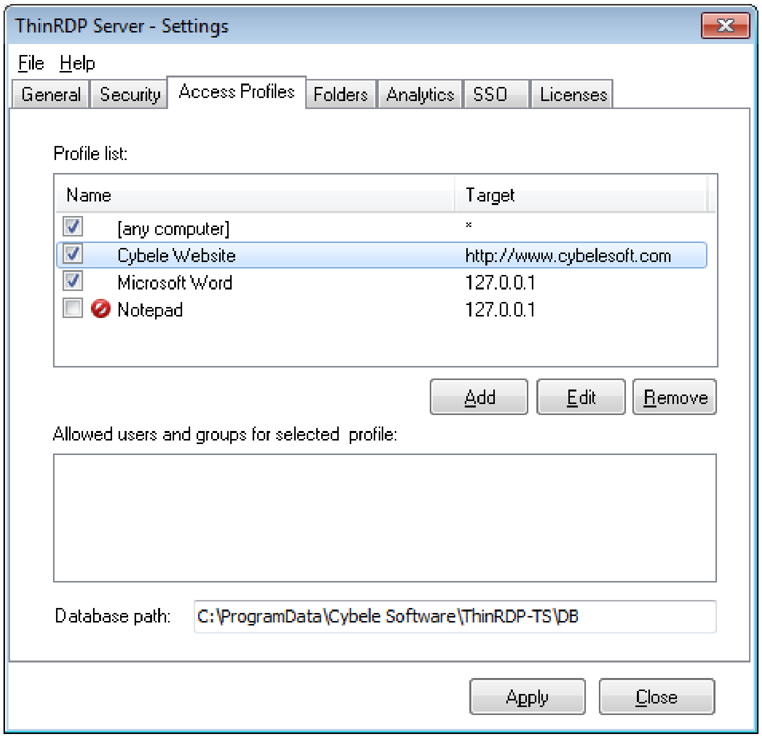
1. Go to ThinRDP Manager's "Access Profile" tab. If it is not there, read the topic Access Profiles first.

2. Select the profile you want do disable.

3. Mark the check-box located beside the profile name.

4. Observe that a forbidden image will be shown on the profile line.

5. Press "Apply" to save the changes.



Profile list:

	Name	Target
☑	[any computer]	*
☑	Cybele Website	http://www.cybelesoft.com
☑	Microsoft Word	127.0.0.1
☐	🚫 Notepad	127.0.0.1

Allowed users and groups for selected profile:

Database path: C:\ProgramData\Cybele Software\ThinRDP-TS\DB

5.3.1.3.2.4 Removing a Profile

Remember that once you remove a profile you won't be able to recover it.

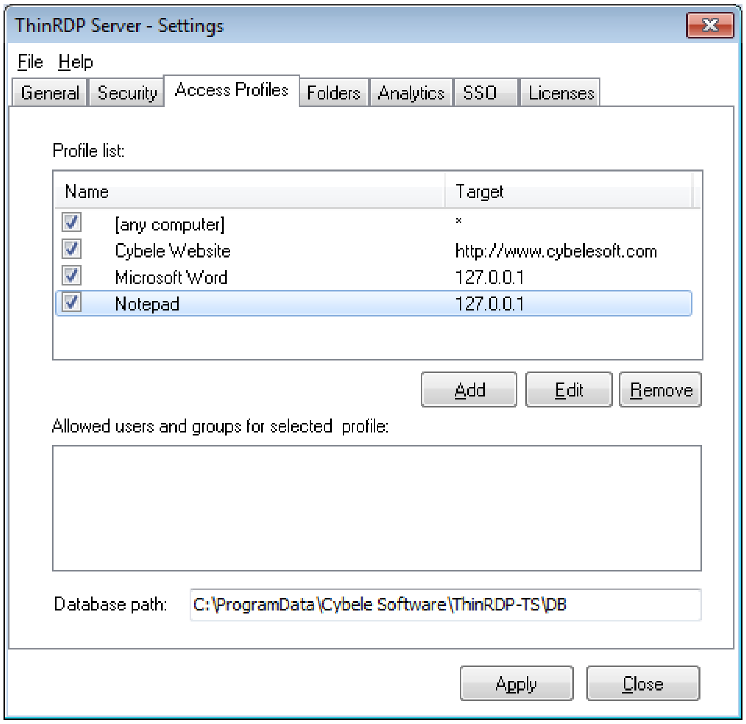
1. Go to ThinRDP Manager's "Access Profile" tab. If it is not there, read the topic Access Profiles first.

2. Select the profile you want to remove.

3. Press the "Remove" button.

4. Press "Yes" on the confirmation message.

5. Press "Apply" to save the changes.



Profile list:

Name	Target
☑ [any computer]	*
☑ Cybele Website	http://www.cybelesoft.com
☑ Microsoft Word	127.0.0.1
☑ Notepad	127.0.0.1

Allowed users and groups for selected profile:

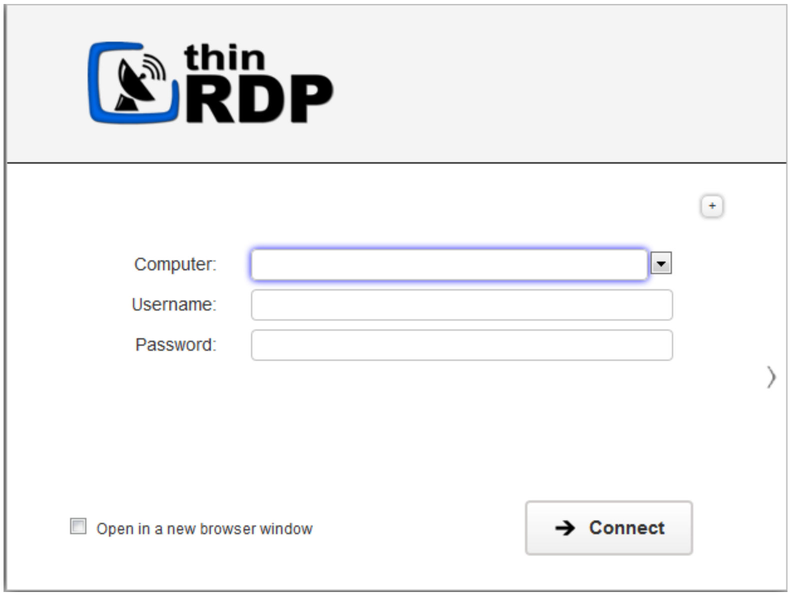
Database path: C:\ProgramData\Cybele Software\ThinRDP-TS\DB

5.3.2 Testing internal access

Although ThinRDP requires no installation on the remote desktops, you might need to enable RDP access if it is turned off.

Once the remote desktop is ready to receive RDP connections and you have set the port and authentication level in ThinRDP, you should be able to access it internally by typing into a web browser: https://internal-ip:port

After accepting the certificate and informing the credentials you will see ThinRDP's main web interface:



This means that ThinRDP is running and you can use it within the LAN.

5.3.3 Configuring internet access

After you verified that ThinRDP is running internally, you can make it available from the internet. If you have a static IP/domain, you might prefer providing internet access through your own external IP.

1. Test the access

Test the internet access by typing into a browser the following url:

https://external-ip:port
or
https://your-domain:port

2. Configuring the router:

Providing access to the internet through the external IP/domain, will require you to forward the port manually:

2.1. Port Forwarding:

a. Access the router by typing into a web browser the IP for the Default Gateway.
b. Authenticate with the router credentials.
c. Go to the port forwarding section and pick a port for internet access. It can be the same port number as the one ThinRDP is running on, or a different one.
d. Forward the internet port to the machine internal IP where you have installed ThinRDP and the port where it's running.
e. Save the changes.

If you need help configuring the router, contact us at **support@cybelesoft.com**

Check out the other possibilities ThinRDP provides you on the Public Access section.

5.3.4 Enabling Remote Sound

The remote sound feature allows you to listen to the sound playing on the remote machine. This feature is only available for Chrome and Firefox browsers until the moment.
Follow the next steps to enable the remote sound on ThinRDP.
If you are using:

a. Access Profiles:

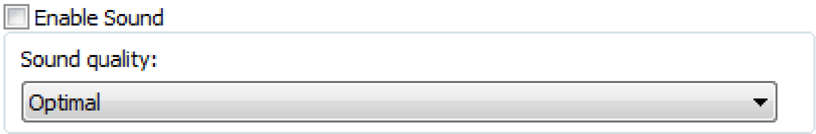
Enable the remote sound on ThinRDP Manager.

1. Go to the Access Profiles tab.

2. Edit the profile you want to enable the remote sound.

3. Go to the tab Resources.

4. Check the "Enable Sound" option.



□ Enable Sound

Sound quality: Optimal

5. The default sound quality is the "Optimal". You can also, increase the quality, by setting it up to Excellent, or make it lower, to gain performance.

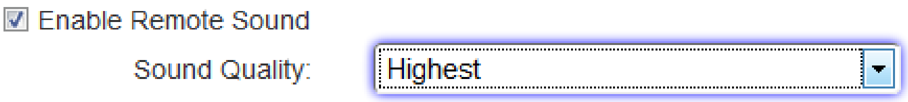
6. On the Web Interface, connect to a remote machine using this profile and try to listen to any sound playing remotely.

b. Other authentication methods (none, username/password, "any computer" profile):

Enable sound right before connecting on the Web Interface:

1. Once on the Web Interface, open the Options (plus sign +) and open the "Resources" tab.

2. Check the option "Enable Sound".



☑ Enable Remote Sound

Sound Quality: Highest

3. Choose the quality.

4. Connect and play a remote sound, so that you can enjoy it from your preferred browser.

5.3.5 Mapping remote drives

ThinRDP allows you to map remote drives that enable you to interchange files between the remote environment and the local one.
You can map remote drivers using two different features:

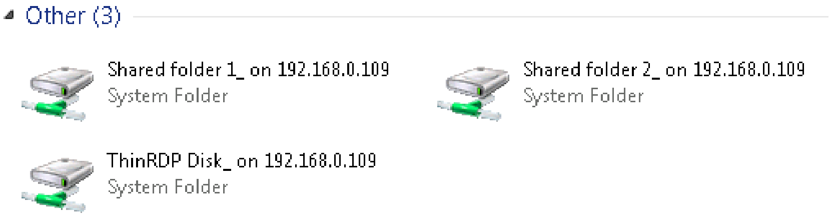
1. Intermediate Disks

2. Shared Folders

5.3.5.1 Intermediate disks

An intermediate disk is a directory created by ThinRDP to keep files that users will exchange between the remote computer and the browser.
The intermediate files will be available to ThinRDP users on two places:

1) On the remote connection Windows Explorer, as a mapped drive:



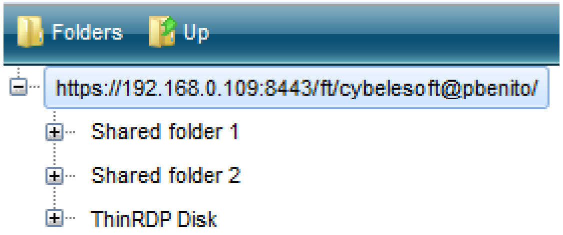
Other (3)

Shared folder 1_ on 192.168.0.109
System Folder

Shared folder 2_ on 192.168.0.109
System Folder

ThinRDP Disk_ on 192.168.0.109
System Folder

2) On the File Transfer Manager as a remote directory to exchange files with.



https://192.168.0.109:8443/ft/cybelesoft@pbenito/

Shared folder 1

Shared folder 2

ThinRDP Disk

Configuring an Intermediate disk is very easy:

If using Access Profiles:

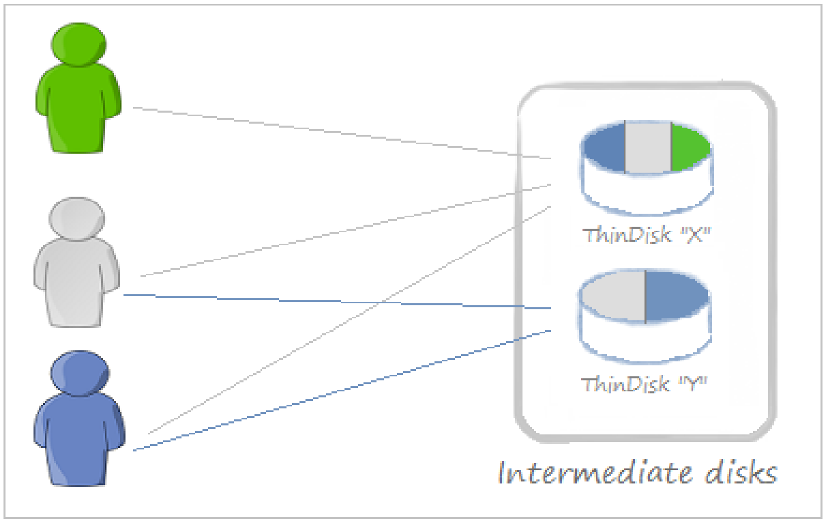
1. On ThinRDP Manager, go to the Access Profiles tab.
2. Edit the profile you want to enable the intermediate disk.
3. Open the resources tab.
4. Check the option "Enable Intermediate Disk", give a name to the disk and save the changes.
5. When you connect using this profile, look for this drive on the remote machine Windows Explorer.

If using other authentication methods:

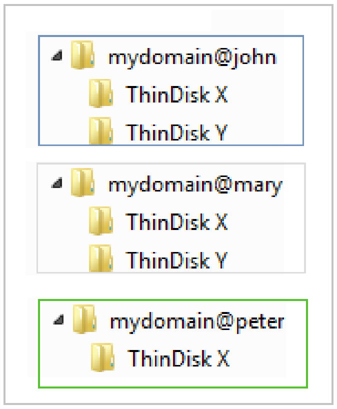
1. On the Web Interface, open the tabbed option (plus [+] sign)
2. Go to the resources tab.
3. Check the option "Enable Intermediate Disk" and give a name to the disk.
4. Connect and look for the drive that was created, on the remote machine Windows Explorer.

Intermediate physical files location:

The location where these files are kept physically is called "Temporary Folders" and can be also customized on ThinRDP manager.
Inside the temporary folders, each user has its files kept separately from the others.



The temporary folder structure for the users John (blue), Mary (gray) and Peter(green) above would look like the image below:



mydomain@john
ThinDisk X
ThinDisk Y

mydomain@mary
ThinDisk X
ThinDisk Y

mydomain@peter
ThinDisk X

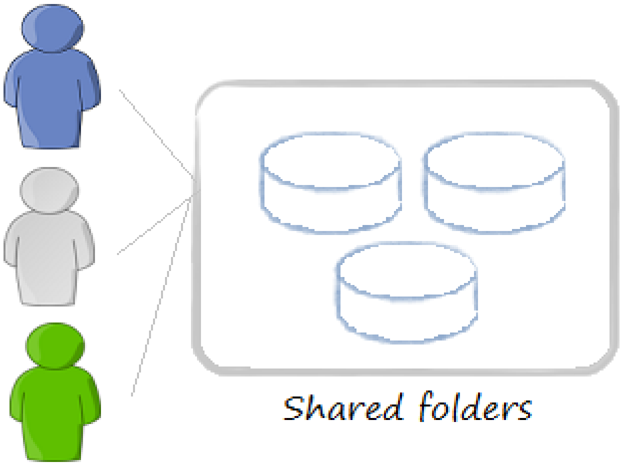
Temporary folders

A user will have access to an intermediate disk, if he/she has access to any profile associated with this disk.
When a profile is set to anonymous, all users that connect through it will also have access to the

disk associated with this profile.

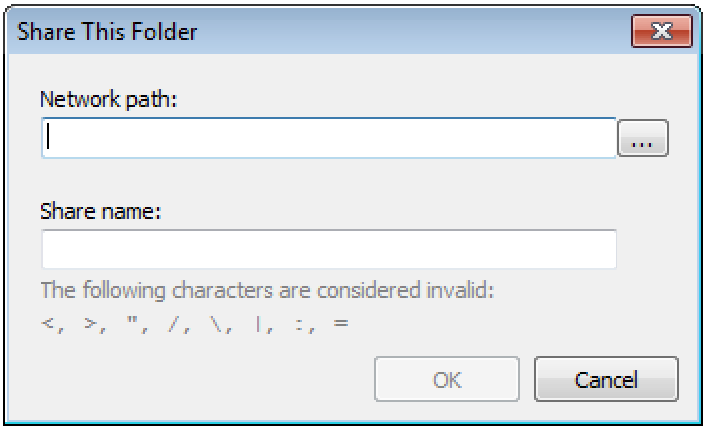
5.3.5.2 Shared folders

The shared folders are existing local network directories that you can map as a drive on ThinRDP remote connections.
Once set, they will be accessible from every connection and by all ThinRDP users.



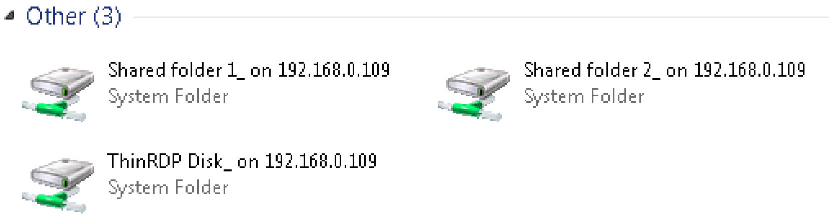
Follow the next steps to configure a new Shared Folder:

1. On ThinRDP Manager open the "Folders" tab.
2. Click on the bottom "Add" button.
3. Inform the "Network path" to be shared
4. Give a name ("Share name") to be shown on the remote mapped disks.



The following characters are considered invalid:
<, >, ", /, \, |, :, =

5. Press OK.
6. From now on, users will find this directory as a mapped drive in every ThinRDP connection, and also as a Remote location on the File Transfer Manager.


◢ Other (3)

Shared folder 1_ on 192.168.0.109
System Folder

Shared folder 2_ on 192.168.0.109
System Folder

ThinRDP Disk_ on 192.168.0.109
System Folder

As you probably have realized, you can set as many Shared folders as you want and each one of them will be mapped as a different drive on the remote connection.

5.4 After customization

If you have already customized ThinRDP, check out the following sections to see how your changes will reflect on ThinRDP application:

Connecting to a desktop

Connecting to an application

Connecting from Mobile Devices

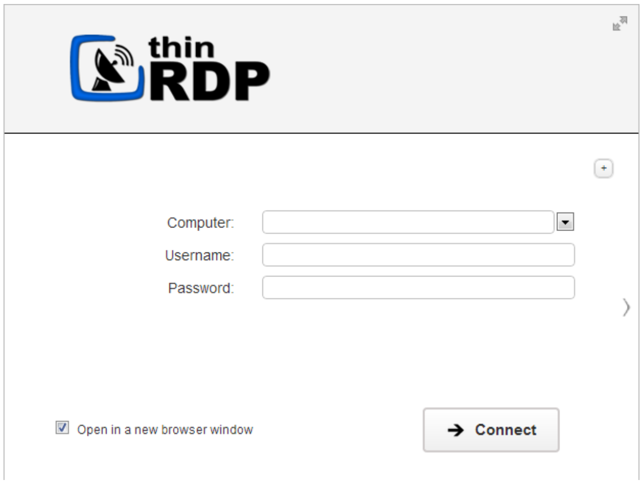
Performing a file transfer

5.4.1 Connecting to a desktop

In order to connect to a remote desktop using ThinRDP, open a browser and type the ThinRDP url, which is composed by https://Server IP:Port. A sequence of steps should happen, as follows:

1. You will be asked for the application login (user and password). This step may not happen depending on the settings you have chosen for the access security level. If you have none as authentication, or all the profiles with the *Allow anonymous access* option enabled, the application will take you directly to the next step.

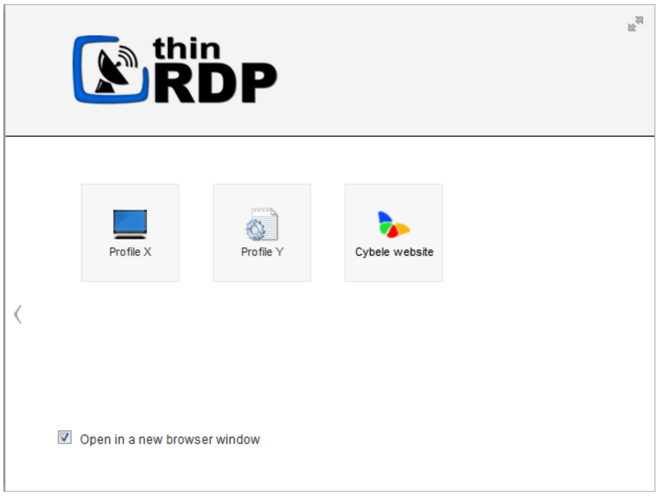
2. After that, you will be presented with the window below:



If you are using profiles and have disabled the any computer profile, you will be taken directly to the profiles page.

3. The right gray arrow will take you to all pre defined profiles assigned to this user.

3.1. If you have the profiles page available:
a) Click on the right arrow.
b) Select the profile you want to use, and click on it.
c) You won't be allowed to change the computer's IP nor the RDP options at this moment, because all profiles have an assigned computer and assigned preferences already set.



3.2. If you want to use the "any computer" profile:
a) Click on the left arrow to go back to the other page.
b) Enter the internal IP/host name for the computer you want to access and press connect.
c) Optionally you can specify the Username and Password so that it will be auto completed in the remote computer's dialog and stored by the browser for future access.

4. If you are allowed to type the computer IP / host name, which will happen only if you have as authentication *none*, username/password, or the [anycomputer] profile active, you can also change the RDP options:
a) Press the right top button (plus [+] sign) in order to access the settings tabbed interface.
b) You can check more about each option on the Web Interface Settings section.

5. Check the "Open in a new browser window" option, if you want the connection to be open on a new tab.

6. When you finish, press "Connect". You will see the remote desktop, application or webpage (in case you have weblink profiles) inside your web browser.

5.4.2 Connecting to an application

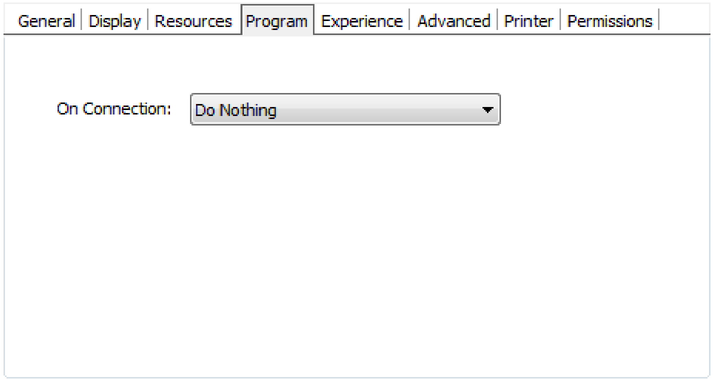
Sometimes you will need to access a remote desktop to connect to a single application. If you are an administrator you might also want to provide, for some users, access only for a particular application. This feature will be only available when you connect to remote desktops running on Windows server versions.

You can set up this option on two different moments:

On configuring a profile (ThinRDP Manager):

You can set up ThinRDP to access a single application through the use of profiles.

a. When you create or edit a profile, go to the Profiles Editor "Program tab" .
b. Mark the "Start Program On Connection" option and then specify the path and the executable file to initialize the desired program. For more information regarding these option, read the topic "Program" tab.

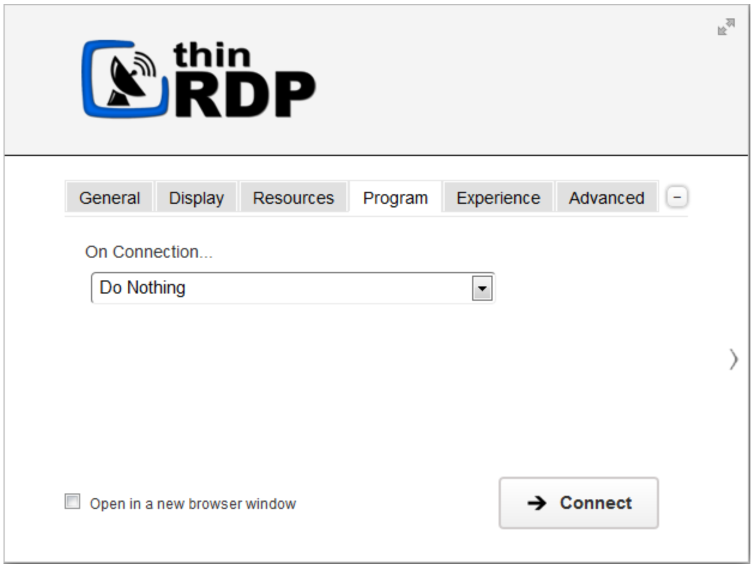


On Connection: Do Nothing

On connecting (through a browser):

You will be able to set up this option while connecting, only if you are using one of the following authentication modes: None, Username/Password and the [any computer] profile.

a. Login to ThinRDP.
b. Press the button Options, in order to have the settings tabs visible.
c. Go to the "Program" tab.
d. Check the "Start Program On Connection" option and then specify the path and the executable file to initialize the desired program. For more information regarding these options, read the topic "Program" tab.



On Connection...

Do Nothing

□ Open in a new browser window

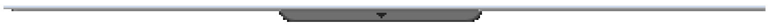
e. Set up the other tabs options, if desired.
f. Press Connect.

Observe now that the web browser got connected to a single application, instead of giving you access to the complete desktop.

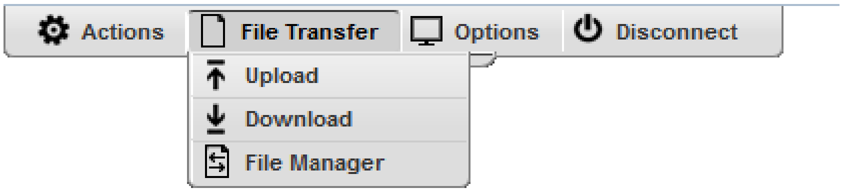
5.4.3 Performing a file transfer

Once a connection is established you have the possibility to perform File Transfers operations between the remote machine and the local computer:

1. Click on the connection middle top arrow, and the toolbar will be presented.



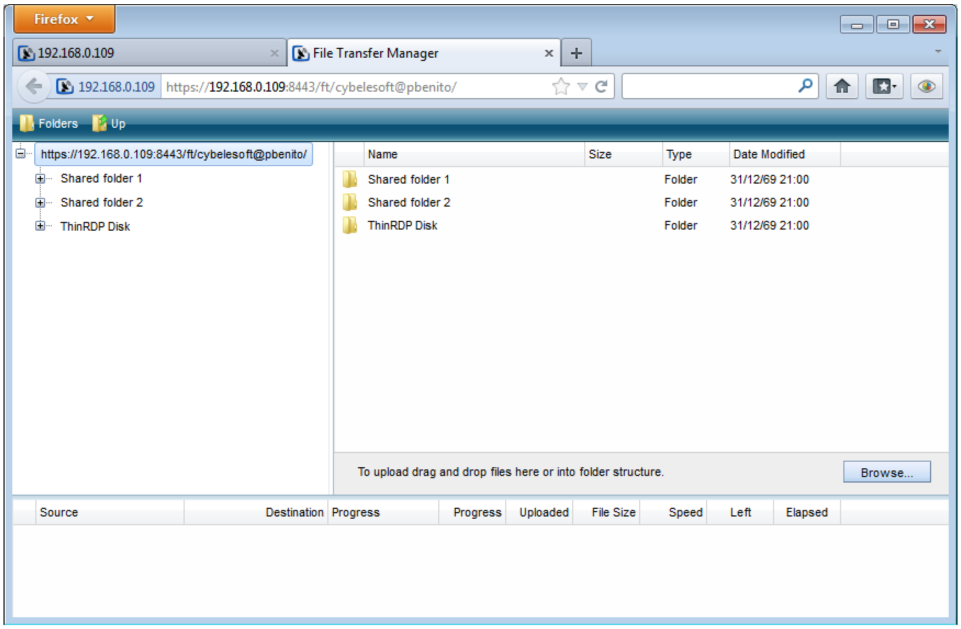
2. Click on the "File Manager" option, located inside the File Transfer toolbar option. If the button is not available ask the system administrator to set you the permissions for it.



Upload	Click on this option to upload a file located on the local computer into the remote desktop. A window will be opened so that you can select the file to be uploaded.
Download	This option enables you to download any file located inside the Intermediate disk. Select the file on the presented list and press the "Download" button.
File Transfer	This option will give you access to the File Transfer Manager.

See also, the option to Download automatically any newly-added file.

3. This is the screen where you can manage files and also transfer them.



https://192.168.0.109:8443/ft/cybelesoft@pbenito/

- https://192.168.0.109:8443/ft/cybelesoft@pbenito/
  - Shared folder 1
  - Shared folder 2
  - ThinRDP Disk

Name	Size	Type	Date Modified
Shared folder 1		Folder	31/12/69 21:00
Shared folder 2		Folder	31/12/69 21:00
ThinRDP Disk		Folder	31/12/69 21:00

To upload drag and drop files here or into folder structure.

Source	Destination	Progress	Progress	Uploaded	File Size	Speed	Left	Elapsed

4. Observe that the "Shared Folders" and the "Intermediate disk" are the only remote directories available to exchange files with. If you need to download or upload remote files from the file manager, you should always move them first into these directories (they are going to be mapped drives also), and after that transfer to the desired location.

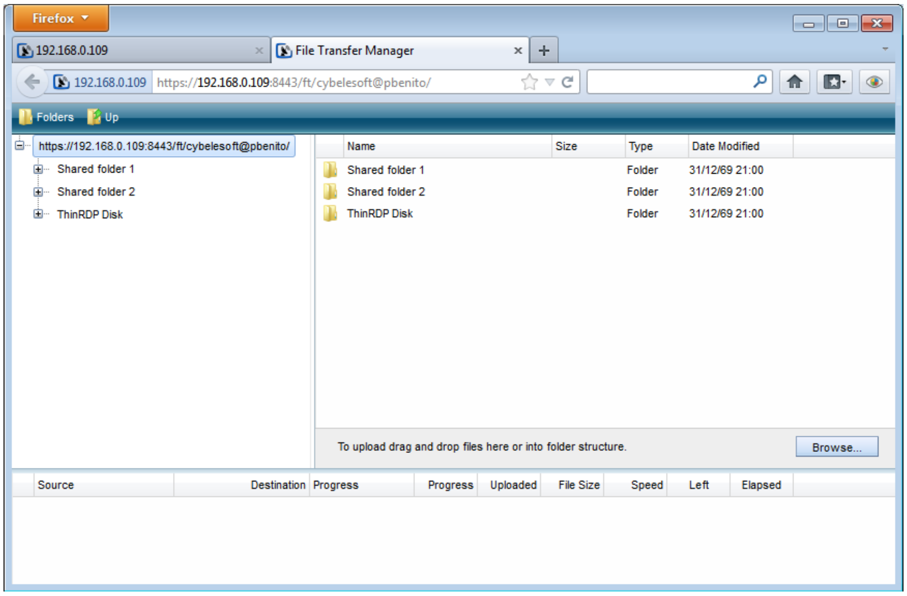
5. Read also, the following sections:

Navigating on the File Transfer Screen
File Options
Folder Area Options

5.4.3.1 Navigating

On the upper part of the screen you will see your remote files and folders. Browse to the remote location by double clicking on the folders on the right, or expanding the tree structure on the left.

In order to upload files, drag them from your local PC and paste them into the remote view area, or press the 'Browse' button.
The lower part of the screen shows the status of the files to be transferred.


Firefox
192.168.0.109
File Transfer Manager
192.168.0.109 https://192.168.0.109:8443/ft/cybelesoft@pbenito/
Folders
Up
https://192.168.0.109:8443/ft/cybelesoft@pbenito/
Shared folder 1
Shared folder 2
ThinRDP Disk
Browse...

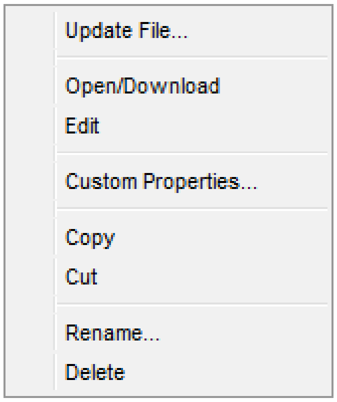
Name	Size	Type	Date Modified
Shared folder 1		Folder	31/12/69 21:00
Shared folder 2		Folder	31/12/69 21:00
ThinRDP Disk		Folder	31/12/69 21:00

To upload drag and drop files here or into folder structure.

Source	Destination	Progress	Progress	Uploaded	File Size	Speed	Left	Elapsed

5.4.3.2 File Options

Right click on a remote file to access these options:



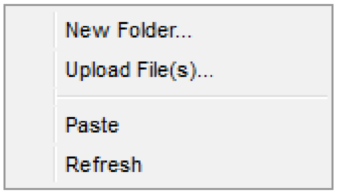
Find the behaviour for each one of these options below:

Update File	Choose this option to replace the selected remote file with a local file.

Open/Download	Choose this option to open or download the selected file.
Custom Properties	Choose this option to see the remote file's properties.
Copy	Choose this option to copy the file into the remote clipboard. You can paste it into another remote folder.
Cut	Choose this option to cut the file into the remote clipboard. You can paste it into another remote folder.
Rename	Choose this option to change the name for the remote file.
Delete	Choose this option to delete the selected file.

5.4.3.3 Remote Folder Area Options

Right click on the blank remote folder area any time to access the following options:



Find the behaviour for each one of these options below:

New Folder	Choose this option to create a new folder in the remote location.
Upload File(s)	Choose this option to upload one or more files to the remote location.
Paste	Choose this option to paste a remote file that is in the clipboard into the remote location. It will be enabled only after you have copied a file into the clipboard.
Refresh	Choose this option to refresh the view of the remote folder.

5.4.3.4 Downloading and Uploading files

1. Downloading remote files:

1. Connect to the remote machine.
2. Open the remote machine Windows Explorer and copy the remote files to be downloaded into a "Shared Folder" or an "Intermediate Disk".
3. Open the "File Transfer" Manager from the upper connection toolbar.
4. Download the remote file to any local directory of your preference.

See also, the option to Download automatically any newly-added file.

2. Uploading local files:

1. Connect to the remote machine.
2. Open the "File Transfer" Manager from the upper connection toolbar.
3. Upload the file you want to transfer to the remote machine into a "Shared Folder" or an "Intermediate Disk".
4. Go back to the connection screen and open the remote machine Windows Explorer.
5. Copy the file from the "Shared Folder" or "Intermediate Disk" drive into the remote directory of your preference.

5.5 Supported RDP Shortcut Keys

The supported shortcut keys in ThinRDP are the same as in regular RDP. Here is a list of the shortcut keys:

ALT+PAGE UP: Switches between programs from left to right.

ALT+PAGE DOWN: Switches between programs from right to left.

ALT+INSERT: Cycles through the programs using the order in which they were started.

ALT+HOME: Displays the Start menu.

CTRL+ALT+BREAK: Switches the client between full-screen mode and window mode.

CTRL+ALT+END: Brings up the Windows Security dialog box.

ALT+DELETE: Displays the Windows menu.

CTRL+ALT+MINUS SIGN (-): Places a snapshot of the active window, within the client, on the Remote Desktop Session Host (RD Session Host) server clipboard (provides the same functionality as pressing ALT+PRINT SCREEN on the local computer).

CTRL+ALT+PLUS SIGN (+): Places a snapshot of the entire client windows area on the RD Session Host server clipboard (provides the same functionality as pressing PRINT SCREEN on the local computer).

6 Dynamic DNS and Certificate Sharing

ThinRDP provides a Dynamic DNS service to link your local and public machine IP with a subdomain under thinrdp.net domain. ThinRDP DNS service gives you a PIN code to identify your installed ThinRDP server uniquely.

Using this option, you are also able to use a wilcard SSL certificate provided under thinrdp.net domain.

Follow the next topics, so you can learn how to configure and access ThinRDP with the "Dynamic DNS and Certificate Sharing" option.

Configuring PIN resolution

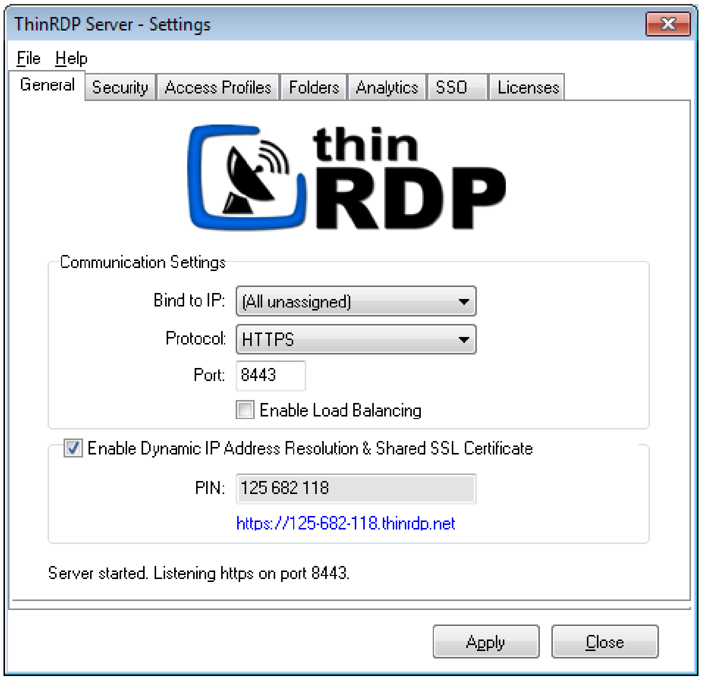
Accessing through thinrdp.net

Note: If you use this option ThinRDP will use its embedded certificate, even when the user have already configured another certificate.

6.1 Configuring PIN resolution

1. Setting up:

Go to the ThinRDP Manager "General" tab and mark the "Enable Dynamic IP Address Resolution & Shared SSL Certificate" option. This will generate your own thinrdp.net public address, similar to the blue link shown on the figure below and will generate also a PIN number:



Bind to IP: (All unassigned)

Protocol: HTTPS

Port: 8443

☐ Enable Load Balancing

☑ Enable Dynamic IP Address Resolution & Shared SSL Certificate

PIN: 125 682 118

https://125-682-118.thinrdp.net

Server started. Listening https on port 8443.

You can then, distribute this address to provide internet access to the LAN desktops and applications.

2. Configuring the router:

If you have UPnP, enabling *Dynamic IP Address Resolution & Shared SSL Certificate* can automatically open the port for you on the router.
In order to test if this option did open the port, access ThinRDP through the provided address (https://*pin_number*.thinrdp.net). If you can connect to the application normally it means the port is already opened and you are ready to go. If you get an "Invalid parameters" message, it means you will need to forward the port manually, as follows:

2.1. Port Forwarding:

a. Access the router by entering the IP for the Default Gateway in a browser.
b. Authenticate with the router credentials.
c. Go to the port forwarding section and pick a port for internet access. It can be the same port number as the one ThinRDP is running on, or a different one.
d. Forward the internet port to the IP of the machine in which you have installed ThinRDP and the port where ThinRDP is running.
e. Save the changes.

If you need help configuring the router, contact us at **support@cybelesoft.com**

6.2 Accessing through thinrdp.net

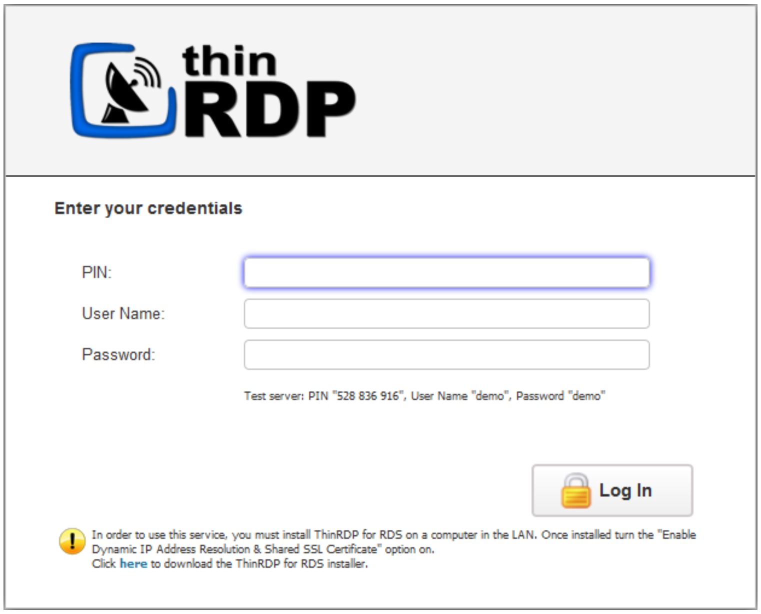
There are two ways of accessing ThinRDP through the generated Dynamic IP Address:

1. Use the whole address:

a. Click on the address generated on the ThinRDP manager General tab or copy it and paste it on browser address bar, and press enter. This will direct you into the ThinRDP Application located inside your LAN. Observe that the field PIN comes filled and you only have to fill "Username" and "Password".

2. Use the PIN Number only:

a. Type in https://www.thinrdp.net/ on a web browser address bar. The screen below will be presented:



Enter your credentials

Test server: PIN "528 836 916", User Name "demo", Password "demo"

In order to use this service, you must install ThinRDP for RDS on a computer in the LAN. Once installed turn the "Enable Dynamic IP Address Resolution & Shared SSL Certificate" option on.
Click here to download the ThinRDP for RDS installer.

b. Enter the pin number (also located on General tab) and the credentials in order to access the ThinRDP application. If you access through an external IP for the LAN, the browser will prompt you for credentials.
The rest of the connection process is the same as if you were using the static IP. Check it out how, on the Connecting to a desktop section.

7 Managing the SSL Certificate

An SSL certificate is an effective way to secure a website against unauthorized interception of data. At its simplest, an SSL Certificate is used to identify the website and encrypt all data flowing to and from the Certificate holder's Web site. This makes all exchanges between the site and its visitors 100 percent private.
A valid SSL certificate is included with the ThinRDP installation and all communications are already encrypted with the product's default certificate. You may want to create your own certificate to identify your company better.

Managing the SSL Certificate:

1. There are two forms of creating your own SSL certificate:

   a. Create A self-signed certificate

   b. Use A CA Certificate

2. Once you already have your certificate files, go to ThinRDP manager's "Security tab".

3. Click on the "Manage Certificate" option. If it is disabled, read the following subtopic "Using Dynamic DNS and Certificate Sharing".

4. On this screen you should inform the location of the certificate files, as follows:

   a. **Certificate File:** Inform the path to the certificate file.
   b. **CA File:** If the certificate is issued by a unknown CA, you should inform here the pathname to the CA certificate.
   c. **Private Key:** You should inform the pathname to the certificate private key file.
   d. **PassPhrase:** Inform the password, if there is any, used when the private key was generated.

Note: The path names can be absolute (C:\MyCertPath\UserThisCert.pem) or relative to the path where ThinRDP is installed (\cert\UserThisCert.perm).

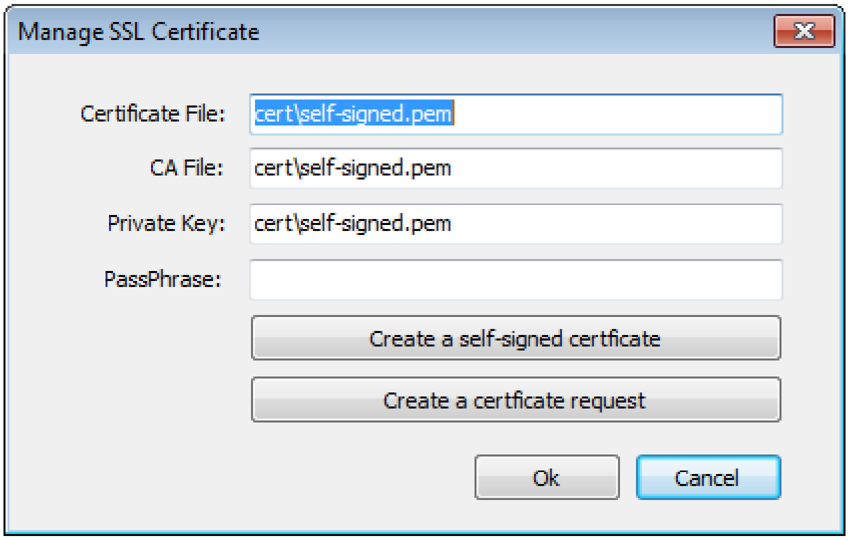
Using Dynamic DNS and Certificate Sharing:

When the "Enable Dynamic IP Address Resolution & Shared SSL Certificate" option is marked, it means that you are going to have a shared SSL Certificate provided by the https://www.thinrdp.net/ service.
In this mode, you will not be able to manage your own SSL Certificate. And for this reason the "Manage Certificate" button located on "Security Tab" will be disabled.

7.1 The default embedded certificate

Along with the ThinRDP installation, goes a certificate called "self-signed.pem". You will find it inside the \cert directory, located inside the ThinRDP application path.

If you want to use this default certificate you should have the files set as the image below:



Manage SSL Certificate

Certificate File: cert\self-signed.pem

CA File: cert\self-signed.pem

Private Key: cert\self-signed.pem

PassPhrase:

Note: Once this certificate is not issued by a known Certificate Authority (CA), the web browsers will warn you they can not verify its authority.

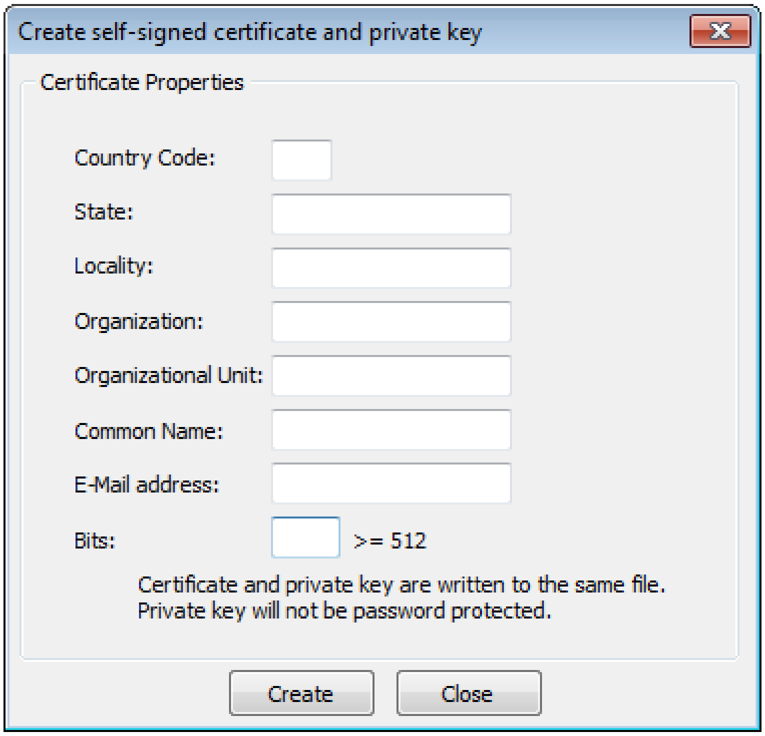
7.2 A self-signed certificate

This option is used to create your own self-sign certificate.

1. Go to the ThinRDP manager's "Security tab".

2. Press the "Create a self-signed certificate" button.

3. Fill in the form below with your organization data:



Create self-signed certificate and private key

Certificate and private key are written to the same file.
Private key will not be password protected.

4. The "Common Name" field should be filled with the server+domain that will be used to access the ThinRDP server (rdp.mycompany.com).

5. Press Create.

6. Select the location where you want the certificate to be stored.

7. The application will start using this self-signed certificate just created by you.

Note: Once this certificate is not issued by a known Certificate Authority (CA), the web browsers will warn you they can not verify its authority.

7.3 A CA certificate

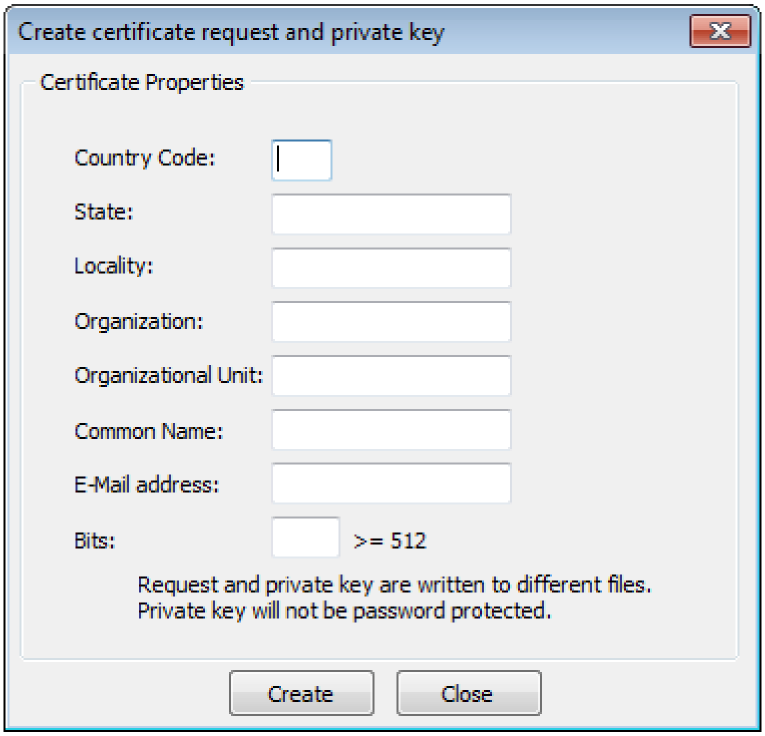
In order to use this option you will have to get a certificate from a known Certificate Authority (CA). Some CA examples are GoDaddy, VeriSign, Thawte, GeoTrust and Network Solutions.

The CA will ask you for a "certificate request". Create one following the next steps:

1. Go to the ThinRDP manager's "Security tab".

2. Click on the "Create a certificate request" button.

3. Fill in the form below with your organization data:



Request and private key are written to different files.
Private key will not be password protected.

4. The "Common Name" field should be filled with the server+domain that will be used to access the ThinRDP server (rdp.mycompany.com)

5. Press "Create" and the application will generate two files.

6. The first window will ask you a location to keep the private key file: "Where do you want the private key file to be stored".

   a. Inform a name for your private key.
   b. Select a place to keep it safe.
   c. Press the "Save" button.

7. The second window will ask you a location to keep the request file: "Where do you want the request file to be stored.".

   a. Inform a name for the request file.

b. Select a directory where you can find the file later on to send to the CA.
c. Press the "Save" button.

8. The first file is the certificate private key. It should always be kept safe with you.

9. Send only the request file to the CA.

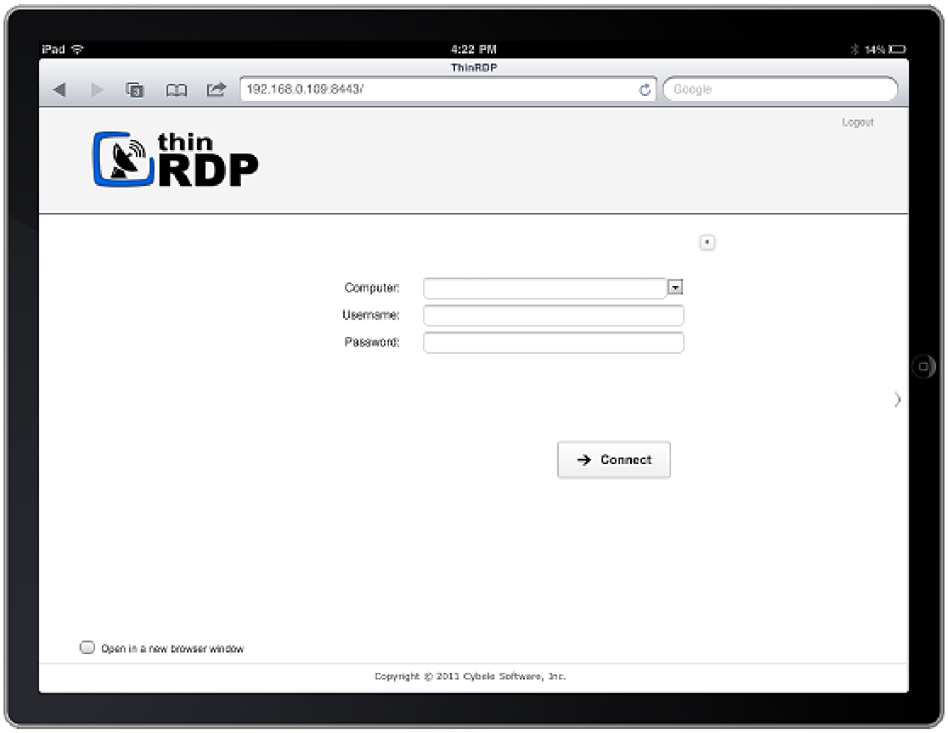
After the CA validation process, place the certificate they sent to you on ThinRDP cert directory and inform the path to the files on ThinRDP Manage Certificate option (Certificate file, CA file and Private Key).

8 Mobile devices

A great advantage you have using ThinRDP Server is the possibility to access remote desktops and applications from many different devices.

Any HTML5 compliant device can became a client of the application: iPhone, iPad, Android tablet, Chrome Book and many more.

Access the ThinRDP URL from a mobile or tablet and you will have a fully adapted interface to make the connection easier, as well as good performance and usability options specially designed for mobile devices.



Most of the mobiles and IPads are Touch Screen and it is through this screen touch you are going to control both remote desktop mouse and keyboard. Learn also about the available mobile Gestures.

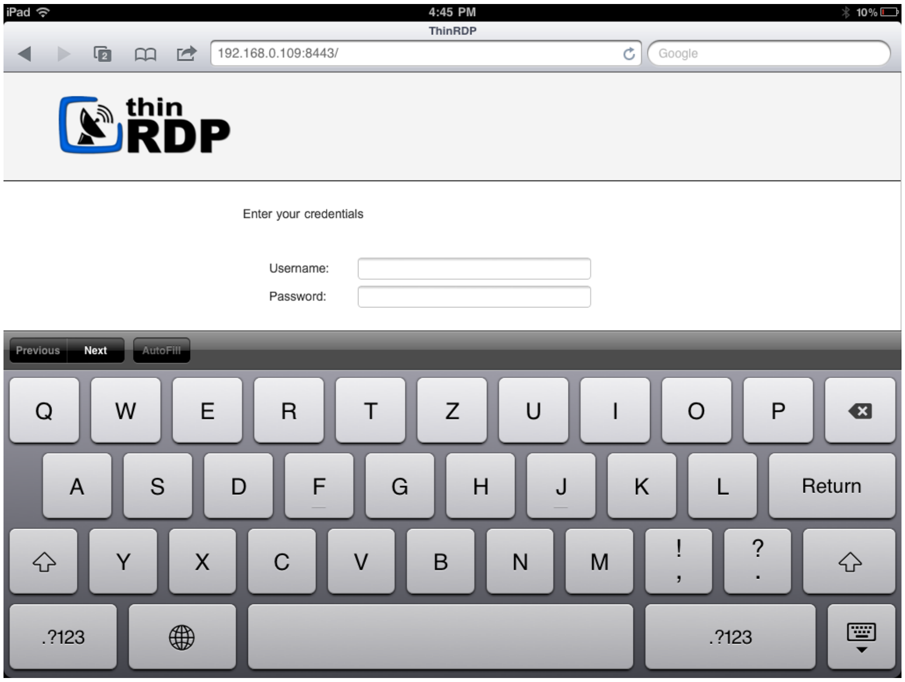
8.1 Getting into ThinRDP

When you access ThinRDP from a web browser, you will have two dialogs to fill. The first one is the application login and the second one has the connections settings you will be able to customize.

1. In order to navigate on both "Login" and "Settings" interfaces, the only thing you need to do is touch the control you want to select or enter. The "Login" and the "Settings" interfaces don't provide any kind of moving or dragging control, since there are no elements with these behavior.

2. The regular keyboard will get enabled every time you enter into a text field, so you can type in the connection information.

On the image below you can see the login interface along with the enabled keyboard.



Enter your credentials

Username:

Password:

Once you get connected with a desktop or an application, you will have many other navigability options and controls available.

Read the next topics and learn how to use these controls inside the connection.

Mouse Control

Keyboards

Gestures

Disconnecting

8.2 Mouse control

Right after you get connected to a remote desktop or application you will have available the remote desktop mouse.
Take a look on the table below how you are going to control this mouse through a mobile screen.
The third column relates the mobile gesture that corresponds to the described mouse action.

Moving the mouse around	In order to move the remote desktop mouse you should drag your finger softly touching the mobile screen. You don't need to drag your finger exactly on the mouse draw position in order to make it move. Wherever the mouse is, it will start moving. Sometimes the mouse is hidden. In that case, keep dragging the finger towards different directions until you can see it on the screen.	-
Regular click	In order to click some element on the remote desktop you need to first position the mouse draw over this element (a icon, or a menu for example). Once you have position the mouse draw over the element, give a quick touch on the element.	Tap gesture
Double click	Just like on the regular click you need to first position the mouse draw over this element you want to double click. After that give two quick touches on the element.	Double-tap
Right click	When you open a connection through a mobile, ThinRDP provides a especial side menu. The second button is used exactly to right click an element of the remote desktop. As for the regular and double click, first of all you need to position the mouse over the element you want to right click. After that touch the second side menu button (the button has a mouse picture with the right button highlighted in red).	-
Drag and drop	To drag and drop elements of the remote desktop to the following: a. Touch the element you want to drag. Do not release your finger. b. Drag the finger towards the position you want to take the element to. c. When you get to the position you wanted, release the finger from the screen.	Press and drag

8.3 Keyboards

1. Regular Mobile Keyboard

Along with most mobile device comes a logical keyboard composed by the main used keys for mobile applications.
With ThinRDP you can use any kind of application located on a remote desktop and that is why ThinRDP has two additional keyboards with all the keys the device keyboard might not support.

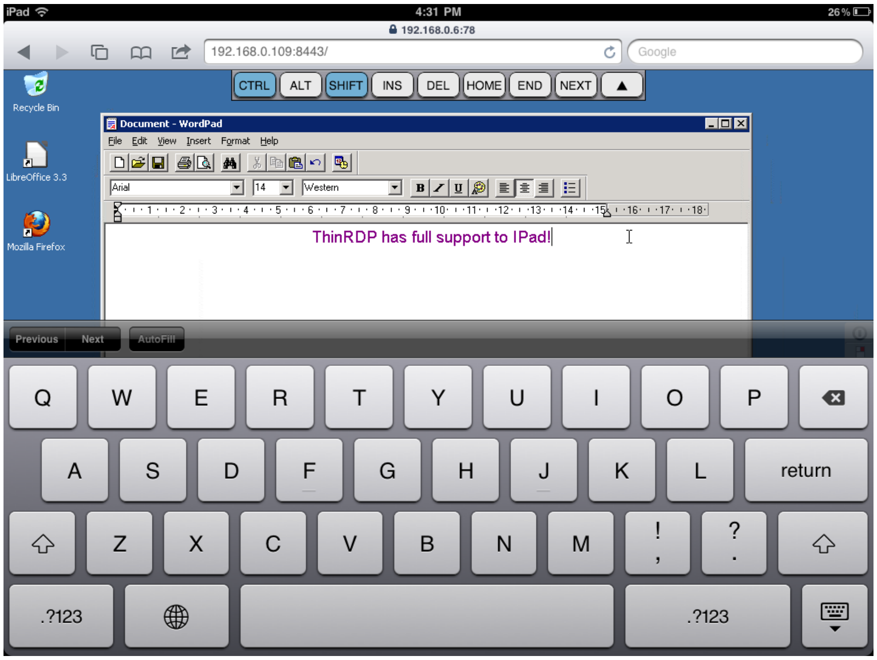
a. Enabling the regular keyboard:

I. If you are on the "Login" or on the "Settings" screen, this keyboard will get automatically enabled every time you enter a text field.
II. Once you get connected to a remote desktop or application, you should touch the last ThinRDP side menu button, in order to enable the regular keyboard.

o

b. Using the regular keyboard:

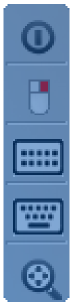
The keyboards use is very intuitive. You just have to touch the keys you want to type in.
To use numbers and special caracters, touch the "*.?123*" key.


ThinRDP has full support to IPad!

If you want to make the regular keyboard invisible, press the last button (the one with a keyboard and a down arrow draw).

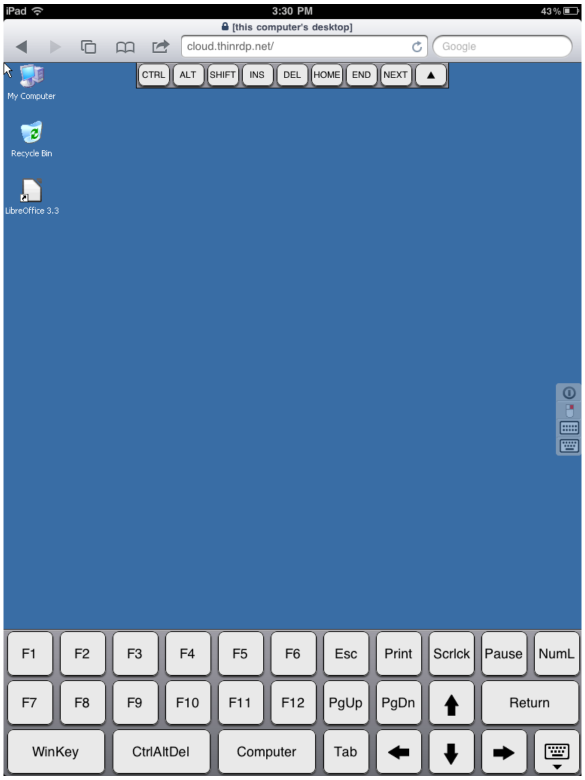
2. ThinRDP Extended Keyboard

ThinRDP has two additional keyboards.
In order to enable them you should touch the first up-down keyboard button, on the ThinRDP side menu.



a. Upper keyboard

The upper ThinRDP keyboard has the keys CTRL, ALT, SHIFT, INS, DEL, HOME, END and NEXT. This keyboard leaves the keys on until you have pressed a valid combination of them, for example, CTRL+ALT+DEL.



b. Bottom keyboard

The bottom ThinRDP keyboard has the F1-F12 keys, the arrow keys and few more, as you can check out on the up image.

If you need to disable both ThinRDP additional keyboards, press the last bottom keyboard key (the one with a keyboard and a down arrow below draw).

8.4 Gestures

These are the gestures ThinRDP provides to improve the experience of mobile device users. Learn which they are and what are the circumstances you can use them:

Regular known gestures:

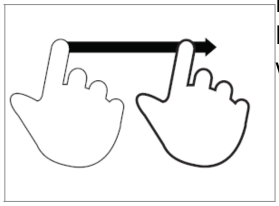
Tap
Briefly touch surface with fingertip

Mouse correspondent
Single-click

Double-tap
Rapidly touch surface twice with fingertip

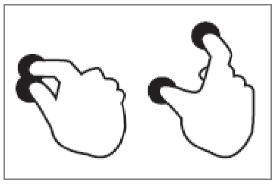
Mouse correspondent
Double-click

Special gestures:



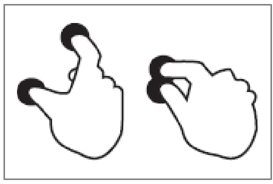
Press and Drag
Move one fingerprint over surface without losing contact

Where
On the Connection Screen you can drag and drop an object using the Press and Drag gesture.



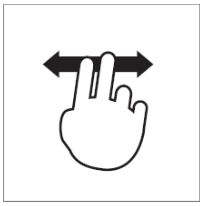
Spread
(zoom in)

Where
On the Connection Screen you can use the Spread gesture to zoom the screen in.



Pinch
(zoom out)

Where
On the Connection Screen you can use the Pinch gesture to zoom the screen out.

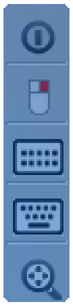


Double finger drag
Move two fingertip over surface without losing contact

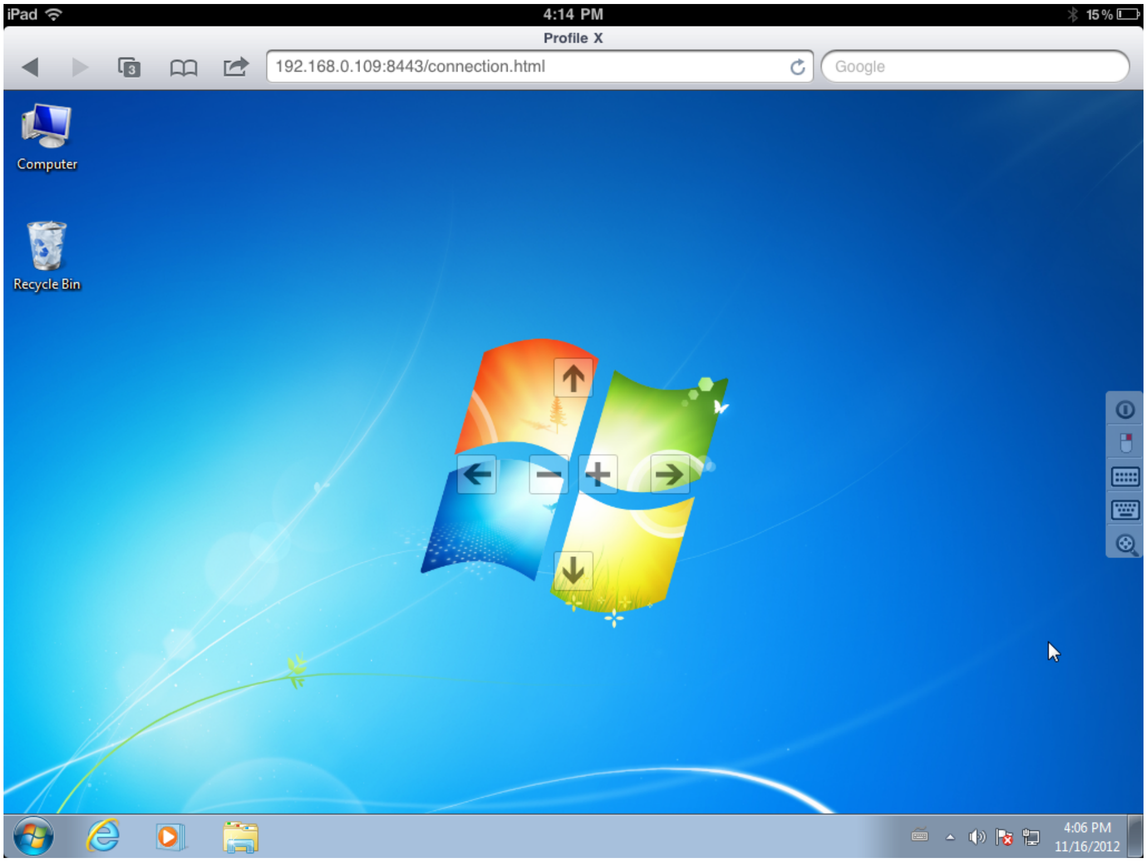
Where
It the Connection Screen is magnified, you can use the "Double finder drag" to move the screen in different directions.

8.5 Zoom

On the right-side connection menu for mobiles, the last button enables the zoom controls on the screen.



Click on the zoom button, and its controls will be shown in the middle of the screen as the image below:



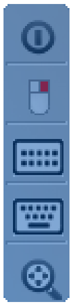
Find below how each one of the zoom controls works and the gesture that is related to it:

+	Zoom In	Spread gesture

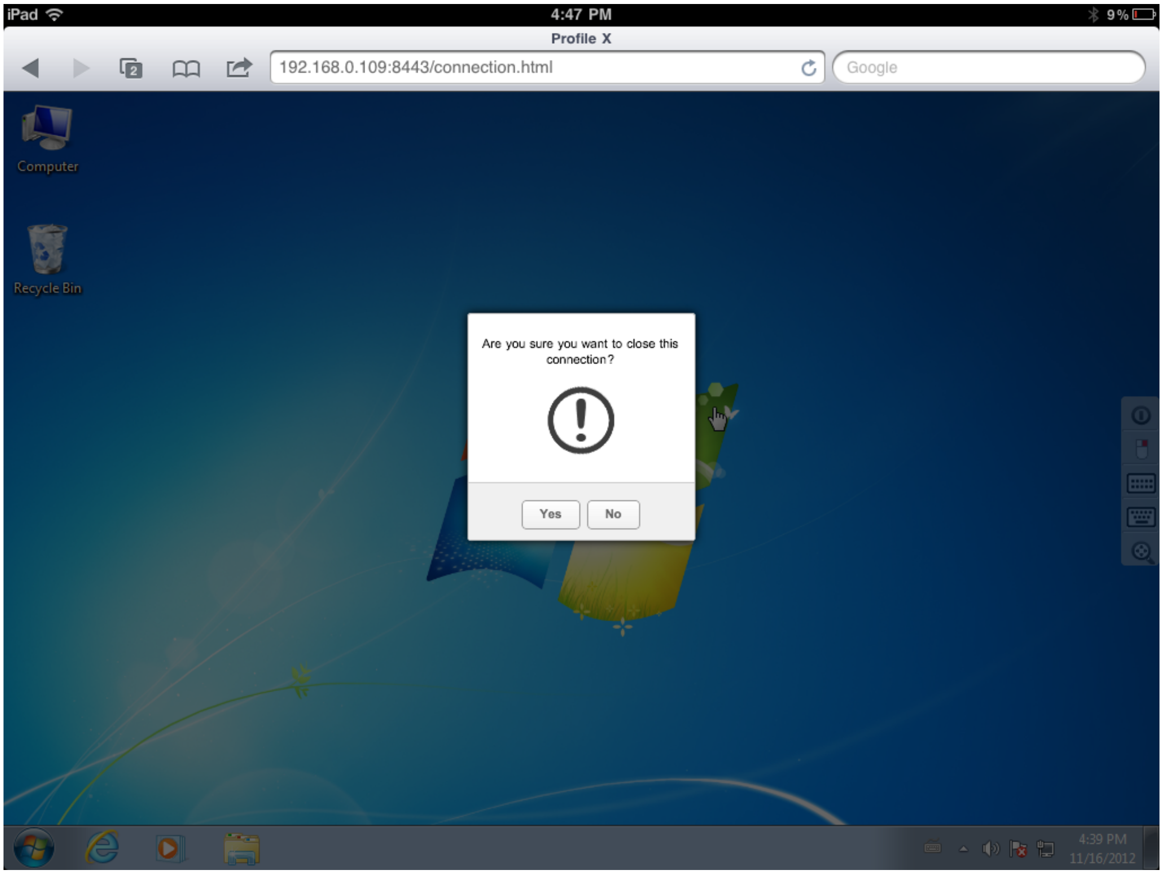
−	Zoom Out	Pinch gesture
→	Move the screen to the right	Double finger drag
←	Move the screen to the left	Double finger drag
↑	Move the screen up	Double finger drag
↓	Move the screen down	Double finger drag

8.6 Disconnecting from ThinRDP

1. In order to disconnect from the remote desktop touch the upper button located on the ThinRDP right side menu.



2. After touching the disconnect option you will receive a confirmation message. Touch "Yes" if you really want to disconnect from the remote desktop, otherwise touch "No".



Are you sure you want to close this connection?

9 Integrating ThinRDP

ThinRDP was designed to interoperate with many different applications.
Find below the ways you can integrate ThinRDP with other applications:

Integration through the SDK library

Performing an External Authentication to ThinRDP

Integrating ThinRDP in a Single-Sign-On schema

Customizing the Web Interface

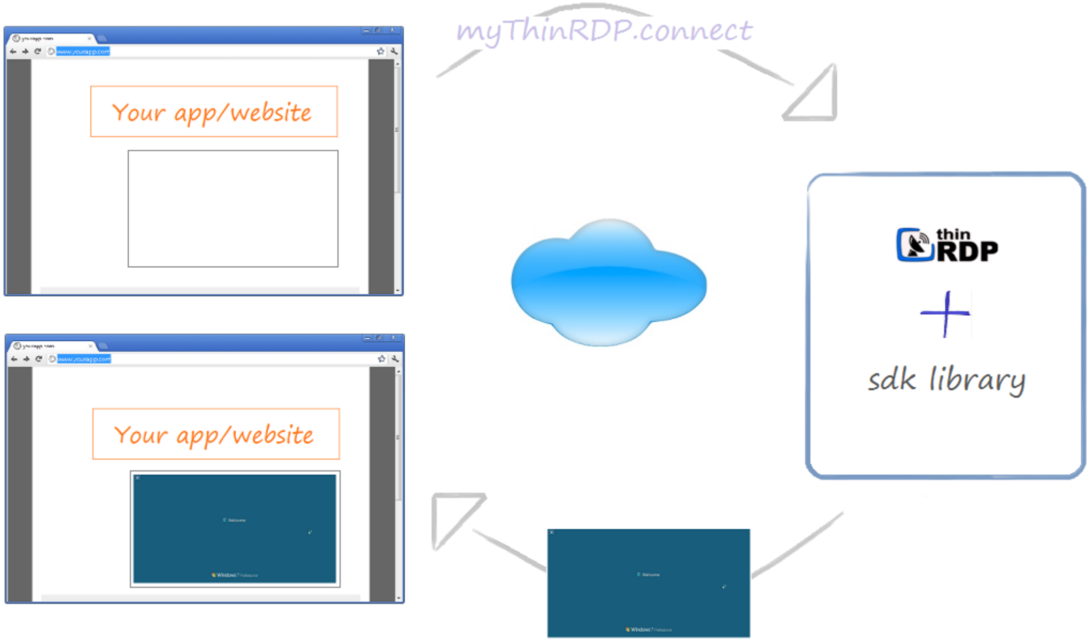
Integration through the Web Service API

Allowing access through the One-Time-URL

If you need to integrate ThinRDP with your own application in a different way, contact us, and let us know your specific integration needs. We will evaluate the scenario and let you know the viability of the integration development.

9.1 SDK

The SDK library allows you to integrate your own website or web application with *ThinRDP Server*, so that you can have a fully functional remote desktop or remote application inside your application .



Requirements for the SDK Library:

1. The website or application target has to be HTML5 compliant.
2. The integration has to be done at a programming level. This is why you will need someone who can modify the target website or application source.

You can use the SDK library with any ThinRDP authentication mode: None, Username/password or Access Profiles.

The integration of ThinRDP with your application will require the edition of an HTML page, adding a few tags and some JavaScript code.
From this point on, we consider you already have ThinRDP installed and configured. Otherwise, please go back to the Getting Started topic.

To learn how to use the SDK library read the next topics:

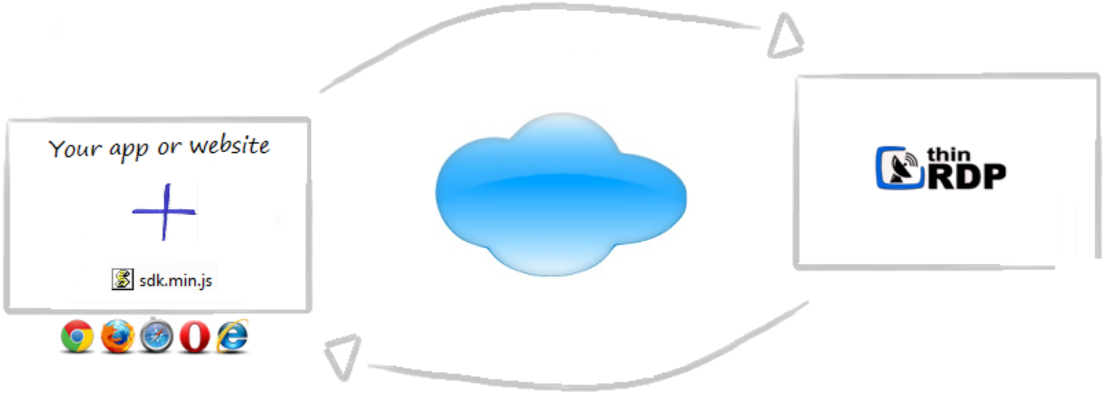
Deploying
Using the SDK
The Connect Method
Events
Keystrokes methods
SSL Certificate

Demos

Tip: You can also take a look at the sdk.html file available in the ThinRDP Server installation directory, under the 'webrdp' folder. After configuring the parameters for the connect method, located inside this html example file, you can try it out from the browser through the address https://server_IP:port/sdk.html.

9.1.1 Deploying

In order for ThinRDP SDK to work all you need is the sdk.min.js and the jquery libraries to be accessible from your app/website:



Add a script tag pointing to the ThinRDP SDK client library: sdk.min.js in the HTML file where you will call the ThinRDP connect method from.
It is recommended that you deploy this file within your website/web app environment for better performance.

Quick setup guide:

1. Copy the sdk.html and sdk.min.js files to your website/web application environment.
2. Edit the sdk.html file: Set the GetThinRDP method first parameter to the ThinRDP server URL following this format: https://127.0.0.1:8443.
3. Also modify the `computer`, `username` and `password` properties to match the remote machine IP and credentials, respectively.
4. Save the changes.
5. Access sdk.html from your website/app environment and press OK on the "connected" and "session start" messages.
6. The page should now show the remote connection (accessed from an external html file).

Tip: The sdk.html file is a demo to quickly try out the ThinRDP SDK integration using the local connection mode, but also it can be used as a template to modify the HTML file you want to embed ThinRDP in.

9.1.2 Using the SDK

Before you actually begin to code:

1) Verify in the ThinRDP Server settings whether you are using "Access Profiles" as the authentication mode. If you do use "Access Profiles", make sure you already have created and configured the profile to be used on this integration.

2) You will be able to place a ThinRDP connection in three different html structures:

a. A new browser window
b. An iFrame placed inside an existing Web Page
c. A div placed inside an existing Web Page

If you want the ThinRDP connection to open in a new browser window (a) or inside an iFrame (b) the connection mode should be set to "Remote". Otherwise, if you want to embed the connection inside in a div (c), the connection mode should be "Local". You will need this information on HTML configuration step 5b below.

Modify your HTML file step-by-step:

1. Open the HTML page you are going to integrate with ThinRDP SDK for editing.

2. Add these meta tags into the <head> tag:

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="chrome=1"/>
```

3. If you want the ThinRDP integration to work under iOS, add the following <meta> tags into the <head> tag.

```
<link rel="apple-touch-icon" href="images/icon.png"/>
<meta name="apple-mobile-web-app-capable" content="yes" />
<meta name="viewport" content="width=device-width, initial-scale=1.0,
maximum-scale=1.0, minimum-scale=1.0, user-scalable=no, target-
densityDpi=device-dpi"/>
```

4. Add the following libraries inside the <head> tag:

a. The jQuery library (jquery.min.js):

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.6.1/
jquery.min.js" type="text/javascript"></script>
```

b. The ThinRDP SDK client library (sdk.min.js): this file will have to be deployed with your website/ application.

```
<script src="sdk.min.js" type="text/javascript"></script>
```

5. Also inside the <head> tag, add one more <script> tag. This one will be used to create the connection with the remote desktop. If the page already has a script tag, just append this code into the `$(document).ready` method.
The GetThinRDP method creates the object that handles the ThinRDP SDK functionality. It has two arguments: the ThinRDP server URL and the connection mode in which ThinRDP SDK will work.
The connect method is the method that creates the connection and positions it on the structure you have selected (div, iFrame, Window).

```
<script type="text/javascript">
    var mythinrdp;
    $(document).ready(function () {
        mythinrdp = GetThinRDP("ThinRDP server URL", connection mode);
        mythinrdp.connect({
                            //Read the "The connect method" to complete
all the expected parameters
        });
    });
</script>
```

a. Substitute the "`ThinRDP server URL`" argument for the getThinRDP method with the ThinRDP protocol + Computer's IP + Port, following this format: https://127.0.0.1:8443.

b. Substitute the getThinRDP second argument with the connection mode:

Mode	How it works	Where you can place the connection
Local (remote =false)	The connection is embedded in the same page and after the connection is established, the data exchange is sent directly to your website/ application, through the sdk.min.js library.	div
Remote (remote=true)	The sdk.min.js posts into ThinRDP Server and all the remote desktop data is exchanged through the ThinRDP Server JavaScript scripts. The connection will occupy the whole target window area (window or iFrame).	browser window or IFrame

c. Find out in the next sub-topic ("Connect method") how you should complete the parameters that go along with the connect method, and substitute the text on the connect method.

6. If you are using the "Local" connection mode you can code special behaviours for the available ThinRDP SDK events and keystrokes,.

9.1.3 Connect method

The "connect" method creates a connection with the remote machine and positions the remote desktop connection on the specified html structure. In order to do so, it expects a JSON argument in which all the connection settings should be informed.
If you want to understand exactly how each JSON parameter will reflect on the connection, read the next topics:

Placement parameters

Destination and Authentication parameters

Settings parameters

Features parameters

Events parameters

Right below you will find the connect method with all the possible parameters set. They should not be sent all together, because each environment will require different parameters to be set:

- The Placement parameters will be required depending on the connection mode (remote or local).
- The Destination and Authentication parameters will be required depending on the authentication mode set on ThinRDP manager.
- The other parameters (Settings, Features and Events) are optional and should be sent whenever you need to change a determined ThinRDP behaviour or enable and configure its features.

```
mythinrdp.connect({
                    // Placement
                    targetWindow: "substitute with the iframe id or window name",
                    postpage:     "connection.html",
                    exitURL :     "about:blank",
                    divId :       "deskdiv",

                    // SDK Settings
                    centered:         false,
                    overrideDefaults: false,
                    showOnStart:      true,
                    showToolbar:      false,
                    hidePointer:      false,
                    kbdControl:      true,
                    mouseControl:      true,
                    tcpReadCount:      true,
                    tcpReadWait:      true,

                    // Tab General
                    profileKey: "substitute with the profileKey if using Access
Profiles",
                    computer:   "substitute with the remote desktop/application IP",
                    username:   "substitute with the remote desktop username
credential",
                    password:   "substitute with the remote desktop password
credential",
                    askForCredentials: false,
                    disablenla: false,
                    desttype:   "substitute with the destination type (for VM's)",
                    destinfo:   "substitute with the destination info (for VM's)",

                    // Tab Program
                    startprg: 0,
                    command:   "substitute with the app path",
                    directory: "substitute with the app context dir",
                    cmdargs:   "substitute with the app arguments",

                    // Tab Display
                    bpp: 16,
                    resolution:"fittobrowser",
                    width: $(window).width(),
                    height: $(window).height(),
                    imagequality: 1,
                    clientAck: 0,

                    // Tab Experience
                    experience: {
                            desktopbackground: false,
                            visualstyles: false,
                            menuwindowanimation: false,
                            fontsmoothing: false,
                            showwindowcontent: false,
                            desktopcomposition: false
                    },

                    // Tab Advanced
                    unicodekeyboard: true,
                    kbdLayout: "substitute with remote desktop keyboard layout",
                    console: false,
                    wscompression: true,
                    relativeTouch: true,  //mobile
                    disableExtKeys: true, //mobile
                    tbSize: "medium",     //mobile

                    // Tab Resources
                    printer: {
                            enabled: false,
                            setasdefault: true,
                            name: "substitute with the printer name",
                            driver: "substitute with the printer driver"
                    },
                    clipboard: true,

                    disk: {
                            enabled: true,
                            name: "substitute with your desired disk name"
                    },

                    sound: {
                            enabled: true,
                            quality: -1
                    },

                    // Events
                    events: {
                            onServerConnecting           : function (reconnecting)
{ },
                            onServerConnect              : function () { },
                            onQueryDisconnect            : function () { },
                            onServerConnectionError      : function (errMessage)
{ },
                            onServerDisconnect           : function () { },
                            onExecResult                 : function (cmd) { },
                            onSessionStart               : function () { },
                            onSessionEnd                 : function (message) { },
                    }

                    // Toolbar customization
                    createToolbar:      true,
                    toolbarVisible:      true
});
```

9.1.3.1 Placement

These are all the parameters related to the ThinRDP connection placement.
Some of the parameters should be sent only when the connection mode is set to Remote and some of them should be sent only when the connection mode is Local.

Parameter	What it means	Type/format	Default	send when mode	
				remote	local
`targetWindow`	Inform "_self" to have the connection open over the current window. The "*" value will open a new window with a name assigned by ThinRDP. If you inform an existing window name or iframe id, ThinRDP will position the connection on this target and if the target does not exist, a new window will be created with that name.	**string** "*" , "_self" , target window (iframe id or window name)	"_self"	yes	no
`exitURL`	Assign a URL to redirect to after the connection has closed.	**string** URL	"about:blank"	yes	no
`postpage`	This parameter configures the server HTML file. The embedded file name is 'connection.html'. You only have to change this value in case you have customized this file.	**string** html file name		yes	no
`divId`	div id where the remote desktop will be placed, when using local mode.			no	yes

9.1.3.2 Destination and Authentication

Find below all the parameters related to the connection destination and authentication.
The last three columns of the table will let you know what parameters should be sent depending on the authentication mode used.

Parameter	What it means	Type/format	Default	Profile	Digest	None
`profileKey`	Key that identifies a profile in order to establish the connection through it. The profileKey access key must be sent when you using "Access Profiles". You will find the key information while Editing a profile.	**string** profile key		must	must not	must not
`computer`	The remote desktop IP and port to connect to. For "None", "Username/Password" as authentication mode or for the [any computer] profile you will have to specify the computer parameter.	**string** IP:Port		must not	must	must
`username`	The remote desktop username credential.	**string** username		could	could	could
`password`	The remote desktop password credential.	**string** password		could	could	could
`askForCredentials`	The askForCredentials parameter set to true, will make sure that whenever the username or password values to authenticate against the remote machine are not available, ThinRDP will prompt the user to inform them. If the askForCredentials is set to false, no dialog will be shown to the user and in case there is no password or username to	**boolean** true,false	false	could	could	could

	authenticate, the user will not be able to log in.					
overrideDefaults[1]	If you are using Access Profiles as authentication mode and set this property is set to true, most of the Profile settings will be overridden by the parameters sent on the Connect method.	**boolean** true,false	false	could	must not	must not
disablenla[2]	Set the option disableNLA if you use a CredSSP other than Microsoft on the Remote Machine.	**boolean** true,false	false	could	must not	must not

[1]. The properties computer, profileKey, startprg and command can not be overridden for security reasons.
[2]. This option will only be considered by ThinRDP if you are not using profiles as authentication mode, or for the any computer profile.

If you wish to use the integration in order to connect to a specific application/program, set the following parameters:

Parameter	What it means	Type/format	Default	Profile	Digest	None
startprg	Sets the launching application mode. Set 0 for "Do nothing" option; 1 for "Start a program" option; 2 for "Launch RemoteApp" option.	**integer** 0,1 or 2	0	could	could	could
command	Full remote application path that should start upon connection establishment.	**string** app path		could	could	could
directory	Initial context directory to be used by the application set on command parameter described above.	**string** dir path		could	could	could
cmdargs	Arguments to start the application specified on the "command" property.	**string** app args		could	could	could

If you want to establish Hyper-V or RDS collection VM connections, set the parameters below:

Parameter	What it means	Type/format	Default	Profile	Digest	None
desttype[2]	Set the desttype to "VMID" in case you want to establish a connection to a Hyper-V Virtual Machine or set "RDS" if you want to create a connection to an RDS Collection VM. The connection will act as a regular connection in case you don't inform this property of inform any value different from "VMID" and "RDS".	**string** VMID or RDS		could	could	could
destinfo[2]	Inform the Virtual Machine ID, for Hyper-V Virtual Machine connections or inform the TSV URL for RDS Collection Virtual Machines.	**string** Virtual Machine ID or TSV URL		could	could	could

[2]. This option will only be considered by ThinRDP if you are not using profiles as authentication mode, or if you are connecting through the any computer profile.

9.1.3.3 Settings

These are all the settings that can be configured through ThinRDP SDK.
If you are using Access Profiles, you should set the parameter 'overrideDefaults' to true, in order to have these settings considered on the connection, otherwise the profile's predetermined settings will be used.

Parameter	What it means	Type/format	Default
showOnStart	Set to false in order hide the Windows start up and logon process. In this case you will have to call the div 'show' method on the startSession event. A "wait" message will be shown until the session starts.	**boolean** true,false	true
showToolbar	Set to false to hide the ThinRDP toolbar	**boolean** true,false	true
centered	Configures whether the connection should be centered on the browser window or not. On certain cases, this parameter set to false might prevent flickering.	**boolean** true,false	true
bpp	Color Depth: sets the number of bits per pixel. Set 8 for 256 colors; 15 for True Color (15 bit); 16 for True Color (16 bit) ; 24 for True Color (24 bit)	**integer** 8,15,16 or 24	16
resolution	"fittobrowser", "fittoscreen", "fixed". When fixed, the width and height parameters will be considered.	**string** toolbar size	"fittobrowser"
width	Remote desktop screen width. It will only be considered when the 'resolution' parameter is set to "fixed".	**integer** pixels	$("#deskdiv").width()
height	Remote desktop screen height. It will only be considered when the 'resolution' parameter is set to "fixed"	**integer** pixels	$("#deskdiv").height()
imagequality	Specifies the image quality/compression. Set 0 for "Highest!; 1 for "Optimal"; 2 for "Good"; 3 for "Faster"	**integer** 0,1,2 or 3	1
clientAck	This parameter sets the number of images sent from the server to the client at a time. It can prevent slow connections from timing out. The faster the connection is, the higher clientAck parameter should be set. The default value (0) does not control the number of images, sending the images all together.	**integer**	0
unicodekeyboard	Allows for using full unicode keyboard charsets. Set to false to connect to xRDP servers.	**boolean** true,false	true
console	Forces the connection to the remote console session.	**boolean** true,false	false
wscompression	Set to true to enable the compression for the exchanged Websocket data and have the application performance improved.	**boolean** true,false	true
relativetouch	Set to false in order to disable this behaviour in mobile devices.	**boolean** true,false	true
disableExtKeys	Set to true if you do not want the ThinRDP extra keys to appear on mobile interfaces.	**boolean** true,false	false
tbSize	Configure the size of the mobile right side toolbar. The possible values are 'small', 'medium' and 'large'.	**string** toolbar size	'medium'
hidePointer	Hides the mouse pointer	**boolean** true,false	false
kbdControl	Enables control of the keyboard	**boolean** true,false	true
mouseControl	Enables control of the mouse	**boolean** true,false	true

`kbdLayout`	Sets the keyboard layout for the remote desktop. When it is not completed, the default keyboard layout is English. Read a reference of accepted values.	**string** Keyboard code.	"1033"
`tcpReadCount`	Number of operation cycles before sending the commands to the browser. Adjust this, together with tcpReadWait, according to your environment to reach maximum effectivity.	**integer** cycles	1
`tcpReadWait`	Waiting time between operation cycles before sending the commands to the browser. Adjust this, together with tcpReadCount, according to your environment to reach maximum effectivity.	**integer** miliseconds	20

Experience settings:

Parameter	What it means	Type/format	Default
`experience.desktopbackground`	Set to true to show the original remote desktop background.	**boolean** true,false	false
`experience.visualstyles`	Set to true to change the start menu and other Windows style features.	**boolean** true,false	false
`experience.menuwindowanimation`	Set to true to show an animation on the Windows start menu.	**boolean** true,false	false
`experience.fontsmoothing`	Set to true to make text easier to read, specially the magnified text.	**boolean** true,false	false
`experience.showwindowcontent`	Set to true to show windows contents while dragging them.	**boolean** true,false	false
`experience.desktopcomposition`	Set to true to configure the DWM to redirected the desktop drawing to off-screen surfaces in video memory. The desktop will also present many visual effects.	**boolean** true,false	false

9.1.3.3.1 kbdLayout values

This option ultimately de

pends on the languages installed in the remote computer. Use:

```
    kbdLayout: "1078",
```

to set the remote keyboard layout to "Afrikaans". Below is a table showing possible values for the keyboard layout parameter.

Value	Keyboard Layout
1033	US
1052	Albanian
1025	Arabic (101)
66561	Arabic (102)
132097	Arabic (102) AZERTY
1067	Armenian Eastern
66603	Armenian Western
1101	ASSAMESE - INSCRIPT
2092	Azeri Cyrillic
1068	Azeri Latin
1133	Bashkir
1059	Belarusian
67596	Belgian (Comma)
2067	Belgian (Period)
2060	Belgian French
1093	Bengali
132165	Bengali - INSCRIPT
66629	Bengali - INSCRIPT (Legacy)
8218	Bosnian (Cyrillic)
1026	Bulgarian
66562	Bulgarian (Latin)
197634	Bulgarian (phonetic layout)
132098	Bulgarian (phonetic layout)
4105	Canadian French
3084	Canadian French (Legacy)
69641	Canadian Multilingual Standard

2052	Chinese (Simplified) - US Keyboard
1028	Chinese (Traditional) - US Keyboard
1050	Croatian
1029	Czech
66565	Czech (QWERTY)
132101	Czech Programmers
1030	Danish
1081	Devanagari-INSCRIPT
1125	Divehi Phonetic
66661	Divehi Typewriter
1043	Dutch
1061	Estonian
1080	Faeroese
1035	Finnish
67643	Finnish with Sami
1036	French
71689	Gaelic
55	Georgian
132151	Georgian (Ergonomic)
66615	Georgian (QWERTY)
1031	German
66567	German (IBM)
1032	Greek
66568	Greek (220)
197640	Greek (220) Latin
132104	Greek (319)
263176	Greek (319) Latin
328713	Greek Latin
394248	Greek Polytonic
1135	Greenlandic
1095	Gujarati

1037	Hebrew
66617	Hindi Traditional
1038	Hungarian
66574	Hungarian 101-key
1039	Icelandic
2141	Inuktitut - Latin
66653	Inuktitut - Naqittaut
6153	Irish
1040	Italian
66576	Italian (142)
1041	Japanese
1099	Kannada
1087	Kazakh
1107	Khmer
1042	Korean
1088	Kyrgyz Cyrillic
1108	Lao
2058	Latin American
1062	Latvian
66598	Latvian (QWERTY)
66599	Lithuanian
1063	Lithuanian IBM
132135	Lithuanian New
1134	Luxembourgish
1071	Macedonian (FYROM)
66607	Macedonian (FYROM) - Standard
1100	Malayalam
1082	Maltese 47-Key
66618	Maltese 48-key
1153	Maori
1102	Marathi

2128	Mongolian (Mongolian Script)
1104	Mongolian Cyrillic
1121	Nepali
1044	Norwegian
1083	Norwegian with Sami
1096	Oriya
1123	Pashto (Afghanistan)
1065	Persian
66581	Polish (214)
1045	Polish (Programmers)
2070	Portuguese
1046	Portuguese (Brazilian ABNT)
66582	Portuguese (Brazilian ABNT2)
1094	Punjabi
1048	Romanian (Legacy)
132120	Romanian (Programmers)
66584	Romanian (Standard)
1049	Russian
66585	Russian (Typewriter)
133179	Sami Extended Finland-Sweden
66619	Sami Extended Norway
3098	Serbian (Cyrillic)
2074	Serbian (Latin)
1115	Sinhala
66651	Sinhala - wij 9
1051	Slovak
66587	Slovak (QWERTY)
1060	Slovenian
66606	Sorbian Extended
1070	Sorbian Standard
1034	Spanish

66570	Spanish Variation
1053	Swedish
2107	Swedish with Sami
4108	Swiss French
2055	Swiss German
1114	Syriac
66650	Syriac Phonetic
1064	Tajik
1097	Tamil
1092	Tatar
1098	Telugu
1054	Thai Kedmanee
132126	Thai Kedmanee (non-ShiftLock)
66590	Thai Pattachote
197662	Thai Pattachote (non-ShiftLock)
1105	Tibetan (People's Republic of China)
66591	Turkish F
1055	Turkish Q
1090	Turkmen
1152	Uighur
1058	Ukrainian
132130	Ukrainian (Enhanced)
2057	United Kingdom
1106	United Kingdom Extended
66569	United States - Dvorak
132105	United States - International
197641	United States-Devorak for left hand
263177	United States-Dvorak for right hand
1056	Urdu
2115	Uzbek Cyrillic
1066	Vietnamese

1157	Yakut

9.1.3.4 Features

Each ThinRDP Feature requires a set of parameters to be enabled and configured. Find below how you can use ThinRDP features through the SDK integration:

Clipboard:

Parameter	What it means	Type/format	Default
clipboard	Set to false in orderto disable the remote desktop clipboard. The clipboard w orks for text only.	**boolean** true,false	true

Printer:

Parameter	What it means	Type/format	Default
printer.enabled	Set to true in order to enable ThinRDP PDF printer.	**boolean** true,false	false
printer.setasdefault	ThinRDP printer as the remote default printer.	**boolean** true,false	true
printer.name	Specify the printer name that you w ant to be show n on the remote machine's printer list.	**string** name	
printer.driver	Mark this option to set ThinRDP printer as the remote machine default printer.	**string** driver	

Disk:

Parameter	What it means	Type/format	Default
disk.enabled	Set to false in order to disable Intermediate Disk.	**boolean** true,false	true
disk.name	Specify the disk name that you w ant to be show n on the remote machine's.	**string** name	"ThinDisk"

Sound:

Parameter	What it means	Type/format	Default
sound.enabled	Set to true in order to enable remote sound.	**boolean** true,false	false
sound.quality	Sets the sound quality. 0 = Excellent, 1 = Optimal, 2 = Good and 3 = Poor.	**integer** 0, 1, 2 or 3	1

9.1.3.5 Events

The events parameter allows you to handle each one of the available ThinRDP events from the SDK.

```
events: {
            onServerConnecting            : function (reconnecting) { },
            onServerConnect               : function () { },
            onQueryDisconnect             : function () { },
            onServerConnectionError       : function (errMessage) { },
            onServerDisconnect            : function () { },
            onExecResult                  : function (cmd) { },
            onSessionStart                : function () { },
            onSessionEnd                  : function (message) { },
    }
```

Observe on the code above that all the event functions are empty. On the following table you can find a description, parameters and a use example for each one of the available events:

Event	Parameters	When it is triggered	Example

onServerConnecting	reconnecting	This event is fired during the server connection establishment.
		The 'reconnecting' argument informs whether this is a reconnection or a first-time connection.
			onServerConnecting :
			function (reconnecting) {
			$.blockUI("Establishing connection");
			}

onServerConnect	obj	The "onServerConnect" event is fired every time a "connect" command is exchanged between the browser and the ThinRDP Server. It is a way of making sure the server received a sent "connect" command.
		If you have shown a message on the onServerConnecting, this would be a good moment to hide that message ($.unblockUI ();).
		The 'obj' parameter ships the generated connection object.
			onServerConnect :
			function (obj) {
			$.unblockUI();
			}

onQueryDisconnect	-	Anytime the Web client is about to be disconnected, the "onQueryDisconnect" will be triggered. This is useful to ask the user for confirmation before proceeding to disconnect.	onQueryDisconnect: function () {
			if (confirm("A remote session is active. Are you sure you want to disconnect?"))
			{
			    mythinrdp.disconnect();
			}
			}

onServerConnectionError	errMessage	If an error prevents the client connection to be established, this event will be fired. The errMessage argument brings the error message.	onServerConnectionError: function (errMessage){
			alert("connect error: " + errMessage);
			}

onServerDisconnect	-	Anytime the Web client gets disconnected from the ThinRDP server, the "onServerDisconnect" event will be fired. It could be triggered because the connection was lost incidentally or also because the user disconnected from the server on purpose.	onServerDisconnect: function () {
			alert("disconnect");
			$.unblockUI();
			mythinrdp.updateTools();
			$("#" + mythinrdp.rcParams.divId).hide();
			}

onExecResult	cmd	This event fires only when the SDK is integrated with a remoteApp application. Through this event it is possible to get to know if the remoteApp was started or if there was an error during the application start up. If the application was started without errors, the cmd.rc is going to be 0, otherwise cmd.rc will carry the application error code. As you can see on the example below you can also get the executable name accessing the cmd.exename value.	onExecResult: function (cmd) {
			alert("exename: " + cmd.exename + " rc: " + cmd.rc);
			}

onSessionStart	-	This event will be fired when the client session has been started on ThinRDP Server.	onSessionStart: function () {
			$("#" + mythinrdp.rcParams.
			divId).show();
			mythinrdp.updateTools();
			}

onSessionEnd	message	As soon as the client Session is closed, the "onSessionEnd" event will be fired.	onSessionEnd: function (message)
			{
			alert(message);
			},

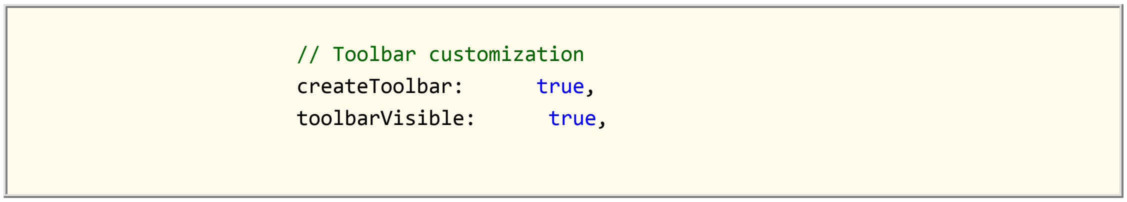
These event usage reference can also be found in the sdk.html file, located in the application directory, under the "webrdp" directory.

In versions previous to 2.2.0.20 the SDK events had a different syntax. That old sintax is still compatible with newer versions. However, it is highly recommended to translate the old code to the method described above.
This is how the previous event names are related to new ones:

Old Event Name	Current Event Name
establishingConnection	onServerConnecting
serverConnect	onServerConnect
execResult	onServerConnect
sessionStart	onSessionStart
serverConnectionError	onServerConnectionError
disconnectConfirmRequest	onQueryDisconnect
serverDisconnect	onServerDisconnect
sessionEnd	onSessionEnd

9.1.3.6 Toolbar Customization

The toolbar customization parameters allow you to restrict partially or totally the user's options by eliminating buttons from the ThinRDP toolbar's defaults.



```
// Toolbar customization
createToolbar:      true,
toolbarVisible:      true,
```

Observe on the code above that for the toolbar Res trictions parameter all the options are included for visibili typurposes. In this case the toolbar would have no buttons. The same can be accomplished by "createToolbar":false.

In the following table you can find a description of each parameter along with its type/format and default value.

Parameter	What it means	Type/format	Default

`createToolbar`	Set to false to have all the ThinRDP connections not have the ThinRDP toolbar above the remote desktop. This is useful if you want to keep users from sending keystroke combinations.	**boolean** true,false	true
`toolbarVisible`	Set to true to have the ThinRDP toolbar start expanded. Without modifying this value, the toolbar will start collapsed and the user needs to click on a button the expand it. This is useful if you think the ThinRDP toolbar settings should be displayed so it's more evident to users.	**boolean** true,false	true

Read more about the ThinRDP toolbar and how to customize it.

9.1.4 Browser resizing

When the browser window is resized by the end-user, you can make the connection resize proportionally to the new environment dimensions.
To do that you can perform a reconnection against ThinRDP Server (mythinrdp.restart()) on the browser resize event, so that the remote screen size will be updated with the new browser size.
Here is a code example that can be placed on the $(document).ready :

```
var resizeTimeout = null;
var waitToResize = 1000; // 1000 = 1 second (-1 deactivates it)


if (waitToResize != -1) $(window).bind("resize", restartToNewSize);

function restartToNewSize() {

    if (mythinrdp && mythinrdp.connected) {

        if (resizeTimeout) window.clearTimeout(resizeTimeout);
        resizeTimeout = window.setTimeout(function () { mythinrdp.
        restart();}, waitToResize);

    }

}
```

9.1.5 Keystroke methods

Some keyboard keystroke combinations are not sent to the remote machine because they are intended to work only on the local environment.
Through ThinRDP SDK library it is possible to send any keystroke combination to the server by using a list of methods available in any ThinRDP instance you create.

The table below lists and describes those methods.
The first four methods are general base methods that once combined could generate any keystroke sequence.
The last eight methods are commonly used key combinations that might be useful to enhance functionality to your ThinRDP integration.

Method	Behaviour	Arguments
sendText(textValue)	This method sends a plain text value to the current remote cursor position.	textValue **String** Text to be sent

sendKeyStroke (keyCode)	The sendKeyStroke method sends a key code, emulating the key's press and release sequentially.	keyCode **Number** Unicode representing the key the user pressed and released
sendKeyDown(keyCode)	Sends a key down.	keyCode **Number** Unicode representing the key the user pressed
sendKeyUp(keyCode)	Sends a key up.	keyCode **Number** Unicode representing the key the user released
sendCtrlAltDel()	Sends a CTRL+ALT+DEL sequence.	
sendShiftCtrlEsc()	Sends a CTRL+ALT+DEL sequence.	
sendShellExplorer()	Sends a CTRL+ALT+E (or WINDOWS+E) sequence.	
sendShellRun()	Sends a CTRL+ALT+R (or WINDOWS+R) sequence.	
sendCtrlEsc()	Sends a CTRL+ESC sequence.	
sendCut()	Sends a CTRL+X sequence.	
sendCopy()	Sends a CTRL+C sequence.	
sendPaste()	Sends a CTRL+V sequence.	

Usage Examples:

The next examples are JavaScript methods which are intended to show you a couple of usage cases for combining ThinRDP Library Keystroke methods.

Example 1 - Enter:

This first example shows you how to send a single keystroke, by sending its key code on the sendKeyStroke method argument.

```
function sendEnter() {
    if (mythinrdp) {
        mythinrdp.sendKeyStroke(13);
    }
}
```

Example 2 - Select next word / Select Line:

Observe on these next examples how to use the combination of "keydown" followed by "keyup" keys in order to select the next word inside of a text.
These next two examples simulate a combinations of keys pressed all together.
Remember that the sendKeyDown method has to be followed, at some point, by the sendKeyUp method, in order to release the key. If you only call the sendKeyDown method it is as if a key

was constantly pressed on the keyboard.

```
    function selectNextWord() {
        if (mythinrdp) {
            mythinrdp.sendKeyDown(0x11); //CTRL
            mythinrdp.sendKeyDown(0x10); //SHIFT
            mythinrdp.sendKeyStroke(39); // RIGHT ARROW
            mythinrdp.sendKeyUp(0x10); //SHIFT
            mythinrdp.sendKeyUp(0x11); //CTRL
        }
    }

    function selectLine() {
        if (mythinrdp) {
            mythinrdp.sendKeyDown(0x10); //SHIFT
            mythinrdp.sendKeyStroke(40); // DOWN ARROW
            mythinrdp.sendKeyUp(0x10); //SHIFT
        }
    }
```

Example 3 - Send a plain text:

This next example sends a plain text followed by an 'enter' to the remote environment.

```
    function sendText() {
        if (mythinrdp) {
            mythinrdp.sendText("This is a test...");
            sendEnter();
        }
    }
```

9.1.6 SSL Certificate

When you embed ThinRDP into a website you need an SSL certificate. Otherwise if the browser can not verify the configured certificate authenticity, your integration won't work.
There are two ways to set up the SSL certificate:

1. Using your own certificate

If you already have your own certificate or will get one from a Certificate Authority (CA), all you have to do is configure the certificate as described in the "A CA Certificate" section.

2. ThinRDP.net certificate

In case you don't have a certificate but want to use the https protocol, you can still use the certificate provided by ThinRDP.net .
Follow these simple steps to configure your application to use the ThinRDP certificate:

1. Configure the PIN resolution.

2. Set the 'server' property on the 'connect' method to your thinrdp.net public address. For more information on this address, read the Configure the PIN resolution section.
Also you can set the 'server' property to the ThinRDP server's IP separated by underlines instead of dots, following the example below:

Suppose your ThinRDP server IP is 192.168.0.10 and it's listening under port 8443.

The 'server' property should be:

```
server: "192_168_0_10.thinrdp.net:8443"
```

If none of these options work for you, disable the SSL certificate, setting the "protocol" property to "HTTP:". Find out how to do it on the connect method subsection.

9.1.7 Demos

Along with the ThinRDP installation we have shipped two SDK demos: an html demo and an asp.net demo.

HTML demo:

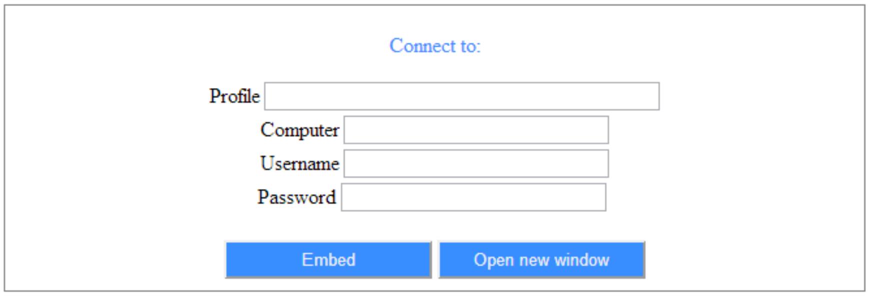
This demo is an HTML page that has an example of SDK usage in "Local mode". ThinRDP is embedded in a div placed inside the same web page.
This HTML example is located in the 'sdk.html' file inside the ThinRDP web directory under the ThinRDP installation directory (e.g.: C:/Program Files/ThinRDP Server/webrdp) .

You can try this demo directly from ThinRDP Server, by opening on your web browser the ThinRDP Server Address followed by /sdk.html (e.g.: http://127.0.0.1:8443/sdk.html).
To use this demo on your environment, follow the Quick Setup Guide instructions, on the Deployment page.

C# asp.net demo:

The asp.net demo is an example on how to use the SDK in a "Remote mode". This example allows you to open the remote screen on a "New window", or "Embed" it in a iFrame located on the same webpage. Besides the SDK integration, the application shows how to perform an External Authentication by dynamically negotiating a encryption key with ThinRDP Server.

ThinRDP SDK asp.net demo



The website demo is accessible from the Users documents folder, under the directory **\ThinRDP Demos\SDK.** Download it here.
In order to compile this application, you can use the Microsoft Visual C# Studio 2010 Express. Open the application from the menu *File-Open Web Site.*

The web.config parameters:

username/apikey:

The external authentication is set to use username/password as credentials by default, but you can also change the web.config file to start using the username/apikey pair of values as credentials.
Once you set the corresponding "`APIKEY`", the application will start performing the external

authentication using the username/apikey values.

```
<add key="APIKEY" value="3884F316-3429-49A0-9282-AF0C52B62107"/>
```

HTTP Protocol:

The example application is completely functional for environments where the ThinRDP Server is deployed on the same machine and running under the HTTP protocol.
If your environment does not attend these conditions you can also personalize those values on the web.config file:

```
<add key="PROTOCOL" value="http:"/>
<add key="SERVER" value="127.0.0.1:8443"/>
```

HTTPS Protocol:

A valid certificate will be required when using the HTTPS protocol.
You can use the Cybele Software embedded certificate, by setting the application to work with Dynamic DNS and Certificate Sharing and changing the "`SERVER`" key on the web.config file following the format below:

```
<add key="PROTOCOL" value="https:"/>
<add key="SERVER" value="127-0-0-1.thinrdp.net:8443"/>
```

If you want to use your personal Certificate, read the Managing the SSL Certificate section.

If you have problems regarding Google Chrome Frame installation on Interner Explorer 8 (and older versions) when using ThinRDP on iFrames, add these script tags on the page where the iFrame is located:

```
 <script type="text/javascript">
     var CFInstall;
     var CheckChromeFrame = false;
</script>

  <script src="jquery.min.js" type="text/javascript"></script>
  <script src="sdk.min.js" type="text/javascript"></script>
```

This will allow Google Chrome Frame to be installed properly.

9.2 External Authentication

ThinRDP Server incorporates a mechanism to validate users in a corporate environment so that the user will not need to authenticate every time they access ThinRDP.

How to authenticate against ThinRDP from external applications:

The authentication against ThinRDP Server can be done using:

- username and password or
- username and an ApiKey.

Every time you call ThinRDP Server, you can send within its URL the authentication information. The URL format to authenticate this way is presented below:

http[s]://[username]:[password or apikey]@127.0.0.1:8443

The External Authentication requires the option "Use Standard brow ser authentication dialog" to be set as true.

Encryption:

Whether the authentication is done using password or apikey, the secrecy of this data is indispensable. That is why ThinRDP enables external applications to dynamically negotiate a key to use the Diffie Hellman Key Exchange method for posterior encryption.

Demo:

The IIS asp.net demo application is an example on how to authenticate and encrypt the exchanged data.

Read the next topics to find out how to configure and use these ThinRDP mechanisms:

Apikey
Diffie Hellman Key Exchange
Demo

Learn also about these single-sign-on methods ThinRDP is compatible with:

OAuth/2
CAS

9.2.1 Apikey

The ApiKey is a secret value, known only by ThinRDP Server and a corporate application that connects to it.
By sending the ApiKey, the corporate application is identifying itself as trusted. In some cases, ThinRDP will recognize the user who is authenticating as logged on the corporate network, so that the password would not be required.
This method is useful for applications that do not keep the user's passwords and only authenticate their users against Windows or a network Active Directory Server.

The ApiKey is a configurable value. It is set in the ThinRDP ini configuration file. The location of this file depends on the Windows version ThinRDP is running at:

Windows 2003: C:\Documents and Settings\All Users\Application Data\Cybele Software\ThinRDP-TS\ThinRDPTS.ini
Windows 2008: C:\ProgramData\Cybele Software\ThinRDP-TS\ThinRDPTS.ini

Inside the ini file, the apikey information should be appended following the format below:

```
[API]
Key = 3884F316-3429-49A0-9282-AF0C52B62107
Ips = 192.168.0.22; ...
```

You should use a personal value for the ApiKey setting, as long as it follows the pattern shown above in the 'Key' parameter and matches the value sent by the external application.
Do not use the example value shown above, as this content is public on the internet.
Filter access. Grant access to a set of desired ips by adding them in the 'Ips' parameter. This will restrict the rest of ips from connecting.

If the ApiKey does not exist in the ini configuration file, the server won't be able to authenticate external applications or establish connections using the One-Time-URL .

9.2.2 Diffie Hellman Key Exchange

"Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher." [wikipedia]

Using Cybele's ThinAPI library to perform a Diffie Hellman key exchange:

1. Add the Cybele.ThinAPI.dll to your application. It is available on the Demo application under the 'bin' directory.
2. Create an object instance of the `DHCypher` class.
3. Call the 'Init' method, sending the ThinRDP Server address as argument. This method is responsible of negotiating the key with ThinRDP Server.
4. Call the `EncodeStr` method passing as an argument the data to be encrypted .

c# example:

```
 using Cybele.ThinAPI;

...

       DHCypher myDHCypher = new DHCypher();
       myDHCypher.Init("http://127.0.0.1:8443");
       authInfo = HttpUtility.UrlEncode(myDHCypher.EncodeStr(authInfo));

...
```

Sending encrypted data:

After performing the Diffie Hellman key exchange, the external application may send the encrypted data to ThinRDP Server preceded by an * symbol.

c# example:

```
           using Cybele.ThinAPI;

          ...
                 authInfo = "*" + authInfo;

          ...
```

The authentication information is then ready to be sent to ThinRDP Server within the URL, following one of the two formats below:

http:// + authInfo + @127.0.0.1:8443

The authInfo would be "username:password" encrypted with the Diffie Hellman method, preceded by an * symbol.

http://127.0.0.1:8443/asp/?authInfo

The authInfo should be "_userid=username&_apikey=apiKeyValue", also encrypted and preceded by an * symbol.

Both methods above are used on the Demo example. The first one works by default, and the second one works when there is an ApiKey set on the web.config file.

SDK and External Authentication:

If you want to use the External Authentication with the ThinRDP SDK (remote mode), the authInfo must not be included in the URL.
In that case, you should send the "credentials" on the post to ThinRDP Server.

Assign the credentials to ThinRDP form, before calling the connect method:

```
mythinrdp = GetThinRDP("127.0.0.1", true);
mythinrdp.getForm().elements["credentials"].value = "<%=authInfo%>";.
mythinrdp.connect({...});
```

The authInfo can consist of "username:password" or "username:apiKey", and should also be encrypted and preceeded by an * symbol.

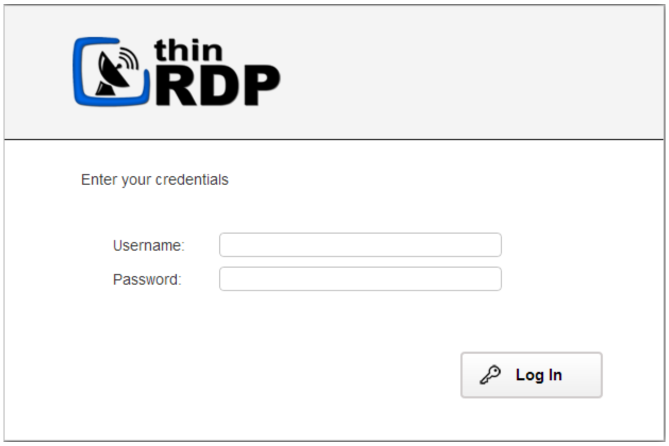
See also: the C# asp.net SDK demo, and have access to the complete example.

9.2.3 Demo

This C# asp.net demo is intended to help you learn how to securely authenticate against ThinRDP Server from an external application.

The demo Logon.aspx page is an authentication form that looks identical to the ThinRDP one. This page was designed to exemplify how to authenticate to ThinRDP externally using username/ password or apikey and having the authentication data encrypted through the Diffie Hellman Key Exchange method.

After authentication against ThinRDP, the application redirects to the Default.aspx page that has an IFrame pointing to ThinRDP index.html page.



Download this demo here.
The website demo is accessible from the Users documents folder, under the directory **\ThinRDP Demos\IISAuth**
In order to compile this application, you can use the Microsoft Visual C# Studio 2010 Express.
Open the application from the menu *File-Open Web Site.*

The web.config parameters:

username/apikey:

The external authentication is set to use username/password by default, but you can also change the web.config file to start using the username/apikey.
Once you set the corresponding "APIKEY", the application will start performing the external authentication using the username/apikey values.

```
<add key="APIKEY" value="3884F316-3429-49A0-9282-AF0C52B62107"/>
```

HTTP Protocol:

The example application is completely functional for environments where the ThinRDP Server is deployed on the same machine and running under the HTTP protocol.
If your environment does not attend these conditions you can also personalize those values on

the web.config file:

```
<add key="PROTOCOL" value="http:"/>
<add key="SERVER" value="127.0.0.1:8443"/>
```

HTTPS Protocol:

If you want to use the HTTPS protocol, then a valid certificate will be required.
You can use the Cybele Software embedded certificate, by setting the application to work with Dynamic DNS and Certificate Sharing and changing the "SERVER" key on the web.config file following the format below:

```
<add key="PROTOCOL" value="https:"/>
<add key="SERVER" value="127-0-0-1.thinrdp.net:8443"/>
```

If you want to use your personal Certificate, read the Managing the SSL Certificate section.

If you have problems regarding Google Chrome Frame installation on Interner Explorer 8 (and older versions) when using ThinRDP on iFrames, add these script tags on the page where the iFrame is located:

```
 <script type="text/javascript">
     var CFInstall;
     var CheckChromeFrame = false;
</script>

  <script src="jquery.min.js" type="text/javascript"></script>
  <script src="sdk.min.js" type="text/javascript"></script>
```

This will allow Google Chrome Frame to be installed properly.

9.3 Single Sign On

On a multi-application Single-Sign-On environment users log in once into one application and gain access to all the other applications without being prompted to log in again for each of them.
As different applications and resources support different authentication mechanisms,ThinRDP has to internally translate and store different credentials for the supported single-sing-on methods, in order to interpret them into the ThinRDP Local credentials

Google accounts integration:

ThinRDP authentication can be integrated to the Google accounts. On the links below you will find the information to set up ThinRDP to work with this method:

- Google OAuth/2
- Google ID for web applications
- Enabling Google OAuth/2 on ThinRDP

Other single-sign-on methods:

Any other method can also be supported by ThinRDP. To make any other methods work with ThinRDP you have to map external users to ThinRDP and substitute the password with the ThinRDP ApiKey mechanism.

The CAS demo shows you how to integrate an external application authentication with ThinRDP through the use of the CAS authentication and Apikey on the ThinRDP side.

9.3.1 Google OAuth/2

Users can be authenticated in ThinRDP Server by using their Google Accounts.
This kind of authentication requires the system administrator to configure a few settings on ThinRDP Manager and on Google Apps servers.
If you want to learn how to configure the Google Accounts Integration feature, follow the steps below:

Requirements

1. A Google account is needed in order to set up the integration in the Google Web Site. This Account is used as a security assurance for the other users who will share their personal account data.

2. The users who will authenticate using this method must also have a previous Google account.

3. The ThinRDP authentication level has to be set to Access Profiles.

Setting up the integration

1. Create a Client ID for web applications

2. Enable the Integration through the ThinRDP Manager SSO tab: OAuth/2 tab

3. Enter the e-mails that will be authenticated against ThinRDP Server. This set up will be available under the OAuth/2 tab Users in the ThinRDP Manager.

4. Associate the Active Directory Users/Groups with the authorized e-mails also on the ThinRDP Server Manager, under the Mapping tab in the ThinRDP Manager.

How to use it

1. Open a web browser and log into Google with one of the authorized accounts (step 4 above).

2. Open a new tab in the same browser instance and access ThinRDP application from this tab, using the configured URI (e.g.: https://ThinRDPServer/google) .

3. The application will automatically recognize you, but before connecting to ThinRDP Server, it will ask you for permission to access your account information.

4. Press the Allow Access button, and you will be automatically authenticated against ThinRDP and redirected to the Start Page.

9.3.1.1 Google Client ID for web applications

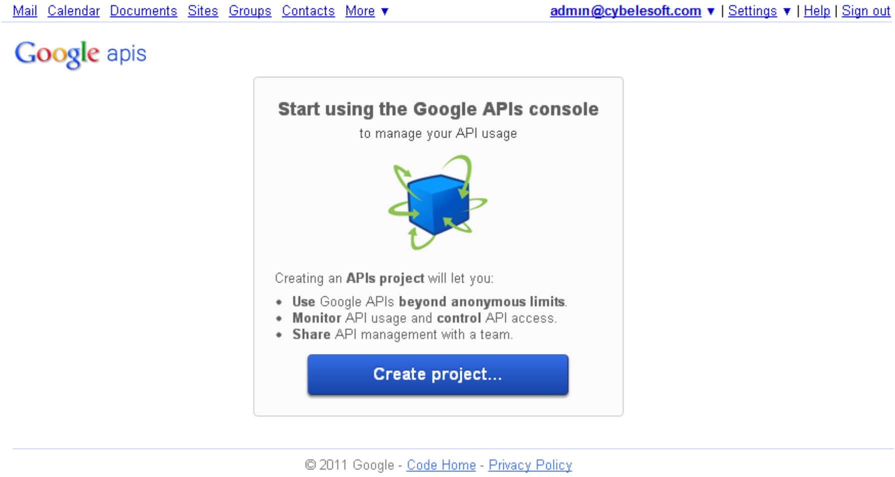
Before configuring the ThinRDP Server integration with Google accounts (single-sign-on), you have to create a Google Client ID for web applications.
Remember that a Google Client ID has to be created under an existing Google account. We recommend that you use a Google account that identifies the system administration, because this account will be shown to users as the responsible for their account personal data that will be accessed from Google.

Follow the next steps to create your own "Google Client ID for web applications".

1. Log into Google with the admin account you will use for the integration configuration.

2. Open this URL: code.google.com/apis/console on the same browser instance.

3. Click on the "Create Project button". This step will only be needed if your Google account has never configured a Google Client ID before. Otherwise it will jump into the next step.


Mail Calendar Documents Sites Groups Contacts More ▾
admin@cybelesoft.com ▾ | Settings ▾ | Help | Sign out
Google apis
Create project...
Code Home
Privacy Policy

Start using the Google APIs console
to manage your API usage

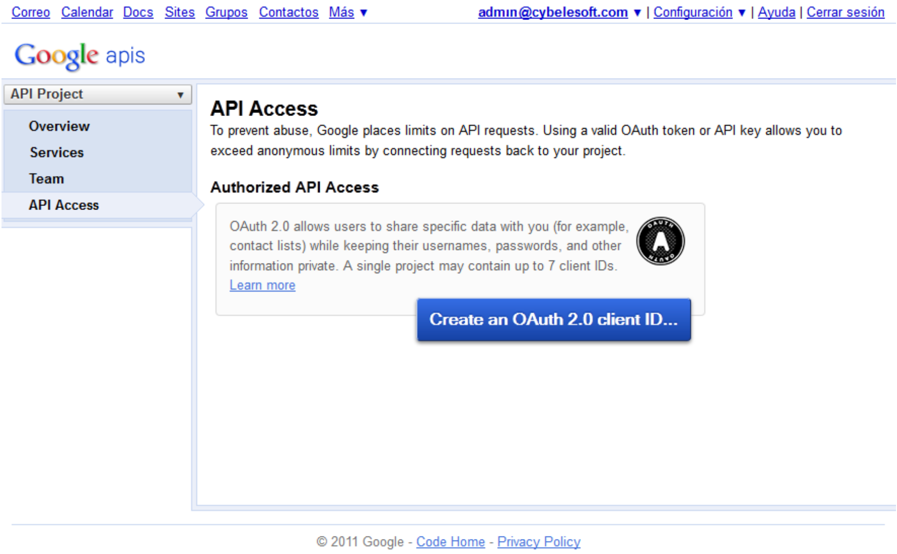
Creating an **APIs project** will let you:

- **Use** Google APIs **beyond anonymous limits**.
- **Monitor** API usage and **control** API access.
- **Share** API management with a team.

© 2011 Google - Code Home - Privacy Policy

4. Click on the left menu option: "API Access".

5. Click on the "Create an OAuth 2.0 client ID..." middle button.


Correo Calendar Docs Sites Grupos Contactos Más ▾
admin@cybelesoft.com ▾ | Configuración ▾ | Ayuda | Cerrar sesión
Google apis
API Project ▾
Overview
Services
Team
API Access
Create an OAuth 2.0 client ID...
© 2011 Google - Code Home - Privacy Policy

API Access

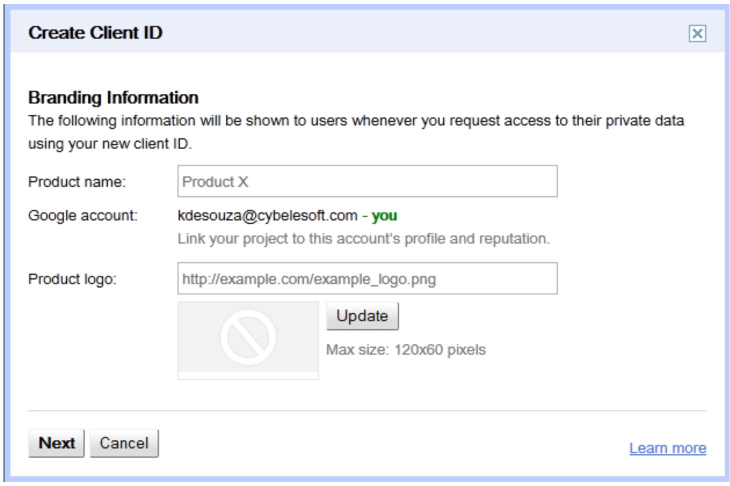
To prevent abuse, Google places limits on API requests. Using a valid OAuth token or API key allows you to exceed anonymous limits by connecting requests back to your project.

Authorized API Access

OAuth 2.0 allows users to share specific data with you (for example, contact lists) while keeping their usernames, passwords, and other information private. A single project may contain up to 7 client IDs. Learn more

6. Fill in the Branding Information on the "Create Client ID" screen:

a) On the "Product name" field enter a name that will identify the application and the company to the users. This information is shown when the users are asked to confirm their data sharing with this entity/product.
b) The Google account does not have to be changed.
c) You can also enter a logo image to be shown to the users on the registration moment (it will be shown in the same step as the product name).



Create Client ID

Branding Information

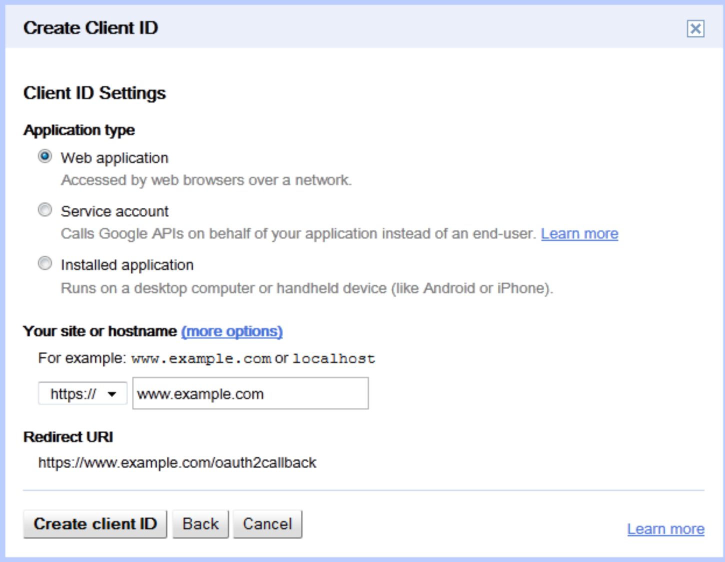
The following information will be shown to users whenever you request access to their private data using your new client ID.

Product name: Product X

Google account: kdesouza@cybelesoft.com - you
Link your project to this account's profile and reputation.

Product logo: http://example.com/example_logo.png
Max size: 120x60 pixels

7. Set the Application Type option to "Web application" and enter the external server URL. This URL should be accessible in the location that users will connecting to the application from.



Create Client ID

Client ID Settings

Application type

● Web application
Accessed by web browsers over a network.

○ Service account
Calls Google APIs on behalf of your application instead of an end-user. Learn more

○ Installed application
Runs on a desktop computer or handheld device (like Android or iPhone).

Your site or hostname (more options)

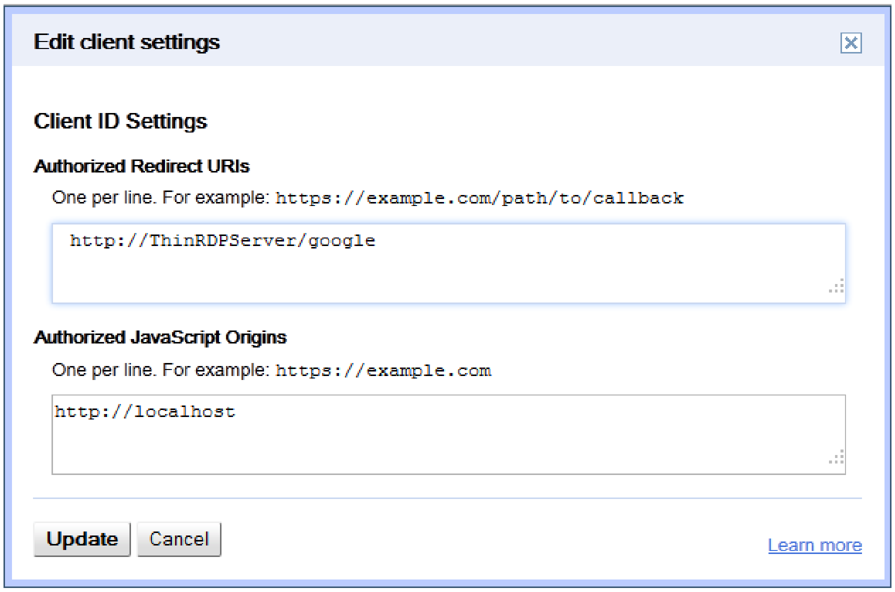
For example: `www.example.com` or `localhost`

https:// ▾ www.example.com

Redirect URI

https://www.example.com/oauth2callback

8. Once the account is created, click on the "Edit Settings" button and change the URI to http://ThinRDPServer:port/google, like the example below, and click on "Update".



Edit client settings

Client ID Settings

Authorized Redirect URIs

One per line. For example: `https://example.com/path/to/callback`

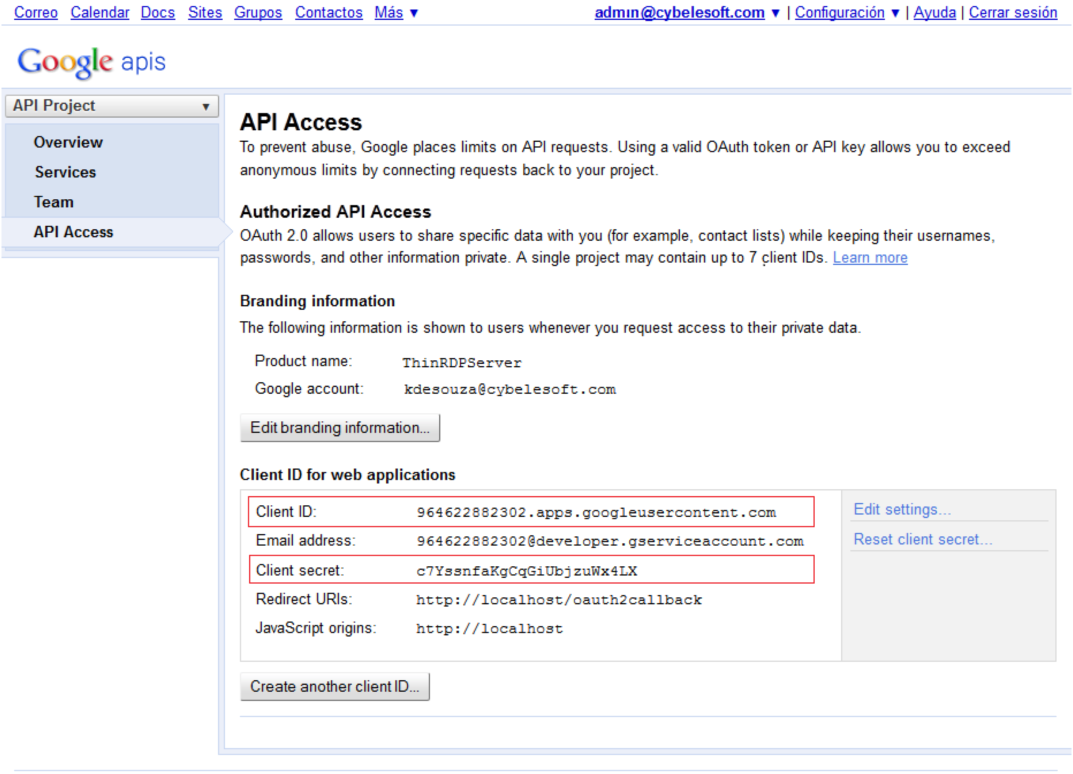
```
http://ThinRDPServer/google
```

Authorized JavaScript Origins

One per line. For example: `https://example.com`

```
http://localhost
```

9. Copy the "Client ID" and "Client Secret" values to posterior use on ThinRDP Server. Find these fields surrounded by a red square, on the image below:


Correo Calendar Docs Sites Grupos Contactos Más ▾
admin@cybelesoft.com ▾ | Configuración ▾ | Ayuda | Cerrar sesión
Google apis
API Project ▾
Overview
Services
Team
API Access

API Access

To prevent abuse, Google places limits on API requests. Using a valid OAuth token or API key allows you to exceed anonymous limits by connecting requests back to your project.

Authorized API Access

OAuth 2.0 allows users to share specific data with you (for example, contact lists) while keeping their usernames, passwords, and other information private. A single project may contain up to 7 client IDs. Learn more

Branding information

The following information is shown to users whenever you request access to their private data.

Product name:	ThinRDPServer
Google account:	kdesouza@cybelesoft.com

Client ID for web applications

Client ID:	964622882302.apps.googleusercontent.com
Email address:	964622882302@developer.gserviceaccount.com
Client secret:	c7YssnfaKgCqGiUbjzuWx4LX
Redirect URIs:	http://localhost/oauth2callback
JavaScript origins:	http://localhost

9.3.2 CAS demo

CAS is an authentication system created to provide a trusted way for an application to authenticate a user. You can find more information about it under the link: http://www.jasig.org/cas

C# asp.net demo:

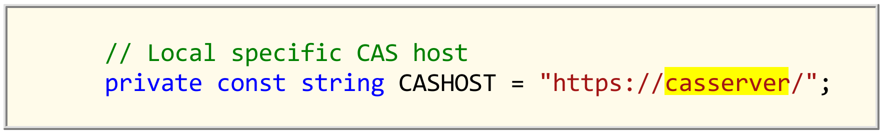
We have shipped an example demo along with ThinRDP, to show you how to integrate ThinRDP in a single-sign-on schema.

Download this demo here. The website demo is accessible from the Users documents folder, under the directory **\ThinRDP Demos\CASAuth**
In order to compile this application, you can use the Microsoft Visual C# Studio 2010 Express. Open the application from the menu *File-Open Web Site.*
You also need a CAS Server to make the integration with ThinRDP work.

The ASP.NET login page for CAS user validation uses the oficial dot-net CAS Client and the ThinRDP ApiKey logon feature. The first one takes care of the CAS login validation while the other one makes sure ThinRDP validates this user.

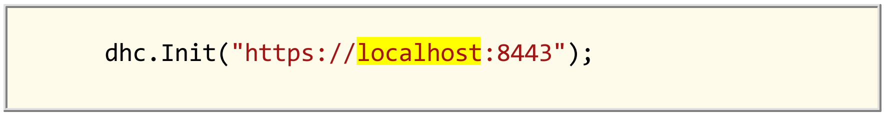
Before running the demo you need to modify three things:

1. In the login.aspx.cs, replace the CASHOST value with the URL of the CAS server.



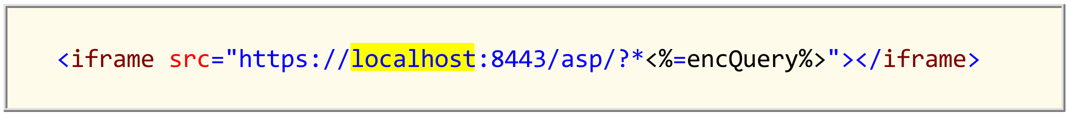
```
// Local specific CAS host
private const string CASHOST = "https://casserver/";
```

2. On the Default.aspx.cs replace the URL in dhc.Init(“...”) with the URL of the ThinRDP server.



```
dhc.Init("https://localhost:8443");
```

3. Finally, on the Default.aspx page, replace the first part of the URL specified as the iframe source (src) with the URL of the ThinRDP server without removing the “/asp/? *<%=encQuery%>”, which is needed for the ApiKey validation.



```
<iframe src="https://localhost:8443/asp/?*<%=encQuery%>"></iframe>
```

NOTE: In order to use CAS you have to configure ThinRDP to use SSL encryption (HTTPS connection) and use a valid certificate, trusted by the CAS server. The same is true for the CAS server which needs to be accessible via an HTTPS connection and present a valid or trusted certificate by the server where ThinRDP is running.

Remember also to map the CAS users to the ThinRDP users in order to make the integration work properly.

9.4 Customizing the Web Interface

ThinRDP Server allows you to modify the web interface and tailor it to your branding scheme.

Customizing the application logo and other image files can be very simple, once it only requires you to have the new image file and tell the application where it is located.

Customizing the structure and style of the application may be a little bit more complex. These kind of customizations have to be done at a programming level (HTML and CSS).

Read also how to protect the customized web files in the Files Location topic.

9.4.1 Changing the logo

Modifying the application logo can be as simple as copying the new logo image and telling ThinRDP Server application where it is located:

1. Create a folder called "BrandingFiles", if it doesn't exist yet, under the folder webrdp located inside the ThinRDP Server installation directory.
   (e.g.: C:/Program Files/ThinRDP Server/webrdp)

2. Copy your own logo image file to the "BrandingFiles" folder.

3. Create the WebAliases.ini file and configure it:

   a. Create a file called "WebAliases.ini" in the installation directory (e.g.: C:/Program Files/ThinRDP Server/WebAliases.ini). If the file already exists, only append the lines to it.

   b. Configure the redirection of the logo files you want to substitute, following the two examples below (ThinRDPSmall.png and favicon.ico):

```
[Alias]

;=================
;Main logo
;=================
/images/idx/ThinRDPSmall.png=BrandingFiles\MyLogo.png

;=================
;Favicon
;=================
/favicon.ico=BrandingFiles\MyFavicon.ico
```

   c. Save it.

4. Open the application to see the changes.

Take into account:

a. Any line in the "WebAliases.ini" file starting with a semicolon will not be considered by the application. It can be used to leave comments in the file.

b. You can substitute any interface image or file, by following the same steps described above.

c. Sometimes the favicon is not shown right the way, because the browser keeps history of the images. In that case, you should clean the browser cache before trying out the changes.

9.4.2 Customizing the web files

To customize the web files, you should:

1. Create a folder called "BrandingFiles", if it doesn't exist yet, under the folder webrdp located inside the ThinRDP Server installation directory. (e.g.: C:/Program Files/ThinRDP Server/webrdp)

2. Make copies of the original web files that you want to modify to the "BrandingFiles" folder. Copy only the files to be modified without their associated folder structure.

3. Customize the files (html, css, etc) as you prefer.

4. Create the WebAliases.ini file and configure it:

a. Create a file called "WebAliases.ini" in the installation directory (e.g.: C:/Program Files/ThinRDP Server/WebAliases.ini). If the file already exists, only append the lines to it.

b. Configure the redirection to the files you have modified, by adding a line similar to the examples below for each modified file:

```
[Alias]

/index.html=BrandingFiles\my_index.html
/css/index.css=BrandingFiles\my_index.css
```

c. Save it.

5. Open the application and check out the changes.

Take into account:

a. Any line in the "WebAliases.ini" file that starts with a semicolon will not be considered by the application. It can be used to leave comments.

b. The paths located in the HTML, CSS, and other contents will be kept relative to the original file location. This means that you won't have to change the content paths when customizing this files.

9.4.3 Files Location

We recommend that you to create a new folder in order to keep the customized files instead of leaving it all together with the original ones. On doing so, you will:

a) Have the possibility to get back to the original interface configuration, at anytime
b) Make sure that your files will be safe after a version upgrade.

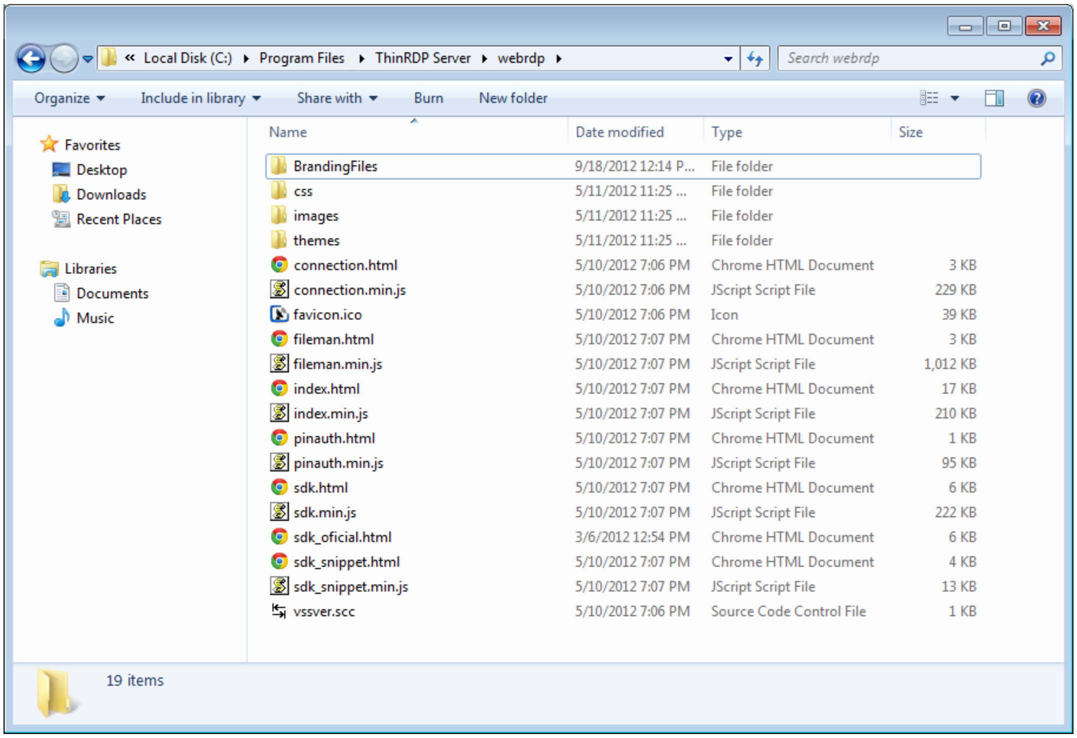
You can also choose whether to place the files inside or outside the webroot structure. Read next, how each option will behave differently.

Inside the webroot :

When the directory that will keep the customized files is created inside the webroot directory:

1) The files will be accessible externally from a URL similar to: https://127.0.0.1/BrandingFiles/customizedFile.html

2) The paths to the files, indicated in the "WebAliases.ini", can be relative to the webroot directory. (e.g. "/img/ThinRDPSmall.png=BrandingFiles\MyLogo.png"). You will find other relative path examples on the topics Changing the logo and Customizing the web files.



Name	Date modified	Type	Size
BrandingFiles	9/18/2012 12:14 P...	File folder	
css	5/11/2012 11:25 ...	File folder	
images	5/11/2012 11:25 ...	File folder	
themes	5/11/2012 11:25 ...	File folder	
connection.html	5/10/2012 7:06 PM	Chrome HTML Document	3 KB
connection.min.js	5/10/2012 7:06 PM	JScript Script File	229 KB
favicon.ico	5/10/2012 7:06 PM	Icon	39 KB
fileman.html	5/10/2012 7:07 PM	Chrome HTML Document	3 KB
fileman.min.js	5/10/2012 7:07 PM	JScript Script File	1,012 KB
index.html	5/10/2012 7:07 PM	Chrome HTML Document	17 KB
index.min.js	5/10/2012 7:07 PM	JScript Script File	210 KB
pinauth.html	5/10/2012 7:07 PM	Chrome HTML Document	1 KB
pinauth.min.js	5/10/2012 7:07 PM	JScript Script File	95 KB
sdk.html	5/10/2012 7:07 PM	Chrome HTML Document	6 KB
sdk.min.js	5/10/2012 7:07 PM	JScript Script File	222 KB
sdk_oficial.html	3/6/2012 12:54 PM	Chrome HTML Document	6 KB
sdk_snippet.html	5/10/2012 7:07 PM	Chrome HTML Document	4 KB
sdk_snippet.min.js	5/10/2012 7:07 PM	JScript Script File	13 KB
vssver.scc	5/10/2012 7:06 PM	Source Code Control File	1 KB

Outside the webroot :

The customized files, can also be placed in any other disk location. In that case:

1) The files will be protected, because it won't be possible to access the customized files from an URL.
2) The paths to the files, indicated in the "WebAliases.ini", have to be absolute, as the example

below:

```
[Alias]

/index.html=c:/BrandingFiles/my_index.html
/images/ThinRDPSmall.png=c:/BrandingFiles/MyLogo.png
```

9.5 Web Services API

The Web Services API is intended to allow external applications to access and manipulate some of ThinRDP data and settings.
ThinRDP has two different Web Services available:

a. Profiles Web Service:

If you need to manipulate ThinRDP users and their permissions from an external software application, you can use the Profiles Web Services to perform this task. If you don't know how to use the Access Profiles feature, take a look on the section that explains it's use and behaviour.

b. Analytics Web Service:

The ThinRDP Analytics feature is included since version 2.0.0.16. This feature keeps statistic data of ThinRDP logins, sessions, connections and used browsers. The Analytics Web Service allows external applications to access these information.

Requirements for the Web Service API:

1. The Profiles Web Service is valid for environments using Access Profiles as the ThinRDP authentication mode.

2. The integration has to be done at a programming level. You will need to develop or modify an application which will act as the Web Service requester and this application will have to implement the ThinRDP Web Service interface.

You may want to keep on reading about the Web Service API Integration:

Architecture

Installing the Web Service

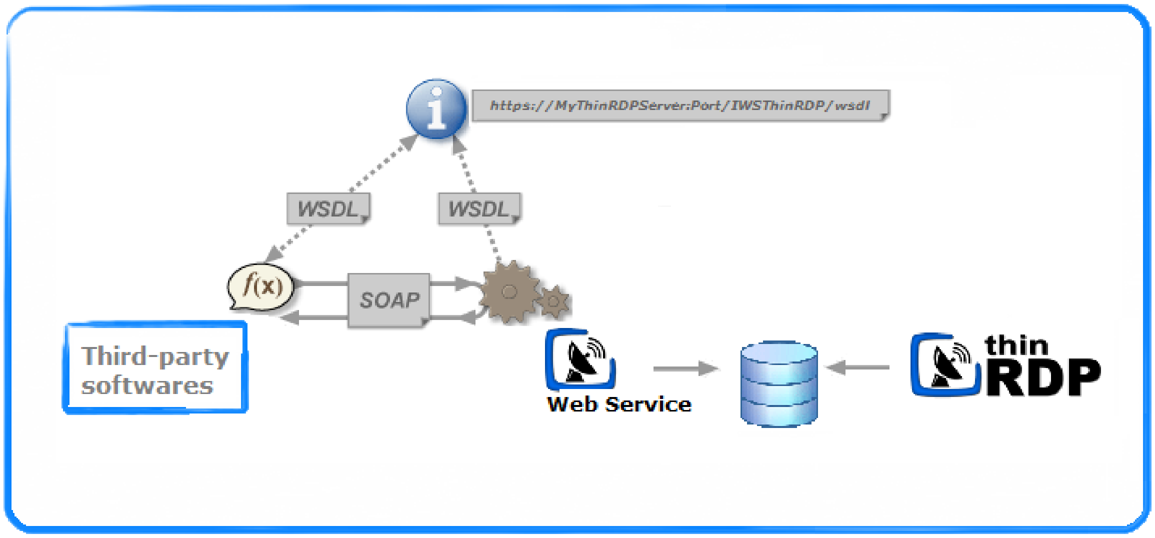
Setting up the communication settings

Profiles Web Service

Analytics Web Service

9.5.1 Architecture

The ThinRDP Web Service architecture is illustrated in the image below:



The "i" symbol represents the interface that should be used by the third-party application in order to make use of the Web Service. The interface is provided by ThinRDP on the following address, once the Web Service is installed:

https://ThinRDPWebServiceIP:port/IWSThinRDP/wsd

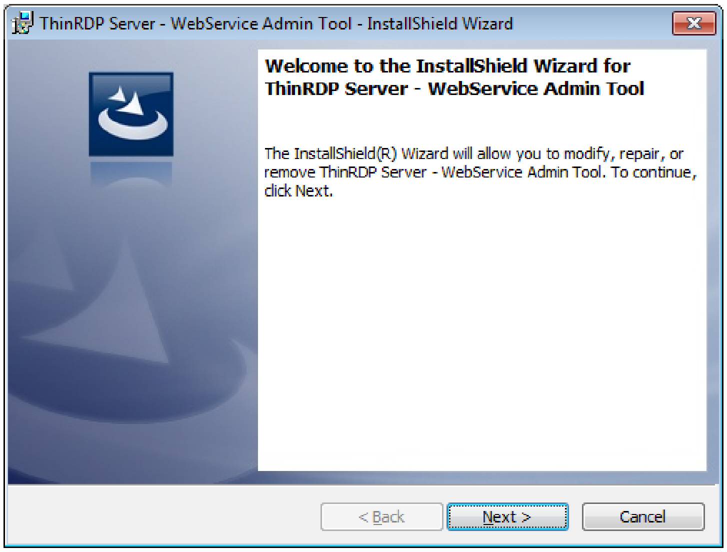
9.5.2 Installing the Web Service

The first step to start developing the integration with ThinRDP Web Service API is to install it:

1. Download the installer from the link below:

   http://www.cybelesoft.com/downloads/ThinRDPWSSetup.exe

2. Execute the installer on the same machine where the ThinRDP server is installed.



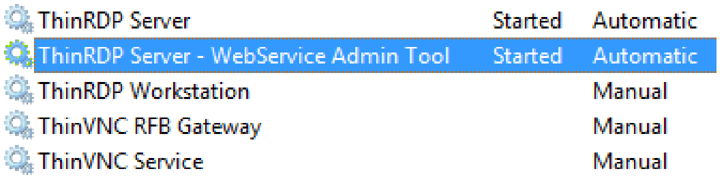
ThinRDP Server - WebService Admin Tool - InstallShield Wizard

Welcome to the InstallShield Wizard for ThinRDP Server - WebService Admin Tool

The InstallShield(R) Wizard will allow you to modify, repair, or remove ThinRDP Server - WebService Admin Tool. To continue, click Next.

3. Besides installing the Web Service, the installer will also:

   I. Set up a service on Windows, so the Web Service will be started every time Windows is turned on.

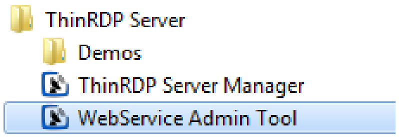


ThinRDP Server	Started	Automatic
ThinRDP Server - WebService Admin Tool	Started	Automatic
ThinRDP Workstation		Manual
ThinVNC RFB Gateway		Manual
ThinVNC Service		Manual

* If you do not want the Web Service to start automatically with Windows, change the "Startup type" to "Manual".

   II. Create a shortcut for the "*Web Service Admin tool"*

   III. Create a shortcut for the "*Demos"* applications directory. These are the three example applications that should illustrate the Web Service use.



ThinRDP Server
Demos
ThinRDP Server Manager
WebService Admin Tool

9.5.3 Setting up the communication settings

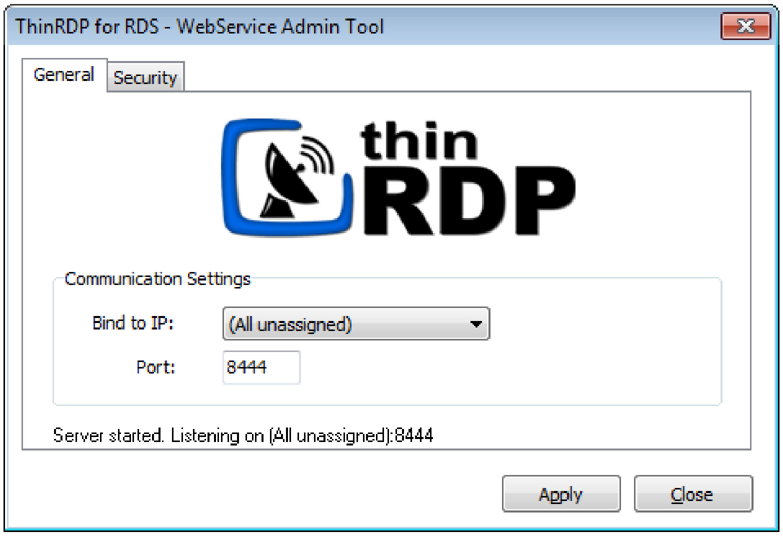
Open the "Web Service Admin Tool" from the Windows start menu.

General tab:

1. Go to the "General" tab.

2. On the "Bind to IP" field inform the IP address you want the Web Service to be listening on. If you need all the server IP's to listen to the service, select the "All unassigned" option.

3. Inform also what "Port" you want the service to be listening on in the "Port" field.



Bind to IP: (All unassigned)

Port: 8444

Server started. Listening on (All unassigned):8444

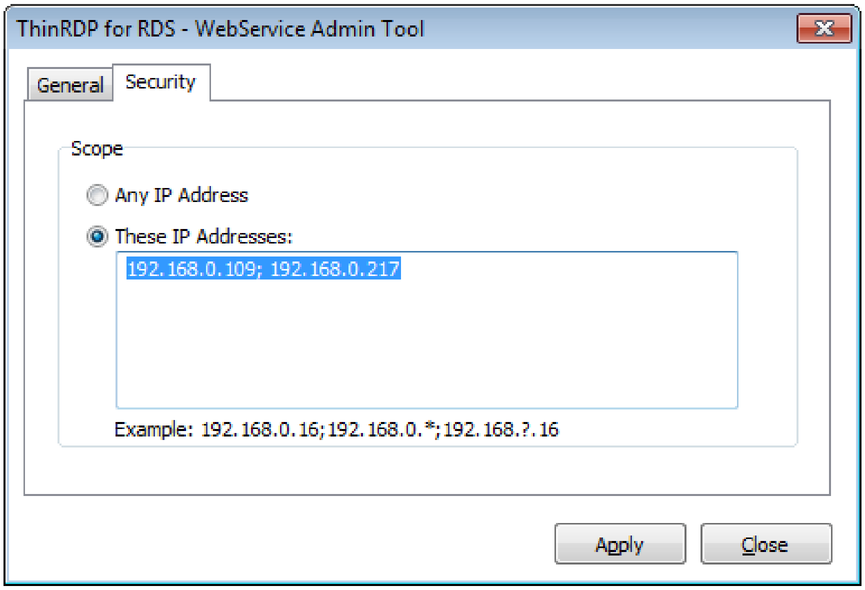
4. If the bottom message says "Server started. Listening on ..." it means the service is on and the communication setup was successful.
Otherwise, if the message says "Could not bind socket. Address and Port are already in use", you should look for conflicts with other services configured on this machine. You can also try changing the 'Port' number value.

Security tab:

1. Go to the "Security" tab.

2. If you don't want to restrict the IP addresses that will access the Web Service, mark the "Any IP Address".

3. If you want only determined IPs to access the Web Service, mark the option "These IP Addresses" and inform the IPs separated by semicolons.



Scope

○ Any IP Address

● These IP Addresses:

192.168.0.109; 192.168.0.217

Example: 192.168.0.16;192.168.0.*;192.168.?.16

1. Substiture a byte by the "*" symbol to select all existing IP addresses from that byte on.
2. Substitute a byte by the "?" symbol, to select all combinations inside this octet.

9.5.4 Profiles Web Service

The Access Profiles Web Service integration allows external applications to:

1. Retrieve any information from the configured profiles at ThinRDP server
2. Create new profiles
3. Delete existing profiles
4. Modify any information on an existing profile

The Web Service Transaction Manager, also available, enables you to execute a series of operations as a single unit of work. The Transaction Manager will guarantee that the series of operations will either be executed all together, or not executed at all.

Learn more about the Access Profiles Integration in the following topics:

Methods

Types

The demo applications

9.5.4.1 Methods

The main goal of this Web Service is to manipulate the Access Profiles set up. The following methods are available for that purpose. By combining these methods, you will be able to perform pretty much any task regarding the profiles set up.

Method name	Method description	Input params	Output params	Exceptions
GetAllProfiles	Retrieves all the existing profiles.		**WSProfileArray**: all existing profiles from ThinRDP server	If there are no profiles yet, returns a WSProfileArray w ith length = 0.
GetProfileCount	Counts how many profiles exist.		**integer**: profiles count	
GetProfile	Returns a profile located on a determined index.	**integer**: profile index	**WSProfile**: profile located on the informed index.	If there is no profile on the indicated index, returns null.
FindByID	Returns the profile that has the indicated ID.	**string**: profile ID	**WSProfile**: profile that has the informed ID.	If there is no profile that has the indicated ID, returns null.
FindByComputer	Returns all profiles associated w ith a computer.	**string**: computer IP	**WSProfileArray**: profiles associated w ith the informed computer.	If there are no profiles associated w ith the computer, returns a WSProfileArray w ith length = 0.
FindByUserName	Returns all profiles assigned to the user.	**string**: username	**WSProfileArray**: user granted profiles.	If there is are no profiles associated w ith the user, returns a WSProfileArray w ith length = 0.
CreateProfile	Creates a new profile.	**WSProfile**: profile to be created	**WSProfile**: created profile carrying the new generated ID and public Key.	If the profile could not be created, returns null.

`DeleteProfile`	Deletes an existing profile.	**string**: profile ID	**boolean**: returns true if the deletion was successful and false if the application could not delete the profile.	If there is no profile with the indicated ID, returns false.
`UpdateProfile`	Updates an existing profile.	**WSProfile**: profile to be updated with the new data already loaded in its structure.	**int:** returns 0 if the profile was updated successfully. Any value different from 0 means the update could not be performed.	If there is no profile matching the WSProfile ID, returns a value <> 0.
`NewPublicKey`	Generates a new public key for an existing profile.	**string**: profile ID	**WSProfile**: profile carrying the new Public Key.	If there is no profile matching the WSProfile ID, returns null.
`Commit`	Commits all the performed methods since the last commit or rollback.			
`Rollback`	Rollbacks all the performed methods since the last commit or rollback.			

9.5.4.2 Types

As you have already probably seen on the Methods sections, the WSProfile and the WSProfileArray type are sent and received as parameters of many methods. Here, you can learn what are these types and how to manage them.

Type name	Kind	Description	Values range
WSProfile	Complex	The WSProfile type represents one profile. It has all the attributes that describe a profile.	
WSProfileArray	Complex	The WSProfileArray is an array of WSProfile. It is used mostly as a parameter for methods that retrieve more than one profile from the server.	
TRdpCredentials	Simple	This type is used to describe the kind of authentication the WSProfile will perform. "crAuthenticated" means no username and password will be required. "crAsk" will use the username and password configured inside the profile. When "crSaved" is set up, the profile will authenticate automatically using the same application credentials.	"crAuthenticated" "crAsk" "crSaved"
TRdpScreenBPP	Simple	Color Depth: sets the WSProfile remote desktop screen number of bits per pixel . Set "bpp8" for 256 colors; "bpp15" for True Color (15 bit); "bpp16" for True Color (16 bit) ; "bpp24" for True Color (24 bit) ; "bpp32" for True Color (32 bit)	"bpp8", "bpp15", "bpp16", "bpp24", "bpp32"
TRdpScreenResolution	Simple	WSProfile remote desktop screen resolution.	"srCustom", "srFitToBrowser", "srFitToScreen", "sr640x480", "sr800x600", "sr1024x768", "sr1280x720", "sr1280x768", "sr1280x1024", "sr1440x900", "sr1440x1050", "sr1600x1200", "sr1680x1050", "sr1920x1080", "sr1920x1200"
TRdpImageQuality	Simple	WSProfile remote desktop image quality.	"iqHighest", "iqOptimal", "iqGood", "iqFaster"
TRdpAppMode	Simple	The application mode is used to determine if ThinRDP will open a specific application and the mode it will use to do it. The "amNone" value will show the whole desktop mode. The "StartApp" and "RemoteApp" are the two possible modes of connecting to a remote application.	"amNone", "amStartApp", "amRemoteApp"

TRdpSoundQuality	Simple	This type is used to describe the different sound qualities that ThinRDP works with.	"sqPoor" "sqGood" "sqOptimal" "sqExcellent"

9.5.4.2.1 The WSProfile type

The complex WSProfile type represents a profile and carries all its information. In order to retrieve, create, delete and update the ThinRDP profiles, you will have to manipulate this WSProfile data structure.

Attribute name	Type	Description	Modifiable
`ID`	`string`	Profile ID	no
`Name`	`string`	Profile name	yes
`Enabled`	`boolean`	Set false if you want the profile to be disabled	yes
`Unrestricted`	`boolean`	Only the [any computer] profile has this property set to true. It means that the profile will enable the users to choose the computer they will access entering the IP, port and credentials on the connection moment.	no
`GuestAllowed`	`boolean`	Set true to make the profile public	yes
`IsBuiltIn`	`boolean`	This attribute identifies the [any computer] profile. Only this profile has this attribute set to true.	no
`PublicKey`	`string`	Key that identifies a profile .	no
`Computer`	`string`	The remote desktop IP and port to connect to	yes
`Credentials`	`TRdpCredentials`	Configures the credential mode ThinRDP will operate on.	yes
`LogonUserName`	`string`	If the credential mode is set to "crAsk", will use this Username to log in into the computer.	yes
`LogonPassword`	`string`	If the credential mode is set to "crAsk", will use this Password to log in into the computer.	yes
`ScreenResolution`	`TRdpScreenResolution`	Sets the remote desktop resolution**.**	yes
`ScreenWidth`	`int`	Remote desktop screen width.	yes
`ScreenHeight`	`int`	Remote desktop screen height.	yes
`BPP`	`TRdpScreenBPP`	Color Depth: sets the number of bits per pixel	yes
`ImageQuality`	`TRdpImageQuality`	Remote desktop image quality.	
`UnicodeKbd`	`boolean`	Allows for full unicode keyboard charsets. Set to false to connect to xRDP servers.	yes
`ConsoleSession`	`boolean`	Set to true to connect to the console session. This requires confirmation from the logged on user and will log out the current session.	yes
`WebsocketCompression`	`boolean`	Set to true to enable the compression for the exchanged Websocket data and have the application performance improved.	yes
`RelativeMouseTouch`	`boolean`	For mobile devices. Uncheck this option to have a mouse behaviour similar to a desktop mouse in which the cursor will always be positioned under the touch. Leave as true to use relative mouse like a trackpad.	yes
`AppMode`	`TRdpAppMode`	Application Mode: sets whether the profile should connect to a specific application	yes
`AppCmdLine`	`string`	Specify the complete path to give access the application you want to start upon connection.	yes
`AppCmdArgs`	`string`	Arguments to start the application informed on the AppCmdLine field.	yes
`AppWorkDir`	`string`	Mark this option if you need to specify a context directory for the program set on the field "Program path and file name"	yes
`DesktopBackground`	`boolean`	Set to true to show the original remote desktop background.	yes
`VisualStyles`	`boolean`	Set to true to change the Start menu and other Windows features styles.	yes
`MenuAnimation`	`boolean`	Set to true to show an animation on the Start menu.	yes
`FontSmoothing`	`boolean`	Set to true to make text easier to read, especially the magnified text.	yes
`ShowWindowOnDrag`	`boolean`	Set to true to show windows content while dragging them.	yes
`DesktopComposition`	`boolean`	Set true to configure the DWM to redirected the desktop drawing to	yes

		off-screen surfaces in video memory. Also, the desktop will present many visual effects.	
PrinterEnabled	boolean	Uncheck this option to disable ThinRDP PDF printer.	yes
PrinterSetAsDefault	boolean	Mark this option to make ThinRDP printer the remote machine default printer.	yes
PrinterName	string	Specify the printer name that you want to be shown on the remote machine's printer list.	yes
PrinterDriver	string	This is the driver to be used by ThinRDP in order to print the remote documents. The "*HP Color LaserJet 2800 Series PS*" driver is compatible with 2008 Windows versions. The "*HP Color LaserJet 8500 PS*" driver is compatible with 2003 Windows versions. If you are not using 2003 or 2008 Windows versions, look for a driver that is already installed on the OS and inform this driver name in this attribute.	yes
Clipboard	boolean	Enables and disables the remote desktop clipboard.	yes
DiskEnabled	boolean	Check this option to have an intermediate disk available on the connections created through this profile.	yes
DiskName	string	This is the name to identify the intermediate disk among the other remote desktop disks.	yes
DiskAutoDownload	boolean	If set to true, ThinRDP will download automatically any file saved/ copied on the Intermediate disk direction.	yes
SoundEnabled	boolean	Check this option to enable the remote sound to be reproduced within the browser. The remote sound works only with Firefox and Chrome web browsers.	yes
SoundQuality	TRdpSoundQuality	Determines what quality ThinRDP will use to reproduce the remote sound. The highest the quality, the more resources it will require.	yes
Users	string	Windows Authentication Users or Groups that will be granted access to this profile. Separate each user or group by semicolons.	yes

9.5.4.3 The demo applications

We have packed, with the ThinRDP installation, two example applications that use ThinRDP Web Service to manipulate Access Profiles.
If you have already installed ThinRDP Web Service, you can access the demos from the Windows Start menu: All Programs/ThinRDP Server/Demos.
Both application were developed in C# and were designed to present you the many integration possibilities the Web Service provides you.
In order to compile this application, you can use the Microsoft Visual C# Studio 2010 Express. Download it here.

ThinRDPWS application example:

This application teaches you how to integrate each Web Service method available.
Observe that the Filter part uses the methods `GetAllProfiles` (none), `FindByComputer` and `FindByUserName`. The `FindByID` method is used every time a profile is selected and loaded on the screen visual components.
The `CreateProfile` method is also always available. After selecting one listed profile the `DeleteProfile`, `UpdateProfile` and `NewPublicKey` will also became available.
The whole data you have modified will only be confirmed through the `Commit` method. If you want to cancel and not confirm the modifications, use the `rollback` method.

ThinRDPWS-CRUD application example:

This example shows how to create profiles simply associating Users and Computers, without any other setup. Be aware that this example is not committing the changes, so the created profiles won't be available on your ThinRDP application, until you call the `Commit` method on the Web Service.

9.5.5 Analytics Web Service

The Analytics Web Service integration allows external applications to retrieve information regarding the system use: logins, sessions, connections and used browsers.

Learn more about the Analytics Integration on the following topics:

- Methods
- Types
- The demo application

9.5.5.1 Methods

The main goal of this Web Service is to access the Statistics information related to the system usage. The following methods are available for this purpose.

Method name	Method description	Input params	Output params	Exceptions
`Count`	Returns an integer value with the count of the records that satisfy the search criteria sent on the QueryType parameter.	**QueryType: WSQueryType**	**Integer**	
`List`	The list method returns an array containing all the records that satisfy the search criteria sent on the QueryType parameter.	**QueryType: WSQueryType**	**WSDBRecordArray**	If the search does not match any record, the result will be a WSDBRecordArray with length = 0.
`RangeList`	The RangeList method returns an array containing all the records that satisfy the search criteria sent on the QueryInfo parameter. The QueryInfo is composed by the QueryType and also a date range to filter the records (QueryRange).	**QueryInfo: WSQueryInfo**	**WSDBRecordArray**	If the search does not match any record, the result will be a WSDBRecordArray with length = 0.
`LoginList`	The LoginList method returns an array containing all the records that satisfy the search criteria which is composed by a QueryRange and the login type (successful logins and failed logins).	**Range: WSQueryRange**; **Successful: Boolean** **Failed: Boolean**	**WSDBRecordArray**	If the search does not match any record, the result will be a WSDBRecordArray with length = 0.

9.5.5.2 Types

As you have probably seen on the Methods sections, the Web Service uses specific types as input and output parameters. Here, you can learn what are these types and how to manage them.

Type name	Kind	Description	Values range
WSQueryType	Simple	The WSQueryType represents the available query types to be performed on the Web Service. The possible options are "qtSessions", "qtConnections" and "qtBrow sers".	"qtSessions" "qtConnections" "qtBrowsers"
WSQueryInfo	Complex	This type is used to send a filter criteria to the server w hen running a search method. It is composed by the queryTypeField (WSQueryType) and the queryRangeField (WSQueryRange).	
WSQueryRange	Complex	This type is used to send a date filter criteria to the server w hen running a search method. It is composed by the dateFromField and the dateToField.	
WSDBRecord	Simple	This type is a generalization interface of all analytics record types (WSLoginRecord, WSDBSessionRecord, WSDBConnectionRecord and WSDBBrow serRecord).	
WSDBRecordArray	Simple	An Array of WSDBRecord. It is used mostly as an output parameter for methods that retrieve more than one WSDBRecord from the server.	
WSDBLoginRecord	Complex	The WSDBLoginRecord describes how a Login record is structured.	
WSDBSessionRecord	Complex	The WSDBSessionRecord type describes how a Session record is structured.	
WSDBConnectionRecord	Complex	The WSDBConnectionRecord type describes how a Connection record is structured.	
WSDBBrowserRecord	Complex	The WSDBBrow serRecord type describes how a Brow ser record is structured.	

9.5.5.2.1 WSQueryInfo

The WSQueryInfo complex type is the query information sent within the RangeList method.

Attribute name	Type	Description	Modifiable
queryTypeField	WSQueryType	Query type (qtSessions,qtConnections,qtBrowsers)	yes
queryRangeField	WSQueryRange	Structure composed by the dateFromField and the dateToField.	yes

9.5.5.2.2 WSQueryRange

The WSQueryRange complex type is date range information to be send to a Analytics query.

Attribute name	Type	Description	Modifiable
dateFromField	dateTime	Low er dateTime limit from w here the records should be searched.	yes
dateToField	dateTime	Upper dateTime limit until w here the records should be searched.	yes

9.5.5.2.3 WSDBLoginRecord

The WSProfile complex type represents a profile and carries all its information. In order to retrieve, create, delete and update the ThinRDP profiles, you will have to manipulate this WSProfile data structure.

Attribute name	Type	Description
`accessTimeField`	`string`	The date and time in which the login was performed.
`userField`	`string`	The username that did the login.
`sourceIPField`	`string`	IP Address from which the login was initiated.
`successfulField`	`Boolean`	Boolean value that informs whether the login was successful or not.

9.5.5.2.4 WSDBSessionRecord

The WSDBSessionRecord type describes how a Session record is structured.

Attribute name	Type	Description
`sessionIDField`	`integer`	The Session ID.
`userField`	`string`	User that started the new session.
`sourceIPField`	`string`	IP Address from which the session was started.
`connectedOnField`	`string`	Date and time when the Session was Started
`disconnectedOnField`	`string`	Date and time when the Session was Ended
`connectionsField`	`integer`	Counter of Connections established within the Session.

9.5.5.2.5 WSDBConnectionRecord

The WSDBSessionConnection type describes how a Connection record is structured.

Attribute name	Type	Description
`userField`	`string`	User that established the connection.
`sourceIPField`	`string`	IP Address from w hich the connection w as established.
`hostField`	`string`	Host Name to w hich the connection w as established.
`connStartField`	`string`	Date and time w hen the Connection w as Started.
`connEndField`	`string`	Date and time w hen the Connection w as Ended.

9.5.5.2.6 WSDBBrowserRecord

The WSDBSessionBrowser type describes how a Browser record is structured.

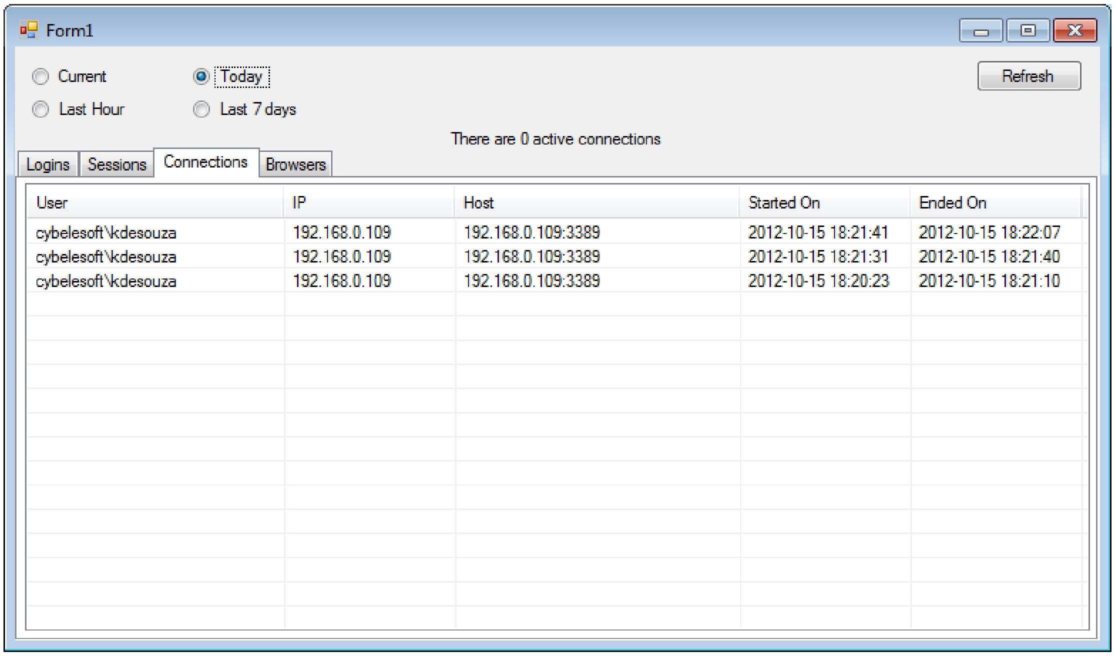
Attribute name	Type	Description
userAgentField	string	Browser User Agent.
sessionsField	integer	Counter of Sessions established within the Same Browser userAgent.

9.5.5.3 The demo application

We have packed along with the ThinRDP installation one example that uses Analytics ThinRDP Web Service to show the application usage data.
If you have already installed ThinRDP Web Service, you can access the demos from the Windows Start menu All Programs/ThinRDP Server/Demos.
The application was developed in C# and was designed to present you an integration possibility the Web Service provides you.
In order to compile this application, you can use the Microsoft Visual C# Studio 2010 Express.
Download it here.

ThinRDPWS-Query application example:

This application is an example of an external application integrating each available Web Service method.
Observe that the upper radio buttons are different date ranges used to filter the statistic records.
Select one of the date options, go to a specific tab (Logins, Sessions, Connections or Browsers) and click on the Refresh button.
The analytics data will be displayed on the tab grid.



○ Current ● Today
○ Last Hour ○ Last 7 days

There are 0 active connections

User	IP	Host	Started On	Ended On
cybelesoft\kdesouza	192.168.0.109	192.168.0.109:3389	2012-10-15 18:21:41	2012-10-15 18:22:07
cybelesoft\kdesouza	192.168.0.109	192.168.0.109:3389	2012-10-15 18:21:31	2012-10-15 18:21:40
cybelesoft\kdesouza	192.168.0.109	192.168.0.109:3389	2012-10-15 18:20:23	2012-10-15 18:21:10

9.6 One-time-URL

ThinRDP Server offers a mechanism to generate One-Time-URL connections that expire after a given period of time.

The One-Time-URL feature is designed to work with the Access Profiles and User/ Password Security Levels.

You have to configure an ApiKey on ThinRDP Server in order to use this method.

These are some situations in which the One-Time-URL might be useful:

a. Giving access to a desktop to external users without having to weaken the Security level to None.
b. Generating a temporary access to a desktop.
c. Integrating ThinRDP on a Single-Sign-On Scheme along with external applications.

How it works:

1. First you need to ask ThinRDP to generate the URL for you. Call ThinRDP Server following this URL format:

```
http(s)://ThinRDPServer:Port/ws/oturl/get?<queryString>
```

2. The queryString should be built with all parameters listed below:

```
apikey= <apikey> &apiuser= <apiuser> &model= <model> &plen= <passlen>
&expires= <expires>
```

Find on the table below a description for each required parameter.

Parameter	Description
apiKey	The ApiKey is a secret value, known only by ThinRDP Server and the corporate application. Find out more about it on the ApiKey topic.
apiuser	Use this parameter to identify the user within ThinRDP. The value should be the user or email registered in your website. The users are seen in the Analytics Web Service.
model	Send a profile key in order make this profile a template for the One-Time-URL connection that will be established.
plen	The plen parameter carries the password length.

expires	Through this parameter you can set an expiration (in minutes) for the URL. Expires = 30 means that the URL won't work anymore after 30 minutes from the URL generation.

On the next topics you can find out other parameters you can use to Configure the connection and Enable features.

3. If ThinRDP gets to authenticate with the parameters sent on the queryString, it will return a One-Time-URL that will allow you to establish an RDP connection with the remote desktop.

```
 /oturl.html?
key=w7NJNschBdJD9e6G6luWhOCalM$oFW7guqC6jE1IQah3AJm3&pass=BOWZB8FG
```

Concatenate the ThinRDP Server address to the generated URL, following this format below:

```
 http(s)://ThinRDPServer:Port/oturl.html?
key=w7NJNschBdJD9e6G6luWhOCalM$oFW7guqC6jE1IQah3AJm3&pass=BOWZB8FG
```

This way, the URL will be ready to be used. You can redirect your application to the desktop connection through it, or even send it to an external user by e-mail.

Find an HTML/ajax example inside the application installation directory, under the 'webrdp' folder. The file is named oturltest.html and implements the features covered on this topic.

9.6.1 Configuring the connection

Besides the basic parameters required to establish a connection, you can send additional settings parameters to customize the connection the way you want.
There are three ways to customize the one-time-url connection:

1. Using an Access Profile that will act as a template to the connection.
2. Using an Access Profile and overriding some parameters by sending them on the queryString.
3. Configuring each setting parameter on the queryString manually.

Find below what parameters you should send in order to configure the connection with each one of these modes:

Mode 1. Using Access Profiles as template for the Connection:

Parameter	What it means	Type/format	Default
`model`	On this parameter you should send the Profile Key, to have this profile taken as the Connection template.	**string** Profile Key	

Mode 2. Overriding the profile settings:

Parameter	What it means	Type/format	Default
`overrideDefaults`	Set this property to true, to have the Profile settings overridden by the parameters sent on the queryString. Then configure the individual settings you want to add to the Profile connection template If you send this parameter as false, only the profile configuration will be taken.	**boolean** true,false	false

Mode 3. Configuring each setting individually:

If you do not send the model parameter or even override its settings (mode 2), you will be able to configure each ThinRDP setting individually.
Find below the list of the parameters you can configure manually:

Parameter	What it means	Type/format	Default
`computer`	The remote desktop IP and port to connect to. If you are using "None" or "Username/ Password" as authentication mode or the [any computer] as profile you will have to specify the computer parameter.	**string** IP:Port	
`username` [1]	The username to authenticate against the remote machine. If this parameter is not sent, ThinRDP will prompt the user for this information.	**string** username	
`password` [1]	The password to authenticate against the remote machine. If this parameter is not sent, ThinRDP will prompt the user for this information.	**string** password	

startprg	If you will use the OneTimeURL to start a specific application, you should change this and the following three fields. Set it to 0 for the "Do nothing" option; 1 for the "Start a program" option; 2 for the "Launch RemoteApp" option.	**integer** 0,1 or 2	0
command	Full remote application path that should start upon connection establishment.	**string** app path	
directory	Initial context directory to be used by the application set on command parameter described above.	**string** dir path	
cmdargs	Arguments to start the application specified on the "command" property.	**string** app args	
bpp	Color Depth: sets the number of bits per pixel. Set 8 for 256 colors; 15 for True Color (15 bit); 16 for True Color (16 bit) ; 24 for True Color (24 bit)	**integer** 8,15,16 or 24	16
resolution	"fittobrowser", "fittoscreen", "fixed". When "fixed", the 'width' and 'height' parameters will be considered.	**string** toolbar size	"fittobrowser"
width	Remote desktop screen width. It will only be considered when the resolution parameter is set to "fixed".	**integer** pixels	Desktop width
height	Remote desktop screen height. It will only be considered when the resolution parameter is set to "fixed"	**integer** pixels	Desktop height
imagequality	Specifies the image quality/compression. Set 0 for "Highest"; 1 for "Optimal"; 2 for "Good"; 3 for "Faster"	**integer** 0,1,2 or 3	1
desktopbackground	Set to true to show the original remote desktop background.	**boolean** true,false	false
visualstyles	Set to true to change the start menu and other windows features style.	**boolean** true,false	false
menuwindowanimation	Set to true to show an animation on the Start menu.	**boolean** true,false	false
fontsmoothing	Set to true to make text easier to read, especially magnified text.	**boolean** true,false	false
showwindowcontent	Set to true to show windows contents while dragging them.	**boolean** true,false	false
desktopcomposition	Set to true to configure the DWM to redirected the desktop drawing to off-screen surfaces in video memory. The desktop will also present many visual effects.	**boolean** true,false	false
unicodekeyboard	Allows for using full unicode keyboard charsets. Set to false to connect to xRDP servers.	**boolean** true,false	true
console	Forces the connection to connect to the remote console session.	**boolean** true,false	false
wscompression	Set to true to enable the compression for the exchanged Websocket data and have the application performance improved.	**boolean** true,false	true
disablenla	Set the option disableNLA if you use a CredSSP other than Microsoft.	**boolean** true,false	false

desttype	Set the desttype to "VMID" in case you want to establish a connection to a Hyper-V Virtual Machine or set "RDS" if you want to create a connection to an RDS Collection VM. The connection will act as a regular connection in case you don't inform this property of inform any value different from "VMID" and "RDS".	**string** VMID or RDS	
destinfo	Inform the Virtual Machine ID, for Hyper-V Virtual Machine connections or inform the TSV URL for RDS Collection Virtual Machines.	**string** Virtual Machine ID or TSV URL	
diskenabled	Set to true to have an intermediate disk available on the connection.	**boolean** true,false	true
diskname	Identify the intermediate disk among the other remote desktop disks.	**string** name	"ThinDisk"
diskautodownload	Set to true to automatically download any file saved/copied on the Intermediate disk.	**boolean** true,false	true

1 . By informing the username and password on the URL you will be setting the "Use these credentials" option. If you don't inform username or password, the behavior will follow the "Ask for new credentials" options'.
The "Use the authenticated credentials" option is not suppose to work with the One Time URL, because in this case there is no prior authentication with a valid user for the remote machine.

To add each of the parameters to the queryString, you have to concatenate an "&" symbol, the name of the parameter, the "=" symbol and the value assigned to the parameter, as shown on the example below :

```
...
&password=myPassword&model=0mwZVL@aTkRMwc$mj3kUCrzM6@08yse0C7MED3it...
```

9.6.2 Enabling features

You can also send some parameters on the queryString to enable ThinRDP features.
Find below the parameters you can send in order to enable and configure ThinRDP features for the One-Time-URL connection:

Clipboard:

Parameter	What it means	Type/format	Default
`clipboard`	Set to false to disable the remote desktop clipboard. The clipboard w orks only w ith text.	**boolean** true,false	true

Printer:

Parameter	What it means	Type/format	Default
`printerenabled`	Set to true to enable ThinRDP PDF printer.	**boolean** true,false	false
`printersetasdefault`	ThinRDP printer as the remote default printer.	**boolean** true,false	true
`printername`	Specify the printer name that you w ant to be show n on the remote machine's printer list.	**string** name	
`printerdriver`	Mark this option to set ThinRDP printer as the remote machine default printer.	**string** driver	

Sound:

Parameter	What it means	Type/format	Default
`soundenabled`	Set to true to enable remote sound.	**boolean** true,false	false
`soundquality`	Sets the sound quality. 0 = Excellent, 1 = Optimal, 2 = Good and 3 = Poor.	**integer** 0, 1, 2 or 3	1

To add each parameter to the queryString concatenate an "&" symbol, the name of the parameter, the "=" symbol and the value for the parameter, following this format:

```
...&password=myPassword&clipboard=false...
```

These parameters will be considered only if you are not using a profile as a template or if you configure the overrideDefaults setting to true (see the "Mode 2" on the Configuring the connection section, for more details)

10 Advanced Settings

Once you have configured basic access for ThinRDP, you might want to learn a little more about the other configuration possibilities available in ThinRDP .

- General
- Security
- Access Profiles
- Folders
- Permissions
- SSO
- Licences
- Load Balancing
- Custom Settings
- Customizing the toolbar

10.1 ThinRDP Manager

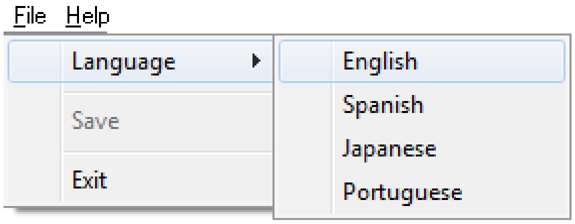
The ThinRDP Server Manager is a tool for administrators to set up general settings.
From this manager you can administer users, profiles, RDP preferences and settings related to the ThinRDP service.
To access ThinRDP manager go over the Start Menu options and look for the "*ThinRDP Server Manager*" item.

The Manager tool is composed by the following tabs:

- General
- Security
- Access Profiles
- Folders
- Permissions
- SSO
- Licences
- Load Balancing

The ThinRDP Manager main menu consists in two sub-menus:

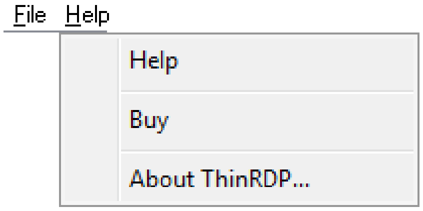
File Menu:



The File Menu is composed by the following options:

Language	Allows you to choose different languages for the application. Click on the Language that you want the application to work with. English is the default language.
Save	Click to save any change done on the system Settings.
Exit	Click on this option to exit the ThinRDP Manager tool.

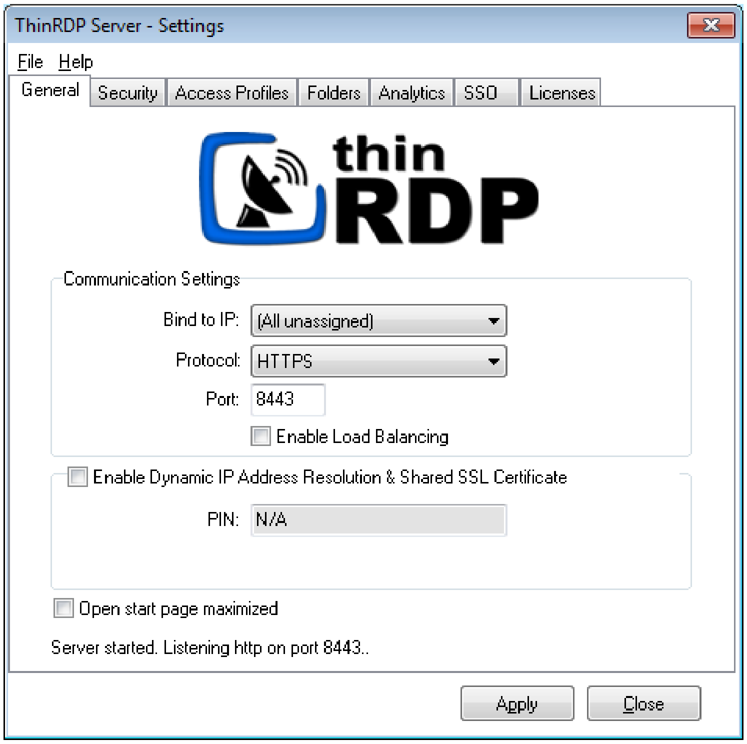
Help Menu:



The Help Menu is composed by the following options:

Help	Takes you to the application online Guide.
Buy	Takes you to the Cybele Sofware Buying page.
About ThinRDP	Click on the About to see the application version and build number.

10.1.1 General



Communication Settings

Bind to IP: (All unassigned)

Protocol: HTTPS

Port: 8443

□ Enable Load Balancing

□ Enable Dynamic IP Address Resolution & Shared SSL Certificate

PIN: N/A

□ Open start page maximized

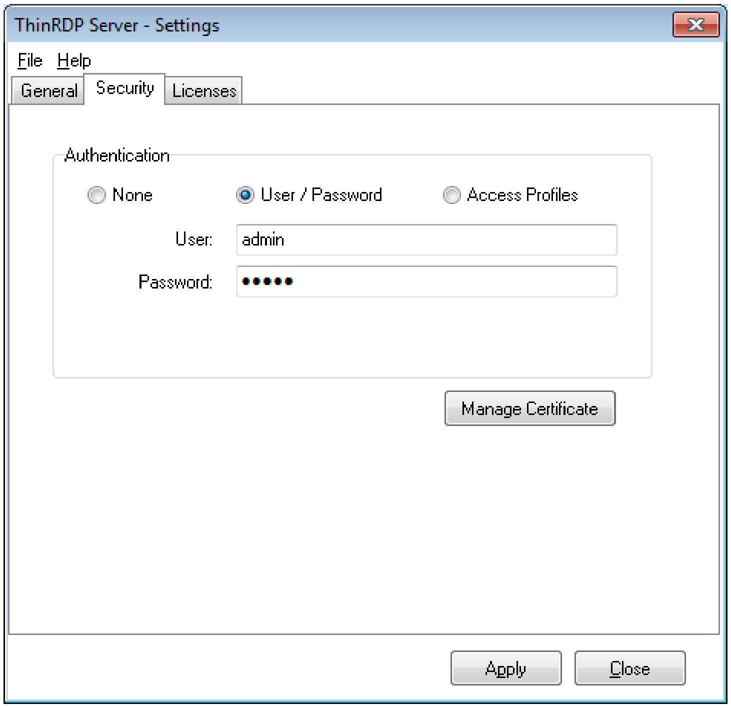
Server started. Listening http on port 8443..

On ThinRDP manager "General" tab you will find the following options:

Bind to IP	Use this option to restrict access to the service through one specific IP. The "All unassigned" option allows access through all the possible IPs for the computer.
Port	Choose which port will ThinRDP be running on. If the port is not available, you will see an error message on the status bar.
Enable Load Balancing	Check this option if you will set the whole ThinRDP environment to work with Load Balancing (this change requires you to adapt ThinRDP architecture and deployment). Once you check this option, the tab Load Balancing will be enabled.
Enable Dynamic IP Address Resolution & Shared SSL	This option works as a Dynamic DNS service to link your IP to a public address in ThinRDP.net and provide you with a Pin code that identifies the ThinRDP server's IP address uniquely. Also in this way you use the SSL certificate provided by the ThinRDP.net site. It is a simple way to provide public access to ThinRDP.
Open start page maximized	Check this option if you want the start page of the Web Interface to be maximized by default. Note: once the user has minimized, the browser will keep it as a user preference, and this setting will not be considered anymore.

Always remember to press "Apply" in order to save the changes.

10.1.2 Security



Authentication

○ None ● User / Password ○ Access Profiles

User: admin

Password: •••••

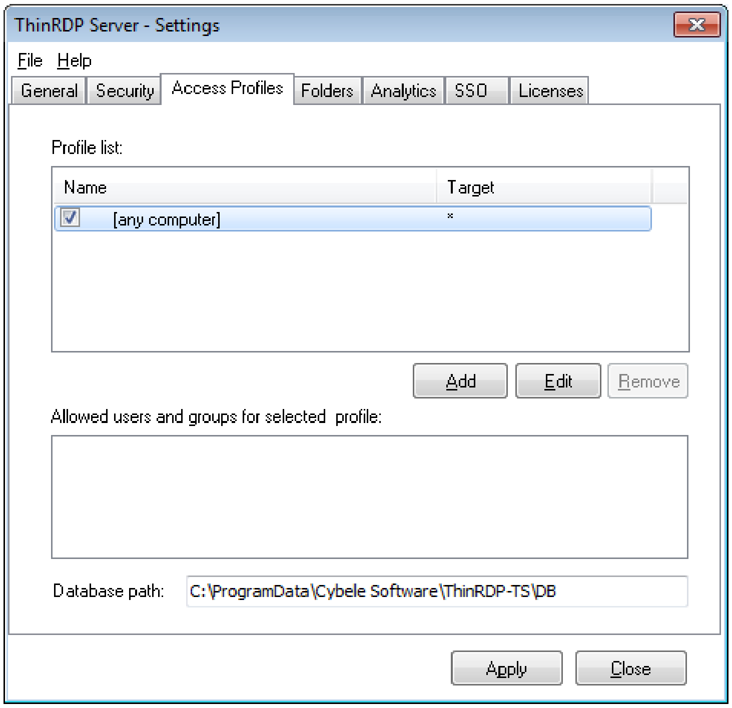
On ThinRDP manager "Security" tab you will find the following options:

<table>
<tr><td>Authentication</td><td>Choose the level of authentication for the users access to ThinRDP. Users will still need to authenticate afterwards against the computer they connect to.
<table>
<tr><td>None</td><td>No authentication for ThinRDP access. This is only recommended for exclusive local access.</td></tr>
<tr><td>User / Password</td><td>Set your own credentials for ThinRDP access authentication.</td></tr>
<tr><td>Access Profiles</td><td>Manage the authentication with Active Directory users by creating a profile. Also select this option to enable profiles and set predetermined preferences for the ThinRDP users.</td></tr>
</table></td></tr>
<tr><td>Use Standard browser authentication dialog</td><td>This option appears when "Authentication" is set to "Access Profiles". Check it to use the standard browser authentication dialog.</td></tr>
<tr><td>Manage Certificate</td><td>Press this button to access the options for replacing the default certificate installed with ThinRDP with your own.</td></tr>
</table>

Always remember to press "Apply" in order to save the changes.

10.1.3 Access Profiles

The "Access Profiles" tab is only enabled when you choose "Access Profiles" as the authentication option on the **"Security" tab**.



Name	Target
☑ [any computer]	*

Database path: C:\ProgramData\Cybele Software\ThinRDP-TS\DB

On ThinRDP's manager "Access Profile" tab you will find the following options:

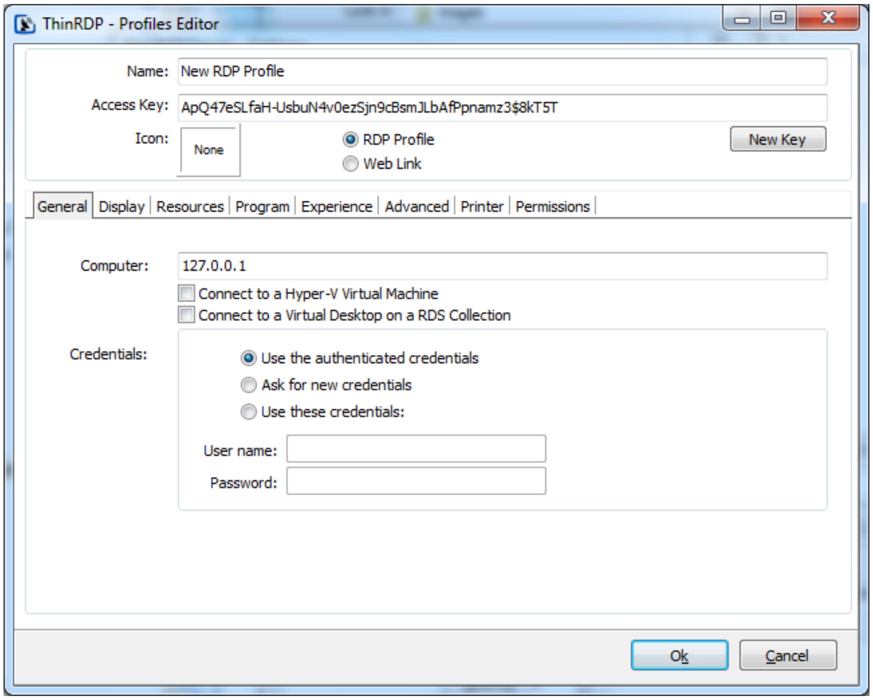
<table>
<tr><td>Profile List</td><td>This list shows the available profiles. You can enable or disable them by checking the box to the left of the name.
<table><tr><td>Name</td><td>Name of the profile.</td></tr><tr><td>Target</td><td>The remote desktop IP or host name for RDP profiles and the web address in case of the Web Link profiles.</td></tr></table></td></tr>
<tr><td>Add</td><td>Press this button to add a new profile.</td></tr>
<tr><td>Edit</td><td>Select a profile and press this button to edit it.</td></tr>
<tr><td>Remove</td><td>Select a profile and press this button to remove it.</td></tr>
<tr><td>Allowed users and groups for selected profile</td><td>See here the allowed users or group(s) of users for the selected profile. If you want to change the user(s), edit the profile.</td></tr>
</table>

Database path	When the application is set to work with Load Balancing, you can set a common database path to all ThinRDP Brokers by informing it on this field.

Always remember to press "Apply" in order to save the changes.

10.1.3.1 RDP Profile Editor

The Profiles Editor is the tool to create, configure and edit RDP "Access Profiles".
When you edit a user profile you will be presented with this screen below.
The RDP profiles must have the radio button "RDP Profile" checked.



ThinRDP - Profiles Editor

Name: New RDP Profile

Access Key: ApQ47eSLfaH-UsbuN4v0ezSjn9cBsmJLbAfPpnamz3$8kT5T

Icon: None

● RDP Profile
○ Web Link

New Key
General | Display | Resources | Program | Experience | Advanced | Printer | Permissions

Computer: 127.0.0.1

□ Connect to a Hyper-V Virtual Machine
□ Connect to a Virtual Desktop on a RDS Collection

Credentials:
● Use the authenticated credentials
○ Ask for new credentials
○ Use these credentials:

User name:

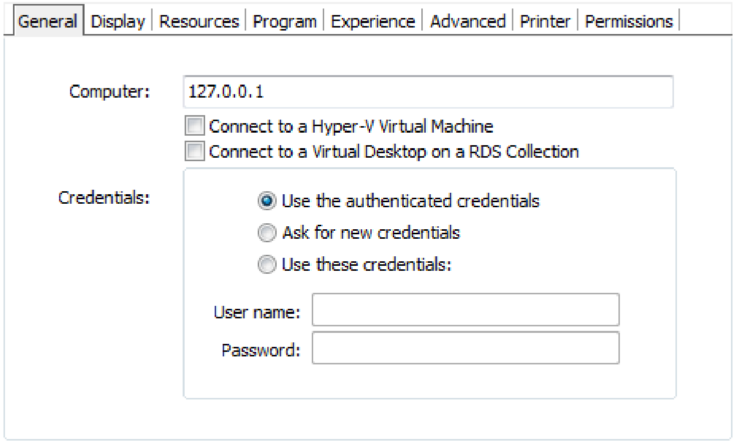
Password:

These are the profile properties you can edit:

Name	Use this field to change the profile name.
Access Key	Used in combination with ThinRDP SDK to access this profile.
New Key	Change the Access Key to disable access through the current key and provide access through a new one.
Icon	Click on the Icon gray box to load an image to be associated with the profile. The image will be presented along with the profile name on the web interface profiles selection.
Web link / RDP Profile	Select the RDP Profile option to have a regular profile that connects to a remote machine or application through RDP.

The properties located inside the tabs will be described throughout the next subtopics.

10.1.3.1.1 General



Computer: 127.0.0.1

□ Connect to a Hyper-V Virtual Machine

□ Connect to a Virtual Desktop on a RDS Collection

Credentials:

● Use the authenticated credentials

○ Ask for new credentials

○ Use these credentials:

User name:

Password:

On ThinRDP's profiles editor "General" tab you will find these following options:

Computer	Specify the computer that this profile will connect to. Enter the internal IP or computer name.
Connect to a Hyper-V Virtual Machine	Check this option if you want to connect to a Hyper-V Virtual Machine through its machine ID or GUID. Learn in details how to set up a Hyper-V profile. If you are able to connect to the Virtual Machine through its IP address or computer name, you can use a regular profile set up, and this option might not be necessary.
Connect to a Virtual Desktop on an RDS Collection	Check this option if you want to connect to a Virtual Machine located within an RDS Collection. Learn in details how to set up a RDS Collection profile.

<table>
<tr>
<td>Credentials</td>
<td>Choose the credentials for logging into the specified computer:
<table>
<tr><td>Use the authenticated credentials</td><td>Use the same credentials entered in the browser for ThinRDP (specified in the "Permissions" tab).
Note: If the credentials are correct for the remote computer, this option will connect the user automatically when selecting the profile, or after authenticating for ThinRDP if this is the only profile for their credentials.</td></tr>
<tr><td>Ask for new credentials</td><td>Prompt the user for new credentials to access the computer.</td></tr>
<tr><td>Use these credentials</td><td>Complete the credentials used to access the computer.
Note: If the credentials are correct for the remote computer, this option will connect the user automatically when selecting the profile, or after authenticating for ThinRDP if this is the only profile for their credentials.</td></tr>
</table>
</td>
</tr>
</table>

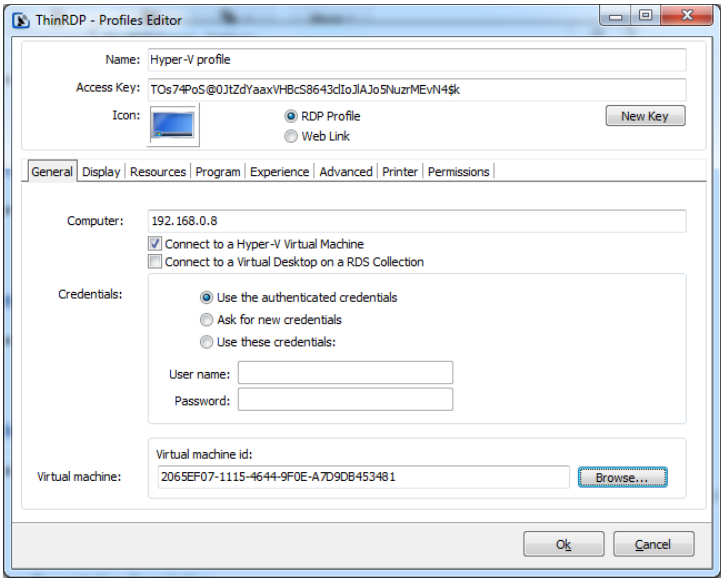
See also, the credentials behavior when using the One-Time-URL.

10.1.3.1.1.1 Setting up a Hyper-V profile

The Hyper-V virtual machine profile will be necessary when you can't access it through a direct IP address or computer name.
When this happens you can use the Hyper-V GUID to locate the virtual machine inside a Hyper-V Server.
Follow the next steps and learn how to configure a Hyper-V profile:

1. Add a new profile.

2. On the profile Computer field, inform the Hyper-V server name or IP address.



ThinRDP - Profiles Editor
General | Display | Resources | Program | Experience | Advanced | Printer | Permissions
New Key
Browse...
Ok
Cancel

Name: Hyper-V profile
Access Key: TOs74PoS@0JtZdYaaxVHBcS8643dIoJlAJo5NuzrMEvN4$k
Icon:
● RDP Profile
○ Web Link

Computer: 192.168.0.8
☑ Connect to a Hyper-V Virtual Machine
□ Connect to a Virtual Desktop on a RDS Collection

Credentials:
● Use the authenticated credentials
○ Ask for new credentials
○ Use these credentials:
User name:
Password:

Virtual machine: Virtual machine id: 2065EF07-1115-4644-9F0E-A7D9DB453481

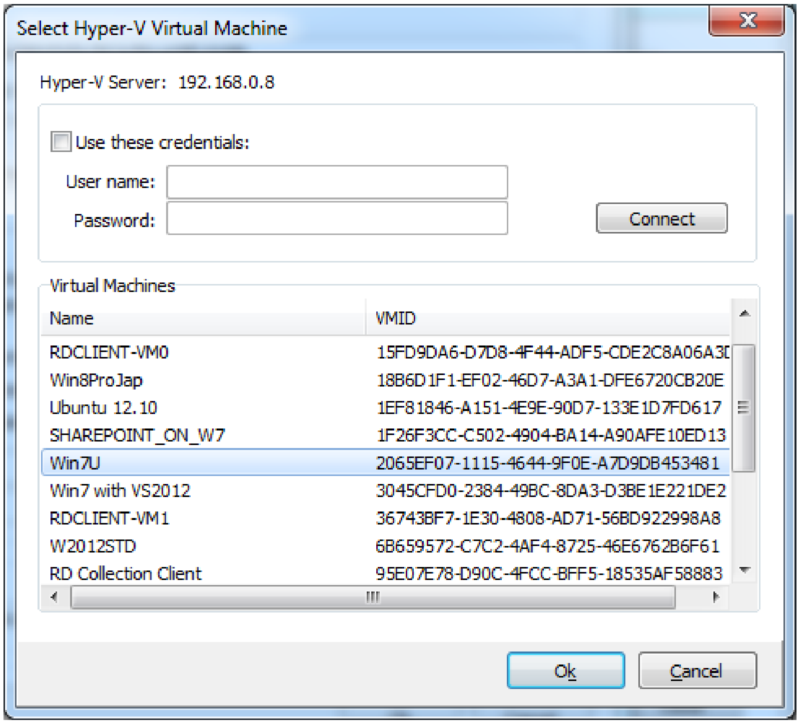
3. Check the option "Connect to a Hyper-V" Virtual Machine.

4. The credentials to be informed will be used to authenticate against the Hyper-V server.

5. If you know the Virtual Machine Id (GUID), inform it on the field "Virtual machine id" and skip the step 6.

6. If you don't know the Virtual Machine GUID, click on the "Browse" button and a search dialog will be presented:

> 6a. Click on the Connect button and the list of virtual machines located on the Informed Hyper-V server will be presented.



Hyper-V Server: 192.168.0.8

☐ Use these credentials:

User name:

Password:

Name	VMID
RDCLIENT-VM0	15FD9DA6-D7D8-4F44-ADF5-CDE2C8A06A3
Win8ProJap	18B6D1F1-EF02-46D7-A3A1-DFE6720CB20E
Ubuntu 12.10	1EF81846-A151-4E9E-90D7-133E1D7FD617
SHAREPOINT_ON_W7	1F26F3CC-C502-4904-BA14-A90AFE10ED13
Win7U	2065EF07-1115-4644-9F0E-A7D9DB453481
Win7 with VS2012	3045CFD0-2384-49BC-8DA3-D3BE1E221DE2
RDCLIENT-VM1	36743BF7-1E30-4808-AD71-56BD922998A8
W2012STD	6B659572-C7C2-4AF4-8725-46E6762B6F61
RD Collection Client	95E07E78-D90C-4FCC-BFF5-18535AF58883

6b. If the Hyper-V server requires authentication you can enter the credentials on the "Use these credentials" box, and the press Connect.

6c. Once the Collection is selected you can double-click on it or click on the OK button.

6d. The virtual machine GUID will be set on the correspondent field.

7. The other profile settings should be configured like any regular profile (Display, Resources, Program, Experience, Advanced, Printer and Permissions).

8. Once you are done configuring the profile, press the OK button and then Apply the changes.

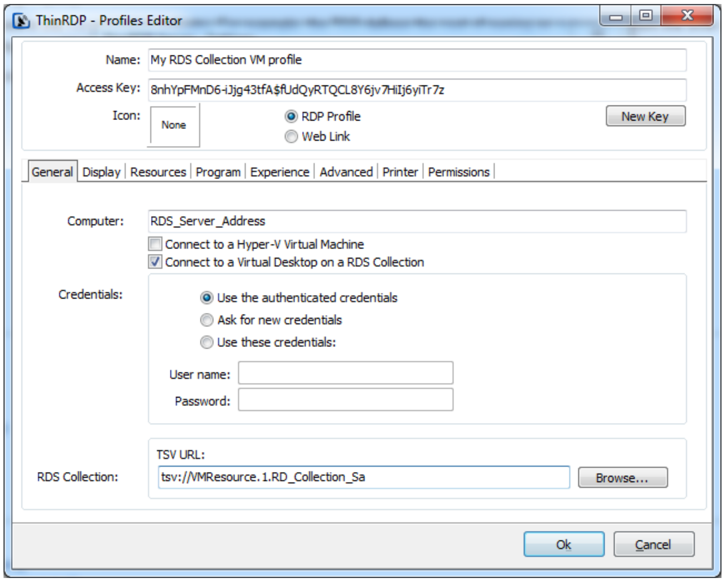
10.1.3.1.1.2 Setting up an RDS Collection profile

When you need to connect to a RDS Collection Virtual machine (pooled or personal), you should set this option.

Follow the next steps and learn how to configure an RDS Collection profile:

1. Add a new profile.

2. On the profile Computer, inform the RDS server name or IP address.


ThinRDP - Profiles Editor

Name: My RDS Collection VM profile

Access Key: 8nhYpFMnD6-iJjg43tfA$fUdQyRTQCL8Y6jv7HiIj6yiTr7z

Icon: None

● RDP Profile

○ Web Link

New Key
General | Display | Resources | Program | Experience | Advanced | Printer | Permissions

Computer: RDS_Server_Address

☐ Connect to a Hyper-V Virtual Machine

☑ Connect to a Virtual Desktop on a RDS Collection

Credentials:

● Use the authenticated credentials

○ Ask for new credentials

○ Use these credentials:

User name:

Password:

RDS Collection: TSV URL: tsv://VMResource.1.RD_Collection_Sa

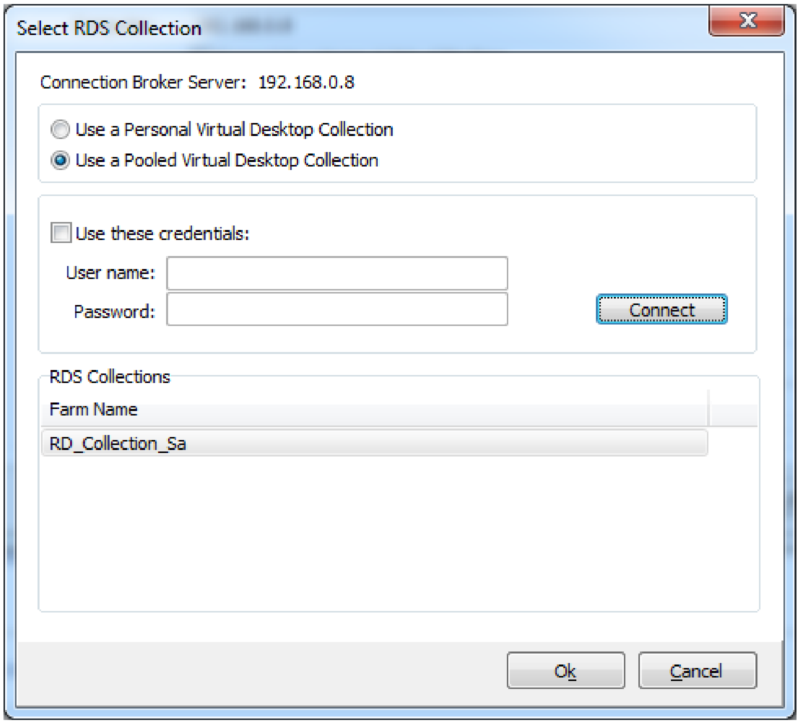
3. Check the option "Connect to a Virtual Desktop on an RDS Collection".

4. The credentials fields are relative to the virtual machine authentication.

5. If you know the URL to the Terminal Service VM Host Agent (the URL follows this format *tsv://VMResource.1.RD_Collection_Sa*), inform it on the field "TSV URL" and skip the next step.

6. If you don't know the TSV URL, click on the "Browse" button and a search dialog will be presented:

6a. Select whether you want to search Personal or Pooled Virtual Desktop Collections.



Select RDS Collection

Connection Broker Server: 192.168.0.8

○ Use a Personal Virtual Desktop Collection

● Use a Pooled Virtual Desktop Collection

□ Use these credentials:

User name:

Password:

RDS Collections

Farm Name
RD_Collection_Sa

6b. Click on the Connect button. If necessary, inform the credentials to the authenticate against the RDS Server.

6c. The Collections found on the server will be presented on the bottom list. Select the one you want to create a profile for.

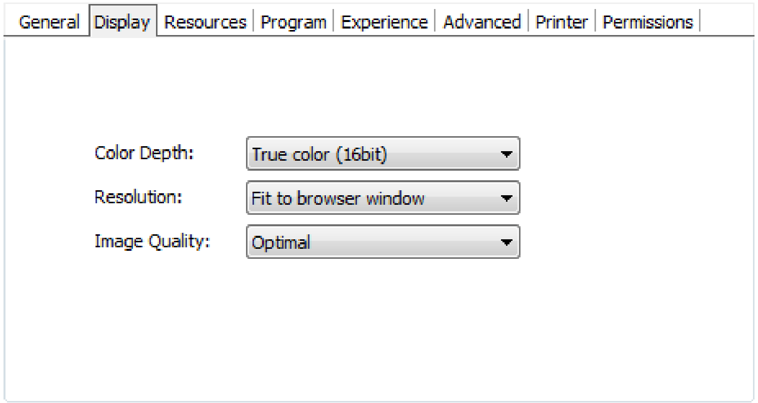
6d. Once the Collection is selected you can double-click on it or click on the OK button.

6e. The TSV URL will be set on the correspondent field.

7. The other profile settings should be configured like any regular profile (Display, Resources, Program, Experience, Advanced, Printer and Permissions).

8. Once you are done configuring the profile, press the OK button and then Apply the changes.

10.1.3.1.2 Display



Color Depth: True color (16bit)

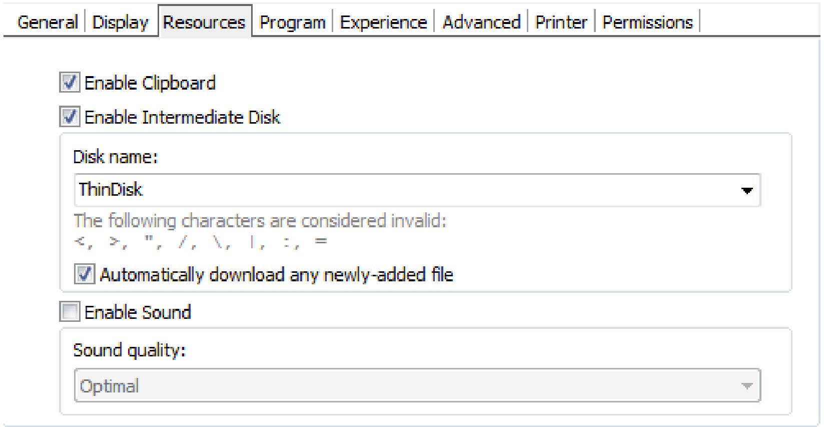
Resolution: Fit to browser window

Image Quality: Optimal

On ThinRDP's profiles editor "Display" tab you will find these following options:

Color Depth	Choose the color depth for the remote computer view.
Resolution	Choose from the available list of resolutions including "Fit to browser window" and "Fit to screen", ideal for hiding the browser and working on a full screen mode.
Image Quality	The connection image quality is a lot related with the application performance (higher quality=lower performance). The default Image quality is Optimal, because it presents the best cost benefit between quality and performance cost. If you need to have more quality or better performance, take a look on the other options below: Highest - Works only with PNG images (0% compression) Optimal - Combines PNG and JPEG images (20% compression). Good - Works only with JPEG images (40% compression) Faster - Works only with JPEG images (50% compression).

10.1.3.1.3 Resources



☑ Enable Clipboard

☑ Enable Intermediate Disk

Disk name: ThinDisk

The following characters are considered invalid:
<, >, ", /, \, |, :, =

☑ Automatically download any newly-added file

□ Enable Sound

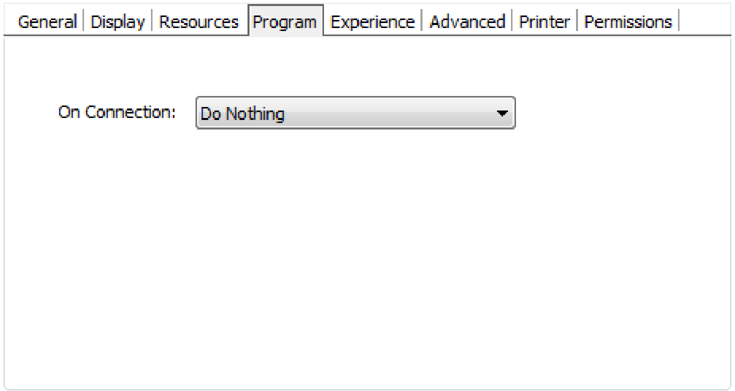
Sound quality: Optimal

On ThinRDP's profiles editor "Resources" tab you will find these following options:

Enable Clipboard	Mark this option to enable the clipboard on the remote connection.
Enable Intermediate Disk	Check this option to have an intermediate disk available on the connections created through this profile.
Disk name	This is the name to identify the intermediate disk among the other remote desktop disks.
Automatically download any newly-added file	If set to true, ThinRDP will download automatically any file saved/copied on the Intermediate disk direction.
Enable Sound	Check this option to enable the remote sound to be reproduced within the browser. The remote sound works only with Firefox and Chrome web browsers.
Sound quality	Determines what quality ThinRDP will use to reproduce the remote sound. The highest quality, the most resources will be required.

10.1.3.1.4 Program

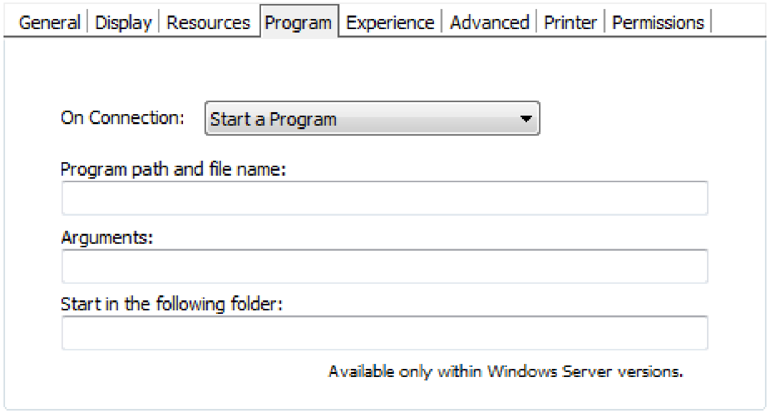
This tab allows users to configure the connection to open a specific application. By default ThinRDP comes with the "Do nothing" option marked. This option will show the whole remote desktop.



On Connection: Do Nothing

Start a Program option:

If you want to set a specific application to start with the connection. Select the "Start a Program" option.
This feature is only available within Windows Server versions.
Once you close the program, the remote session will get disconnected.



On Connection: Start a Program

Program path and file name:

Arguments:

Start in the following folder:

Available only within Windows Server versions.

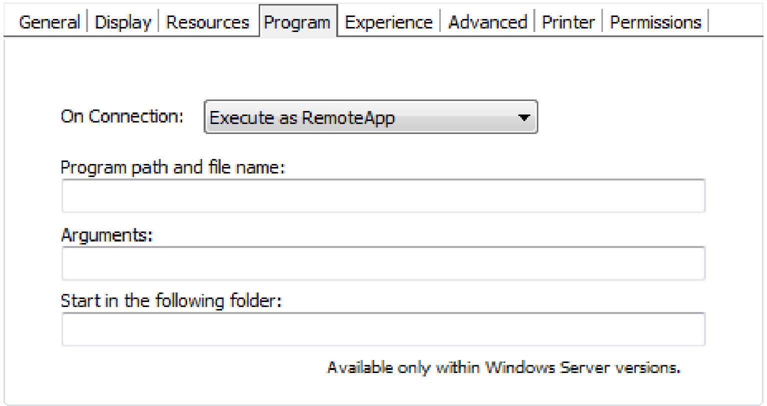
When the "Start a Program" option is selected, you will be presented with the following options:

Program path and file name	Specify the complete path to give access the application you want to start with the connection. Right after the path you should also inform the application arguments, if they exist.
Arguments	Applications arguments.

Start in the following folder	Inform a context directory for the program set on the field "Program path and file name"

Launch RemoteApp:

The RemoteApp is a Terminal Services feature that allows Windows®-based application publishing. You can connect to an application using RemoteApp through ThinRDP, by selecting the "Launch RemoteApp" on the Program tab.



On Connection: Execute as RemoteApp

Program path and file name:

Arguments:

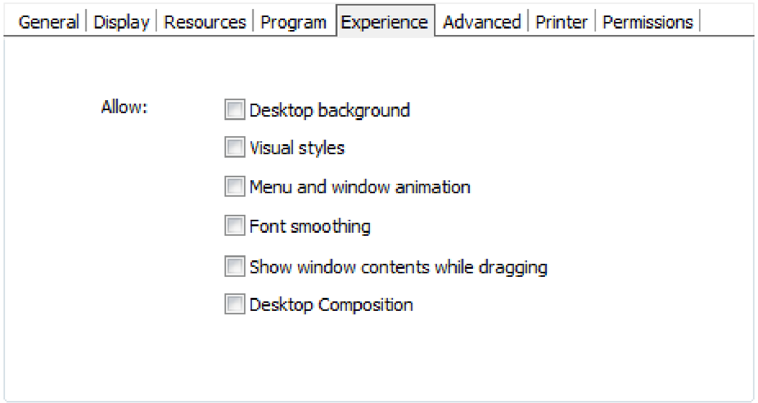
Start in the following folder:

Available only within Windows Server versions.

When the "Execute as RemoteApp" option is selected, you will be presented with the following options:

Program path and file name	Application published name or the direct path to the application file.
Arguments	Applications arguments.
Start in the following folder	Specify a context directory for the program set on the field "Program or file"

10.1.3.1.5 Experience



Allow:

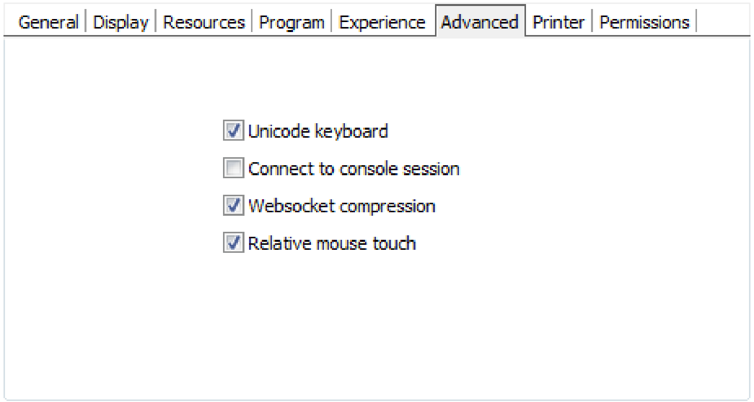
☐ Desktop background
☐ Visual styles
☐ Menu and window animation
☐ Font smoothing
☐ Show window contents while dragging
☐ Desktop Composition

On ThinRDP's profiles editor "Program" tab you will find these following options:

Desktop Background	Check this option to show the desktop background.
Visual Styles	Check this option to show Windows Visual Styles: the appearence of common controls, colors, bordes, and themes.
Menu and Windows Animation	Check this option to show menu and windows animation when you scroll or expand a drop down menu.
Font Smoothing	Check this option to allow "Clear Type", a font smoothing option added to Windows Server 2008.
Show Window Content While Dragging	Check this option to show the contents of the window while being dragged. Otherwise a transparent border is dragged.
Desktop Composition	Check this option to configure the DWM to redirected the desktop drawing to off-screen surfaces in video memory. Also, the desktop will present many visual effects.

All of these options enhance the look of the remote desktop and use more bandwidth.

10.1.3.1.6 Advanced



☑ Unicode keyboard

☐ Connect to console session

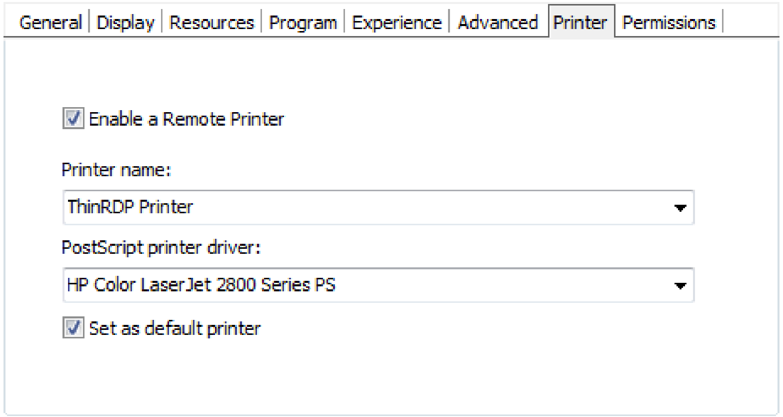
☑ Websocket compression

☑ Relative mouse touch

On ThinRDP's profiles editor "Program" tab will find these following options:

Unicode Keyboard	Uncheck this option to connect to Unix computers through xRDP.
Connect to console session	Check this option to connect to the console session. This require confirmation from the logged on user and log out the current session.
Websocket compression	Check this option to enable the compression for the exchanged Websocket data and have the application performance improved. It only works in browsers which have the websockets compression implemented and enabled.
Relative mouse movement	The relative mouse movement is a mouse behaviour encountered in touch screen mobile devices, in which the screen cursor moves relatively to the touch. Uncheck this option to have a mouse behaviour similar to the real desktop mouse in which the cursor will be always positioned under the touch.

10.1.3.1.7 Printer



☑ Enable a Remote Printer

Printer name:

ThinRDP Printer

PostScript printer driver:

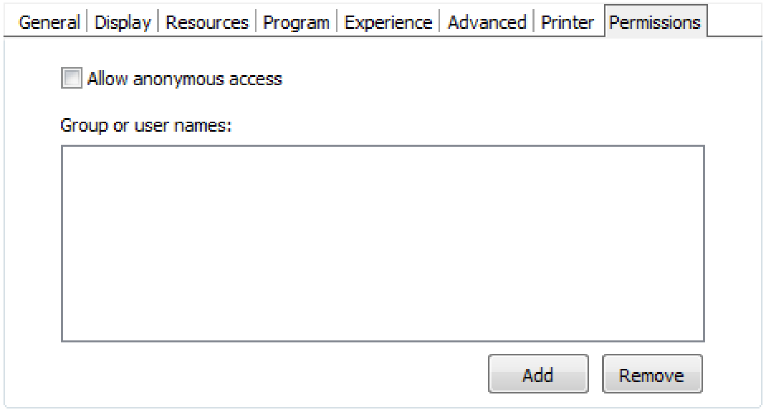
HP Color LaserJet 2800 Series PS

☑ Set as default printer

On this tab you can configure the ThinRDP PDF Printer.
These are the options you will find on the ThinRDP' profiles editor "Printer" tab:

Enable a Remote Printer	Uncheck this option to disable ThinRDP PDF printer.
Printer name	Specify the printer name that you want to be shown on the remote machine's printer list.
PostScript printer driver	This is the driver to be used by ThinRDP in order to print the remote documents. The "*HP Color Laser Jet 2800 Series PS*" driver is compatible with 2008 Windows versions. The "*HP Color LaserJet 8500 PS*" driver is compatible with 2003 Windows versions. The "*Microsoft XPS Document Writer V4*" driver is compatible with Windows Server 2012 and Windows 8. Despite the fact this field is a drop-down menu, you can still type in any other driver that is not listed on the menu. So, if you are not using 2003 or 2008 Windows versions, look for a driver that is already installed on the OS and inform this driver name in this field.
Set as default printer	Mark this option to make ThinRDP printer the remote machine default printer.

10.1.3.1.8 Permissions



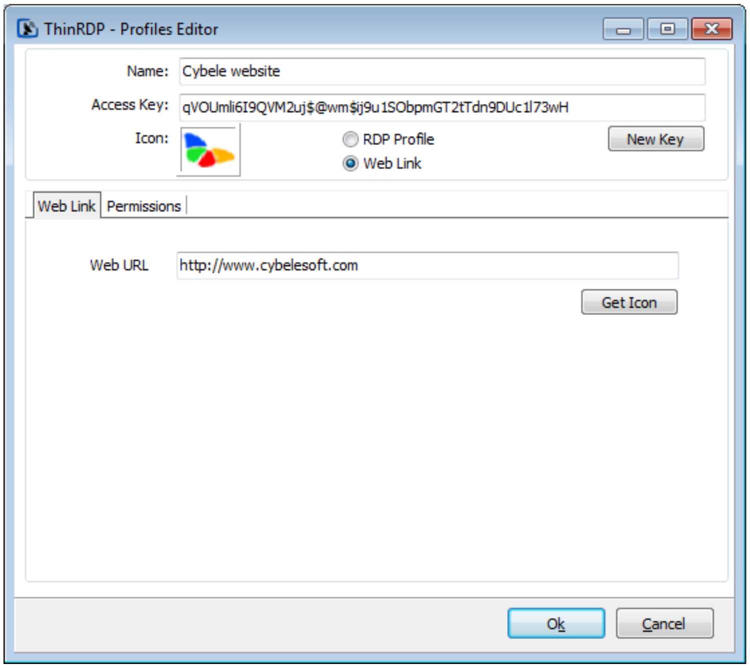
Here you need to select the users that will access this profile. If you don't select any users, this profile will not be accessed.
These are the options you will find on the ThinRDP' profiles editor "Permissions" tab:

Allow anonymous access	Check this option to make this profile available without any authentication. Use this option, if you want this profile to be available for everyone. This means that everybody accessing ThinRDP will see this profile. Checking this option will disable the Add and Remove buttons.
Add	Press "Add" to access the windows dialog for selecting Active Directory users.
Remove	Press "Remove" to remove a user for this profile.

If you want a user or a user group to access more than one computer, you need to create more profiles and then add this user to each profile.
The authenticated user will be able to choose which one of the available profiles to connect.

10.1.3.2 Weblink Profile Editor

The Profiles Editor is the tool to create, configure and edit RDP "Access Profiles".
When you edit a user profile you will be presented with this screen below.
The RDP profiles must have the radio button "RDP Profile" checked.



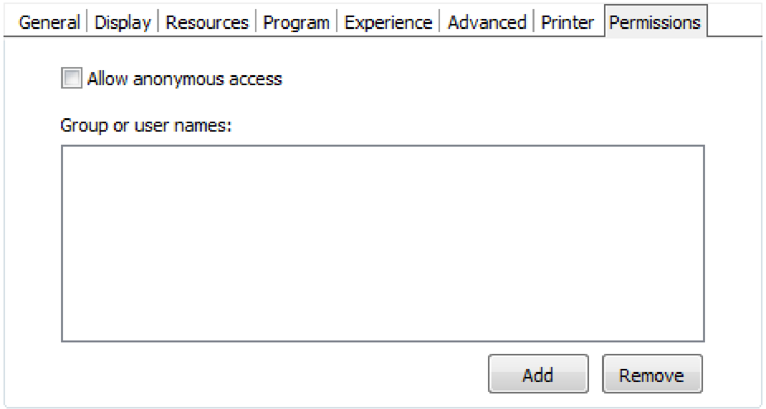
Name: Cybele website
Access Key: qVOUmli6I9QVM2uj$@wm$ij9u1SObpmGT2tTdn9DUc1l73wH
Icon:
○ RDP Profile
● Web Link
Web URL http://www.cybelesoft.com

These are the profile properties you can edit:

Name	Use this field to change the profile name.
Access Key	Used in combination with ThinRDP SDK to access this profile.
New Key	Change the Access Key to disable access through the current key and provide access through a new one.
Icon	Click on the Icon gray box to load an image to be associated with the profile. The image will be presented along with the profile name on the web interface profiles selection.
Web link / RDP Profile	Select the Weblink option to have a profile that connects to a Web link. These links will be shown along with the other profiles on the web interface.
Web URL	Inform in this field the URL that you want this profile to connect to.

The properties located inside the other tabs will be described throughout the next subtopics.

10.1.3.2.1 Permissions



☐ Allow anonymous access

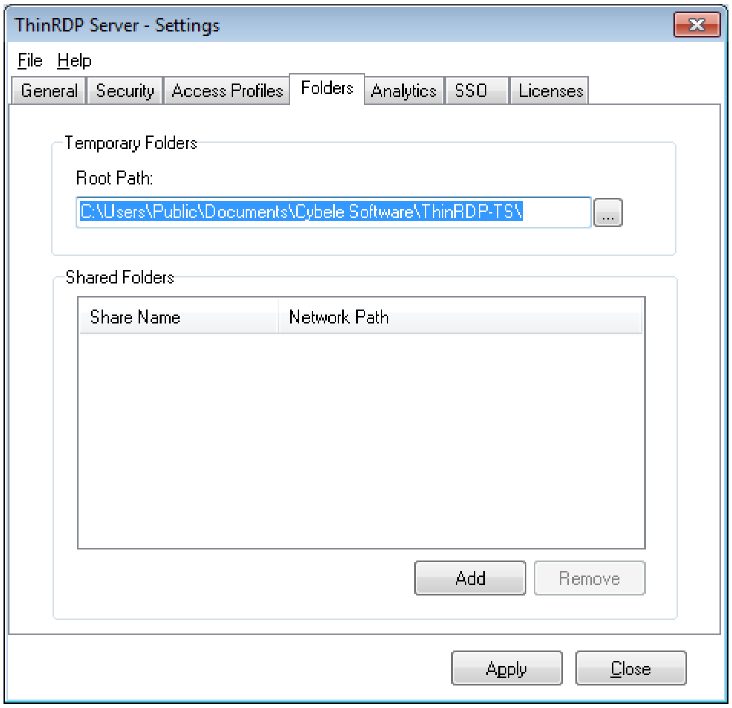
Group or user names:

Here you need to select the users that will access this profile. If you don't select any users, this profile will not be accessed.
These are the options you will find on the ThinRDP' profiles editor "Permissions" tab:

Allow anonymous access	Check this option to make this profile available without any authentication. Use this option, if you want this profile to be available for everyone. This means that everybody accessing ThinRDP will see this profile. Checking this option will disable the Add and Remove buttons.
Add	Press "Add" to access the windows dialog for selecting Active Directory users.
Remove	Press "Remove" to remove a user for this profile.

If you want a user or a user group to access more than one computer, you need to create more profiles and then add this user to each profile.
The authenticated user will be able to choose which one of the available profiles to connect.

10.1.4 Folders

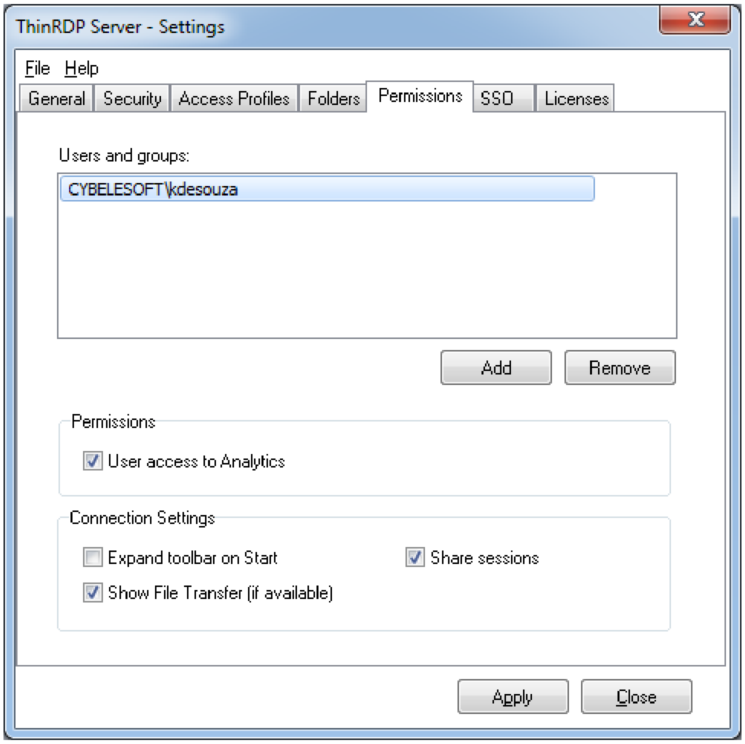


On the ThinRDP manager "Folders" tab you will find the following options:

Temporary Folders (root path)	The temporary folders are used to keep temporary files such as: - Printed documents - Files uploaded from the remote machine - Files copied into the mapped intermediate disks The default root path location is shown on the image above. You may need to modify the temporary folders to another disk location in case you have intensive files exchange or also, if users start using the intermediate disks as their personal storage folder.
Shared Folders	A Shared Folder is a directory that will be set as one mapped disk inside the remote desktop connection. They are accessible by all ThinRDP users/profiles as a disk in the remote connection and also as a File Transfer location. Add: Click on the "Add" button and inform the directory to be shared, in order to create a new shared folder. Remove: Select an existing folder and click on the "Remove" button.

Always remember to press "Apply" in order to save the changes.

10.1.5 Permissions



Users and groups:

CYBELESOFT\kdesouza

Permissions

☑ User access to Analytics

Connection Settings

☐ Expand toolbar on Start

☑ Share sessions

☑ Show File Transfer (if available)

On the ThinRDP manager "Permissions" tab you will find the following options:

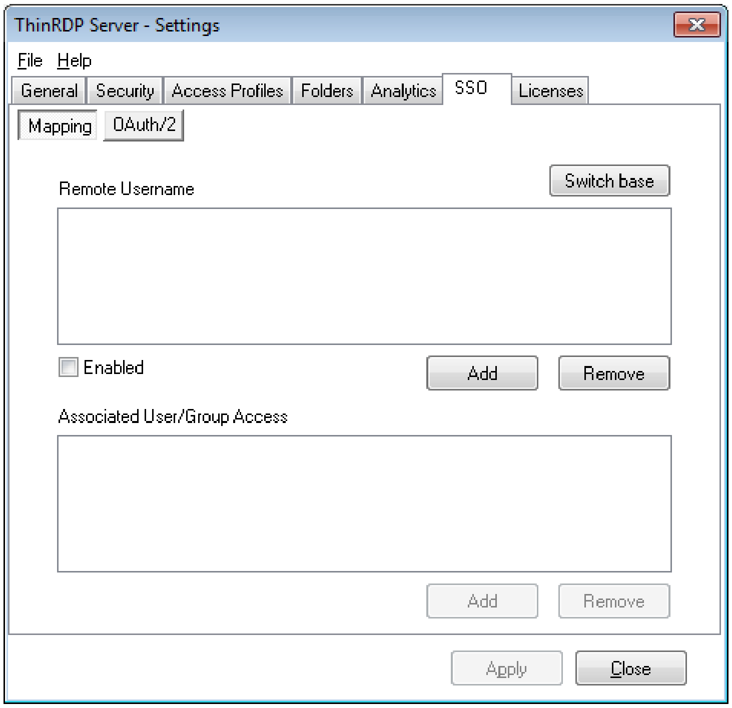
Users and Groups	List with the users and groups to grant permissions to.
Add	Adds a new Active Directory user or group into the Permissions list.
Remove	Select a listed user/group and click on the 'Remove' button to take all of its previous permissions and remove it from the list.
User access to Analytics	Select a user from the list and check this option to give him/her access to the Analytics feature.
Expand toolbar on Start	Through this option you can configure whether the connection toolbar should start expanded or closed for the selected user on the list.
Show File Transfer	If you check this option the selected user will have access to the File Transfer feature (downloads and uploads).

Share Sessions	This checkbox allows you to grant the selected user permission to use the Share Session feature.

Always remember to press "Apply" in order to save the changes.

10.1.6 SSO

Mapping tab:



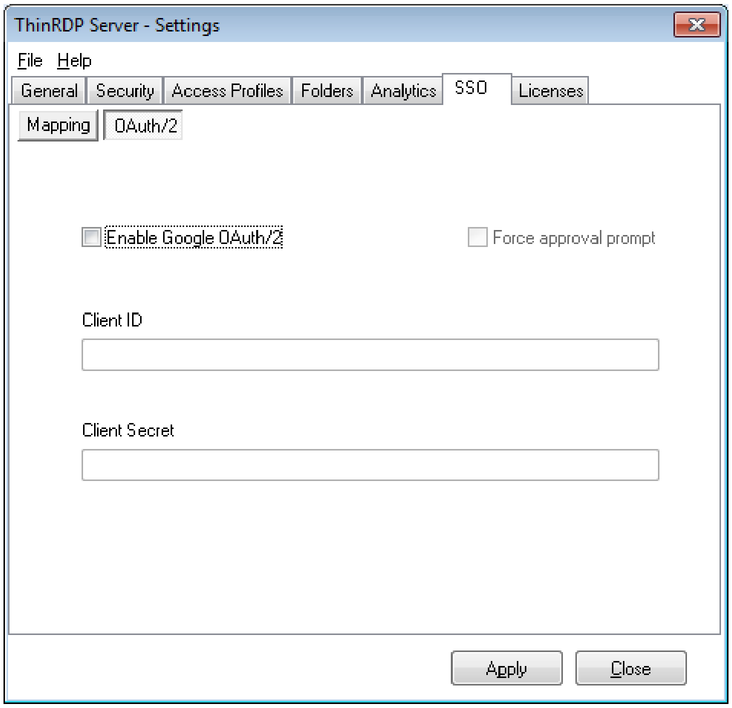
This first tab relates a user from an external Single-sign-on method with a ThinRDP one.
This mapping will allow that remote users will be granted with the same access a local user has.

Remote Username	List with the remote users that will be mapped to the ThinRDP ones. Add: Add a new remote user (SSO) to be mapped with a ThinRDP one. Remove: Select an use and click on the 'Remove' button to take out this remote user from the SSO authentication control. Enabled: Select an user on the list and uncheck the 'Enabled' field if you want to disable the access of this specific remote user.
Associated User/Group Access	List of Active Directory Users and Groups associated with the remote user selected on the List above. Add: Grant the permissions of an Active Directory User or Group to the selected remote user on the list above.

	Remove: Disassociate a User/Group from the remote user selected on the list above.
Switch base	Click on this button to have the Remote Username List switched with the Associated User/Group Access List. The upper list selected item is always the reference to associate the items from the bottom list.

Always remember to press "Apply" in order to save the changes.

OAuth/2 tab:



☐ Enable Google OAuth/2

☐ Force approval prompt

Client ID

Client Secret

On the ThinRDP manager "OAuth/2" tab you will find the following options:

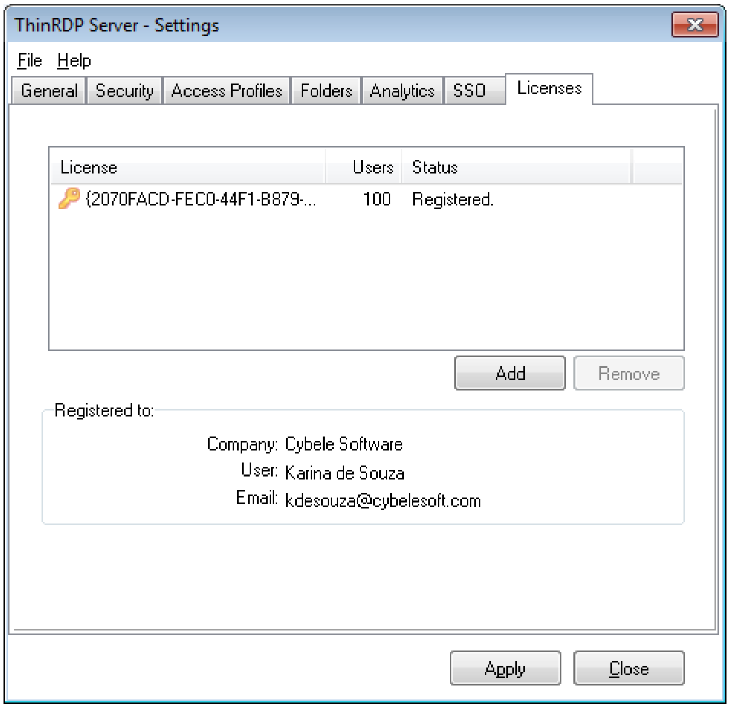
Enable Google OAuth/2	Check this option to enable the Google SSO Integration for the application authorization.
Force approval prompt	If this option is marked, the user will be always prompt to approve the account integrations, when logging into the application.

Client ID	Google Client ID generated while configuring the google account integration.
Client Secret	Google Client Secret generated while configuring google the account integration.

Always remember to press "Apply" in order to save the changes.

10.1.7 Licenses

On the ThinRDP manager "Licenses" tab you will find the following options:



License	Users	Status
{2070FACD-FEC0-44F1-B879-...	100	Registered.

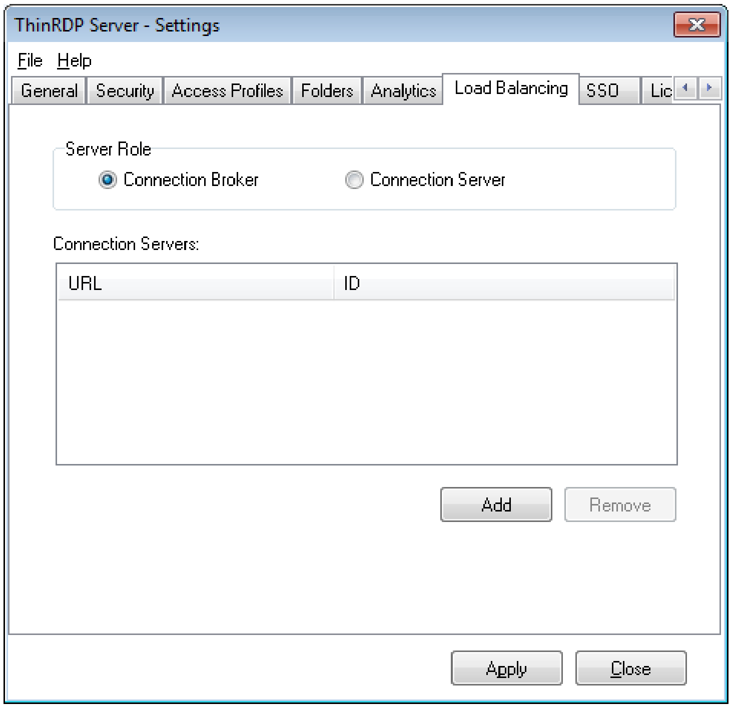
Registered to:

Company: Cybele Software
User: Karina de Souza
Email: kdesouza@cybelesoft.com

This tab always shows the licenses you have currently installed. If you don't have a license yet, you will see a message letting you know how many evaluation days you have left until the trial finishes.
Contact us regarding pricing and/or licensing questions.

10.1.8 Load Balancing

The "Load Balancing" tab is only enabled when you check the option "Enable Load Balancing" on the General tab.
First select the Server Role this machine will play.



Server Role

● Connection Broker ○ Connection Server

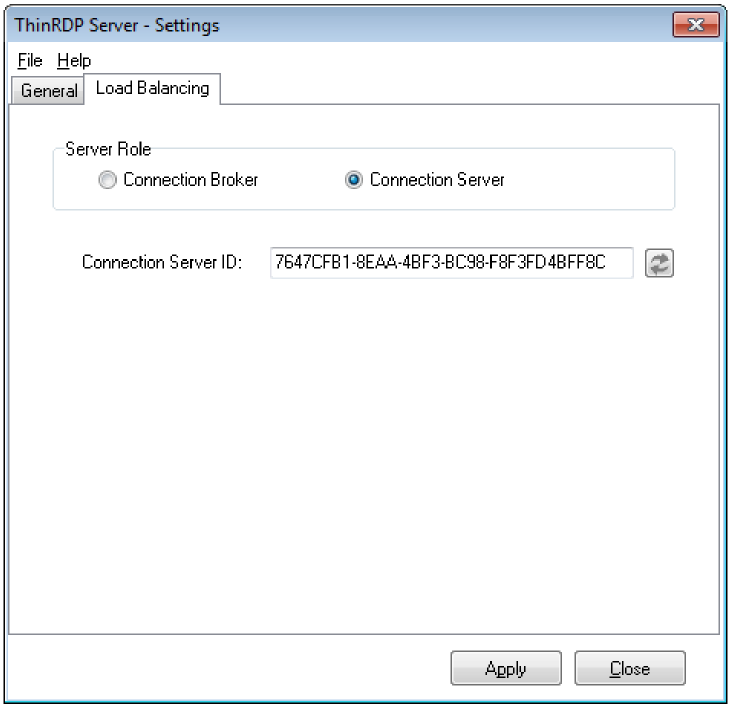
Connection Servers:

URL	ID

If you are configuring a Server "Connection Broker", you will be presented with the following options:

Connection Servers	List with the servers that will help processing the workload managed by this Conection Broker. URL — Server URL ID — Server ID
Add	Add a new server to help processing the workload.
Remove	Select a listed server and click on the 'Remove' button to take out the server.

If you are configuring a Server "Connection Server", you will be presented with the following options:



Server Role

○ Connection Broker ● Connection Server

Connection Server ID: 7647CFB1-8EAA-4BF3-BC98-F8F3FD4BFF8C

Connection Server ID	Click on the "Refresh" button to have a new ID assigned to this server.

Always remember to press "Apply" in order to save the changes.

- Read more about Load Balancing

10.2 Custom Settings

Custom settings is a way to easily set global parameters that will affect all the ThinRDP Server functioning, regardless of the session.

The customsettings.js file is distributed with the ThinRDP Server installation. You can find it in the installation directory, inside the 'webrdp' folder. It is a javascript file that contains javascript code which is read by the client's browser when they access ThinRDP Server and then communicates with ThinRDP Server to send information, like toolbar parameters. You can open it with any text editor, like notepad.

These are the initial values:

```
var customSettings = {
    "createToolbar": true,                  // Create ThinRDP toolbar
    "toolbarVisible": false                 // ThinRDP toolbar starts expanded (visible)
};
```

The customSettings variable uses the JSON format, a collection of name/value pairs. When ThinRDP starts it will read the values in customSettings and override with its settings the options that are set in the profiles. It is recommended to always use the profiles for configuring, because it might lead to misinterpretation to have the configuration in a file that is not seen in the interface. Therefore, the use of this file is recommended only for situations when many profiles are already created and it would take too long to modify them all. Custom settings offers a way to quickly configure settings that will affect all the connections, such as customizing the toolbar.

Apart from the initial values, the values that can be passed in the customSettings variable are most of those used in the connect method in the SDK. Add the overrideDefault value when using values that need it. This is specified in the connect method parameter reference.

Read More:
- The connect method.

10.3 Customizing the toolbar

By default, the ThinRDP toolbar displays the wider range of options within reach for the end users. As an administrator, you might want to restrict the end user from accessing certain options, or give them more visibility.

The createToolbar parameter set to false will result in a ThinRDP connection with no ThinRDP toolbar at all. This might be useful if you want to restrict the user from all options in the toolbar. The toolbarVisible parameter set to true, will result in the ThinRDP toolbar expanded when the connection to the remote desktop or application is established. This might be useful if, on the contrary, you want the user to be aware of the options available. If, for some reason, you think the user will not think of expanding the toolbar using the expand small arrow on top of the screen.

If you want a simple and straightforward configuration, you can add these parameters in the the customsettings.js. The options that you set through this method will affect all the ThinRDP connections, regardless of the session. Read more about customizing the toolbar using customsettings.js.

If you want to fine-tune these settings for different profiles, you can use the SDK library. Read more about customizing the toolbar using the connect method.

Read more about the toolbar user reference with option descriptions.

10.3.1 Using customsettings.js

The customsettings.js file is distributed with the installation of ThinRDP Server . You will find this file in the 'webrdp' folder in the ThinRDP Server installation directory.

customsetings.js is a javascript file that contains javascript code which is read by the client's browser when they access ThinRDP Server and then communicates with ThinRDP Server to send information, like toolbar parameters. You can open it with any text editor, like notepad.

The initial values include the createToolbar and toolbarVisible parameters. Change their value to false/true following the format.

```
var customSettings = {
   "createToolbar": true,                  // Create ThinRDP toolbar
   "toolbarVisible": false                 // ThinRDP toolbar starts expanded (visible)
};
```

The double slash indicates a comment, and the text that follows is not considered code —as long as it is on the same line. You can use comments to write notes next to the parameters in customsettings.js

In this example, the comments are being used to describe the function.

When you are done, close the file and save the settings. Don't change the file's location. The changes will be taken by ThinRDP immediately.

- Read more about Custom Settings.

10.3.2 Using the connect method

If you are using the SDK library, you can use the createToolbar, toolbarVisible and toolbarRestrictions parameters in the connect method.

Read more about how to get started with the ThinRDP Server SDK library.

Here is the syntax for the toolbar parameters:

```
mythinrdp.connect({
                    createToolbar:      true,
                    toolbarVisible:      true
});
```

10.4 Load Balancing

Load balancing and Fault-tolerance are methodologies to distribute workload across multiple services to achieve optimal resource utilization, avoid overload and allow the system to operate properly in the event of failure of some of its components.

On this help section you will learn how to set a network configuration using a combination of Round-Robin DNS and the Load Balancing feature included in ThinRDP Server.

Round-Robin DNS

Round-Robin DNS is a simple method of load balancing, where a list of IP addresses are associated with a single domain name. The list is continuously permuted, so the returned IP address varies for each DNS response.

ThinRDP’s Load balancing feature

ThinRDP Server can be configured in two basic ways: normal mode and Load Balancing mode.

Normal mode:

This is the default mode in which one single ThinRDP Server centralizes all the web requests and the same server creates and processes all the RDP connections.

In some occasions, this configuration may cause an overload of the ThinRDP Server machine resources. Some examples are too many concurrent users establishing connections at a time, or also when ThinRDP integrates applications that handle a lot of graphics, sound and other elements that require a great availability of resources. In all those cases, there is a moment in which one machine is not capable of managing all the required resources. This is when you should start considering using the Load Balancing mode.

Load balancing mode:

In this mode, ThinRDP must be installed in two or more servers that will participate in the load balancing /fault-tolerance scenario. Two possible roles can be configured:

Connection Broker: Under this role, ThinRDP responds to all web-pages requests and, when an RDP connection to a remote desktop is solicited, it selects the appropriate Connection Server to forward that request. The final RDP connection is done through the chosen Connection Server.
In case any established connection fails, or a Connection Server falls down, the Broker will be able to reconnect to the Server with the highest availability at a that moment.
All the system settings and profiles are centralized and stored on this server.

Connection Server: Under this role, ThinRDP processes forwarded RDP connections only. This server is responsible for establishing and processing the RDP connections assigned by the Connection Broker. All Connection Servers must have their IPs public to the client’s Web Browser, so that once the RDP connection has been assigned by the server, the browser can redirect its request to this new server.

Some of the benefits of using the Load Balancing architectures are:

- Avoid the overload by distributing the connections among different servers

- Minimize response time
- More reliability (redundancy)
- Fail over control

Before starting to configure a distributed environment to work, there are some previous steps you should go over :

1. Choose the architecture out of the three possible ThinRDP Load Balancing architectures, that will best fit your need.
2. Plan the machines that will work as Connection Brokers, Connection Servers/ThinRDP Servers and DNS Servers, depending on the chosen architecture.
3. Make sure all their IP's addresses are public to the Web Browsers that will access ThinRDP.

10.4.1 Architectures

If you came to the conclusion that your ThinRDP environment needs to work with the Load Balancing mode, there will be three possible architectures to choose from.
The decision on the architecture that will be used is an essential step to be able to plan the hardware scheme and configure the system to work in a distributed way.

The three possible architectures are described on the links bellow. Under these topics, you will also find out how to set up each one of these architectures environment:

1. ThinRDP's Load Balancer only (One connection broker, multiple connection servers)

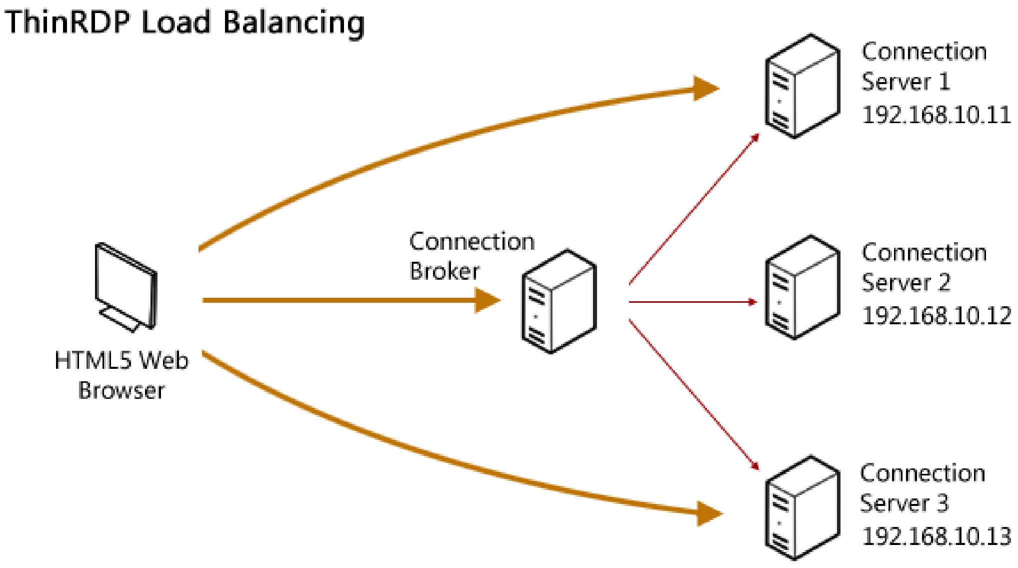
2. Round-Robin DNS only (Multiple ThinRDP Servers associated to a DNS Server)

3. Round-Robin DNS + ThinRDP's Load Balancer (Multiple ThinRDP Servers and multiple connection brokers associated to a DNS Server)

10.4.1.1 ThinRDP's Load Balancer only

With ThinRDP’s load balancing feature, RDP connections are evenly distributed across multiple Connection Servers. This architecture is composed by a single Connection Broker and multiple Connection Servers.

The image below illustrates the ThinRDP’s Load Balancer architecture:


ThinRDP Load Balancing
Connection Server 1 192.168.10.11
Connection Broker
Connection Server 2 192.168.10.12
HTML5 Web Browser
Connection Server 3 192.168.10.13

Setting up the architecture:

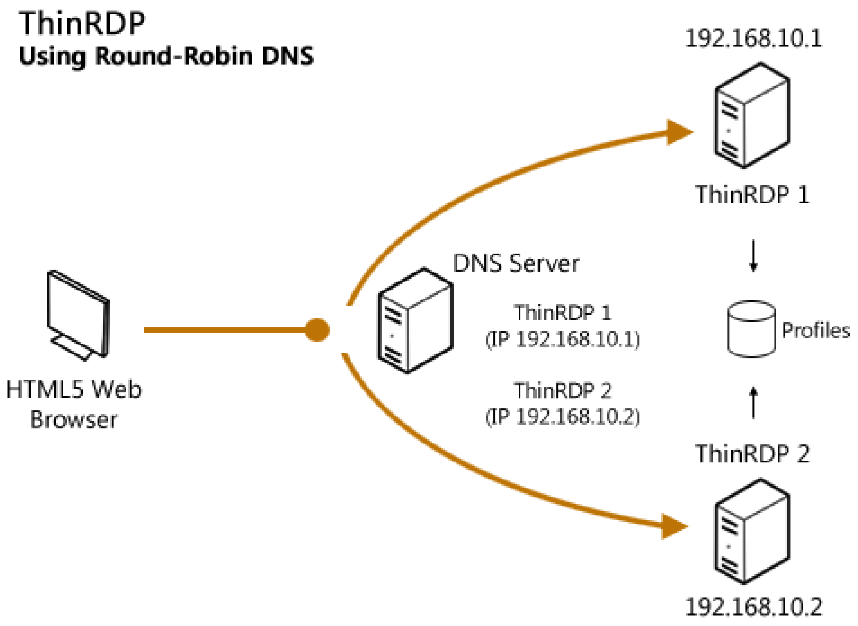
1. Set up each one of the existing Connection Servers
2. Set up the Connection Broker
3. Make sure all the Connection Servers and the Connection Broker IP's are public to the Web Browsers that will access ThinRDP.

10.4.1.2 Round-Robin DNS only

In this case, the DNS will be in charge of distributing load to a number of ThinRDP Servers. Each ThinRDP Server needs to be configured in such way that they can share the profiles database.

The difference between these technique and the ThinRDP Load Balancing is that the Round-Robin DNS does consider the workload of each ThinRDP Server in order to assign a new connection to be processed. This method does not make a failover control, because the DNS Server does not know whether the ThinRDP Server is active and receiving requests. If a Server falls down, the DNS Server will keep redirecting web requests to it.

The image below shows how the "Round-Robin DNS" architecture works:



Setting up the architecture:

1. Install ThinRDP on each one of the machines that will act as ThinRDP Servers.

2. Set the Profiles "Database Path" of all Servers to the same database file. On the bottom of the Access Profiles tab, there is a field called "Database Path".

3. Configure all the settings (General, Security, Access Profiles[1], Folders, Permissions and License)[2].

4. Configure your DNS Server, associating the domain name with all the existing ThinRDP Servers IP's.

5. Make sure all the ThinRDP Servers are public to the Web Browsers that will access ThinRDP.

Important observations:

[1]. On the step 3, the Access Profiles settings have to be done only in one of the existing servers. The other servers should be pointing to the same database file, so that once the profiles are configured in one ThinRDP Server, they will work evenly for all of them.

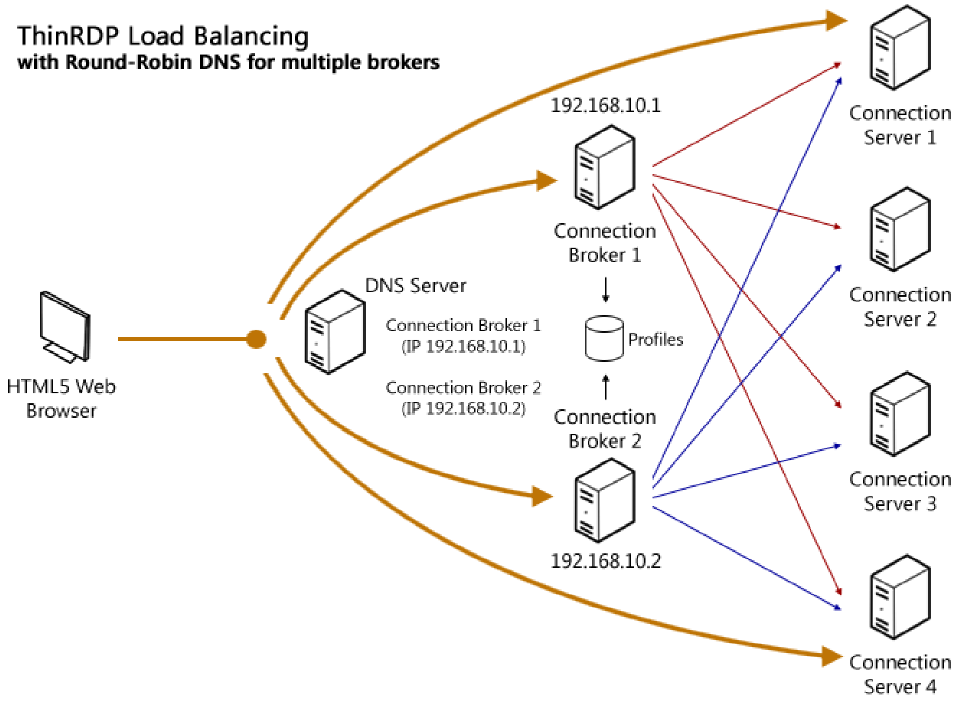
[2]. It is recommended that all ThinRDP Servers have the same "Authentication Method", " Temporary and Shared Folders Settings". That way, the different ThinRDP Servers will establish connections that same way and keep all the Folders data centralized.

10.4.1.3 Round-Robin DNS + ThinRDP's Load Balancer

The combination of the other two architectures will shape this one. It combines the ThinRDP Load Balancer to allow load balancing and failover among the RDP connections and the Round-Robin DNS scheme to allow multiple Connection Brokers. The brokers will be responsible to manage the system settings and profiles, that is why they have to be configured in such way that they can share the profiles database.
The scheme is composed by multiple Connection Servers, multiple Connection Brokers and the DNS Server with the domain name associated to all the available Brokers IP's.

It can guarantee more availability once there is redundancy of the Connection Server and the Connection Brokers. However, the Connection Brokers accessed by the DNS Server do not have a failover control. If one Connection Broker falls down, the DNS Server will keep redirecting the web requests to it, once it does not know whether the server is active or not.

Take a look below on how the architecture is structured:



Setting up the architecture:

1. Set up each one of the existing Connection Servers
2. Set up each one of the existing Connection Brokers
3. Make sure all the Connection Servers IP's are public to the Web Browsers that will access ThinRDP.
4. Set the Profiles "Database Path" of all Brokers to the same database file. On the bottom of

the Access Profiles tab, there is a field called "Database Path".

5. Configure on each Connection Broker all the settings (General, Security, Access Profiles[1], Folders, Permissions and License)[2].

6. Configure your DNS Server, associating the domain name with all the existing Connection Brokers IP's.

3. Make sure all the Connection Servers and all the Connection Broker IP's are public to the Web Browsers that will access ThinRDP.

Important observations:

[1]. On the step 5, the Access Profiles settings have to be done only in one of the existing brokers. The other Connection Brokers should be pointing to the same database file, so that once the profiles are configured in one of them, they will work evenly.

[2]. It is recommended that all Connection Brokers have the same "Authentication Method", " Temporary and Shared Folders Settings". That way, the different Brokers will set the connections the same way and keep all the Folders data centralized.

10.4.2 Setting up a Connection Server

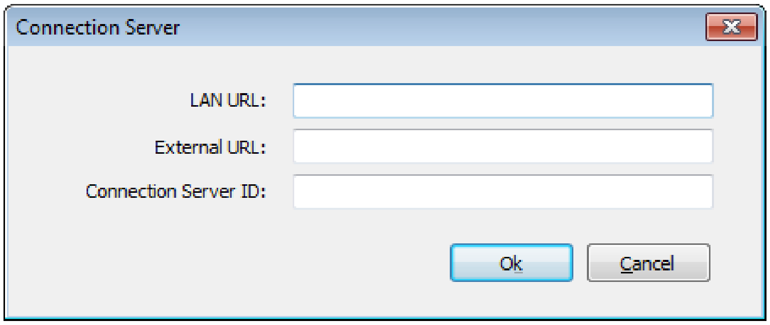
In order to set up a Connection Server to work with the Load Balancing Architectures (ThinRDP Load Balancer and Combined Architecture), you should follow the next steps:

1. Install ThinRDP on the target machine.
2. On the ThinRDP Manager General Tab, check the option "Enable Load Balancing".
3. The Load Balancing tab will be activated. Open this tab.
4. Select the option "Connection Server".
5. You can generate a new ID, by clicking on the Refresh button.
6. Keep the "Connection Server ID" information to be registered on the Connection Broker.

10.4.3 Setting up a Connection Broker

To set up a ThinRDP Broker for the Load Balancing Architectures (ThinRDP Load Balancer or Combined Architecture), you may follow the steps below:

1. Install ThinRDP on the target machine.
2. Open the ThinRDP Manager and on the General Tab, check the option "Enable Load Balancing".
3. The Load Balancing tab will be activated. Open this tab.
4. Select the option "Connection Broker".
5. Click on the "Add" button to register a Connection Server that has been already installed and configured. The dialog below will be presented.



LAN URL	Inform the URL to access the Connection Server from the Local Network.
External URL	Inform the URL to access the Connection Server from the outside the LAN (internet).
Connection Server ID	Inform the Connection Server ID generated while configuring the Connection Server.

6. Repeat the step 5, for all existing Connection Servers.
7. Configure all the other settings (General, Security, Access Profiles[1], Folders, Permissions and License) [2].
8. Press Apply.

Important observations:

[1]. If you will have more than one Broker on your environment (Combined Architecture), you will have to repeat all the steps above. However on step 7, it will not be necessary to configure all the Access Profiles again. From the second Broker on, you will only have to set the Profile Database to same path where the first Broker database is.
On the bottom of the Access Profiles tab, there is a field called "Database Path". All Brokers must have this field pointing to the same path, so that they can share the profiles while distributing connections .

[2]. It is recommended that if there is more that one Broker (Combined Architecture), they all have the same "Authentication Method", Temporary and Shared Folders Settings and Connection Server list. That way, the different brokers will establish connection evenly and keep all the Folders data centralized.

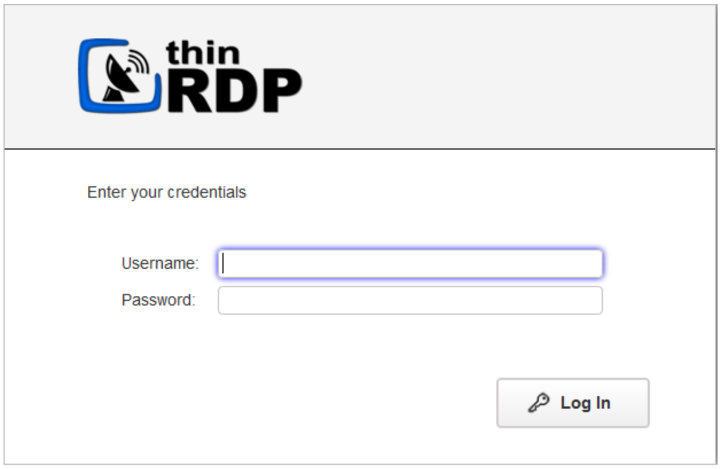
11 User's guide

This section was designed to be a quick User's Guide and it is focused on the everyday use of ThinRDP.

11.1 Logging In

1. Open your preferred web browser.

2. Type into the address bar http(s)://thinRDP_server: thinRDP_port/ .



Enter your credentials

Username:

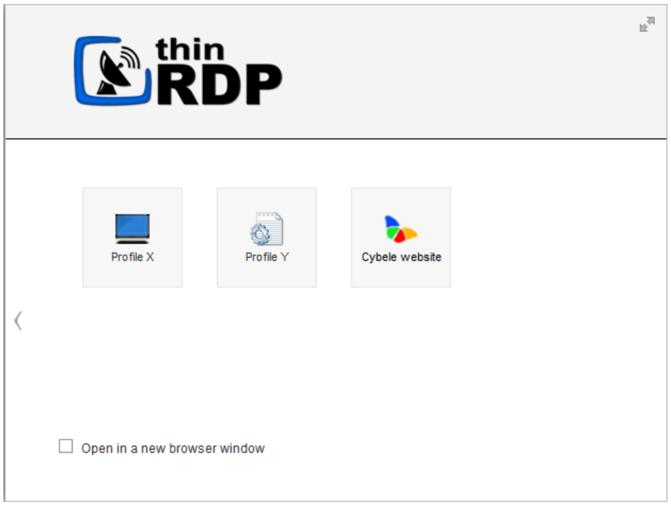
Password:

3. Enter your credentials (username and password) provided by the system administrator.

4. Press the "Log in" button.

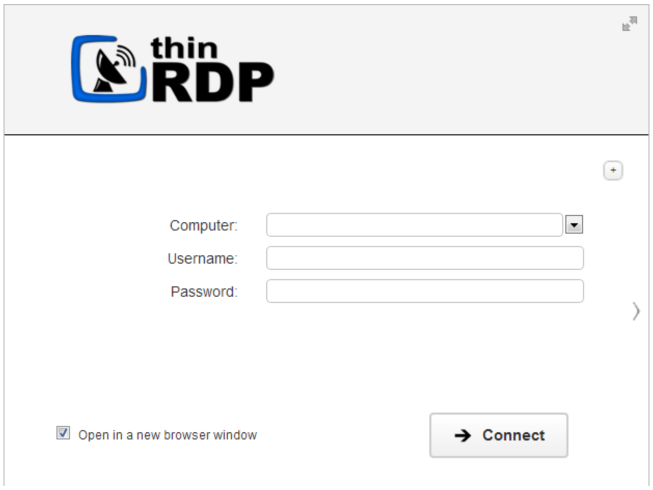
11.2 Connecting

If the application is configured to work only with pre determined profiles, you will be directed to the screen below. In this case, read the Connection through profiles topic to continue.



□ Open in a new browser window

Otherwise if you get to the screen below, read the Connection through open parameters topic, to continue with the reading.



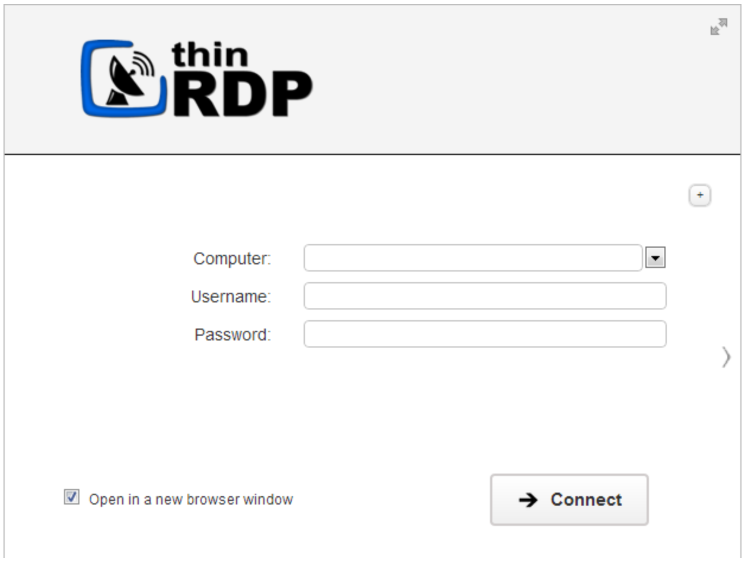
Computer:
Username:
Password:

☑ Open in a new browser window

Click on the two arrows on the right top corner to have the screen maximized.

11.2.1 Connecting with open parameters

The open parameters allow you to configure most of the settings right before connecting to the remote machine. If you have permission to set these parameters you will be presented with the screen below right after getting into the application.



1. Enter the remote desktop IP you want to connect to.

2. Enter the username and password to the remote machine (these fields are optional).

3. If you want to modify the RDP settings before connecting, press the options button (plus (+) sign on the right upper corner) and you will have the settings tabs below available to configure them:

The General tab
The Display tab
The Resources tab
The Program tab
The Experience tab
The Advanced tab

These settings are stored per browser, enhancing the user experience.

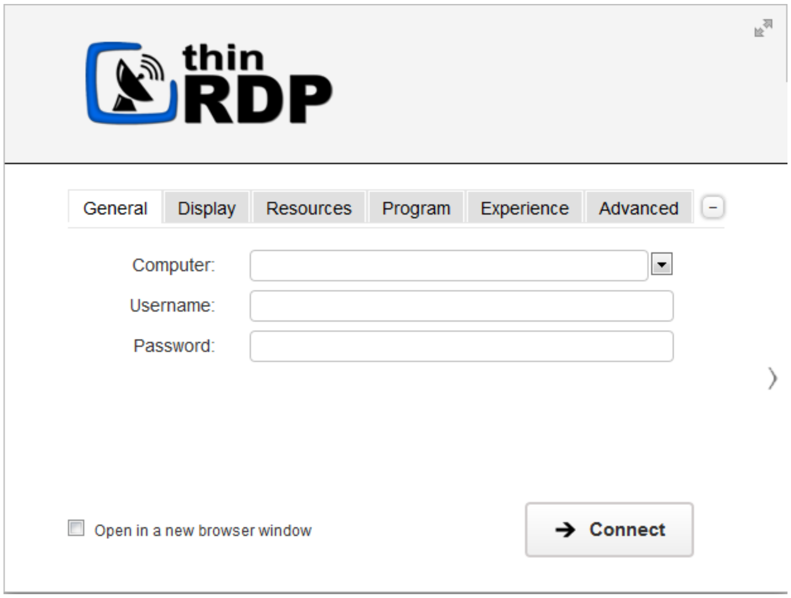
4. Check the "Open in a new browser window" option if you want the connection to be placed on another browser tab.

5. Press Connect.

6. At this moment you are already connected remotely to the desktop. You should be seeing it on your browser as if you were in front of the computer.

If you want to connect using the Profiles, click on the gray middle right arrow .

11.2.1.1 General



Computer:

Username:

Password:

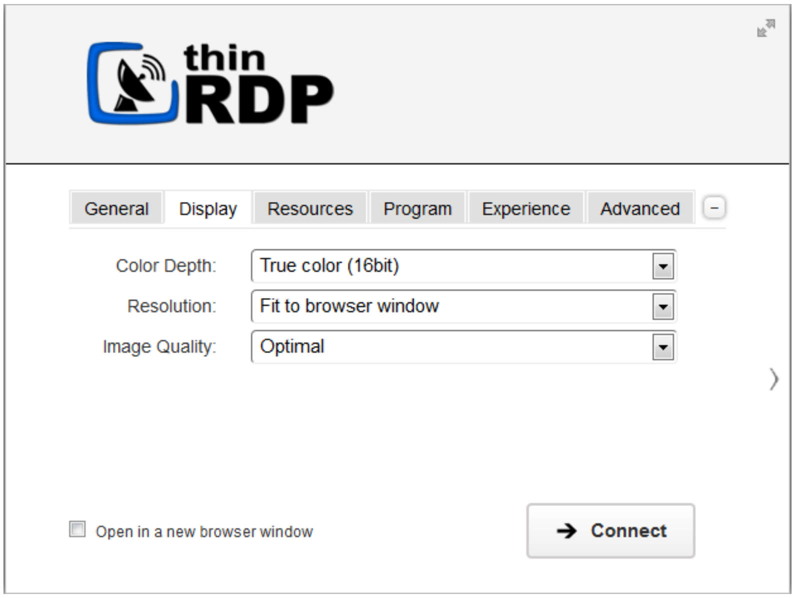
□ Open in a new browser window

The web interface "General" tab presents you with these following options:

Computer	Enter the computer's IP or name.
User Name	Enter the user name to authenticate against the remote computer. You will need to enter the password afterwards, but the browser can store the user name for the next time you connect.
Password	Enter the password to authenticate against the remote computer.

If you are looking for the Access Profiles General tab, check out the **this section**.

11.2.1.2 Display



Color Depth: True color (16bit)

Resolution: Fit to browser window

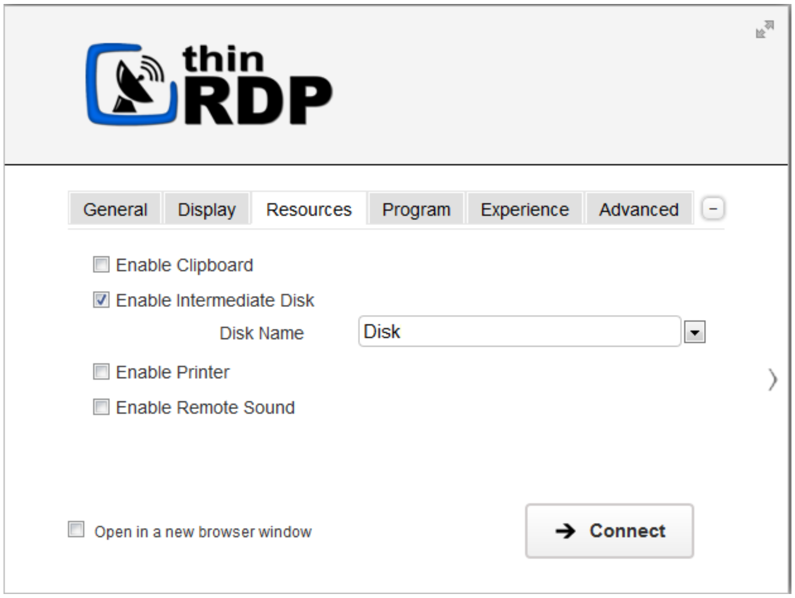
Image Quality: Optimal

□ Open in a new browser window

The web interface "Display" tab presents you with these following options:

Color Depth	Choose the color depth for the remote computer view.
Resolution	Choose from the available list of resolutions including "Fit to browser window" and "Fit to screen", ideal for hiding the browser and working on a full screen mode.
Image Quality	The connection image quality is a lot related with the application performance (higher quality=lower performance). The default Image quality is Optimal, because it presents the best cost benefit between quality and performance cost. If you need to have more quality or better performance, take a look on the other options below: Highest - Works only with PNG images and has no compression (0% compression) Optimal - Combines PNG and JPEG images (20% compression). Good - Works only with JPEG images (40% compression) Faster - Works only with JPEG images (50% compression).

11.2.1.3 Resources



□ Enable Clipboard

☑ Enable Intermediate Disk

Disk Name: Disk

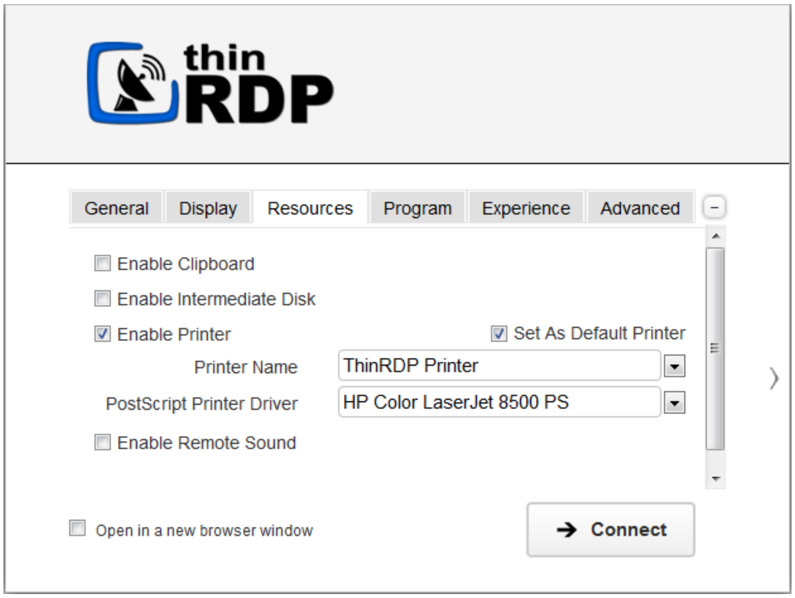
□ Enable Printer

□ Enable Remote Sound

□ Open in a new browser window

In the web interface "Resources" tab you will find these following options:

Enable Clipboard	Mark this option to enable the clipboard on the remote connection.
Enable Intermediate Disk	Check this option to have an intermediate disk available on the connections created through this profile.
Disk name	This is the name to identify the intermediate disk among the other remote desktop disks.



☐ Enable Clipboard

☐ Enable Intermediate Disk

☑ Enable Printer ☑ Set As Default Printer

Printer Name: ThinRDP Printer

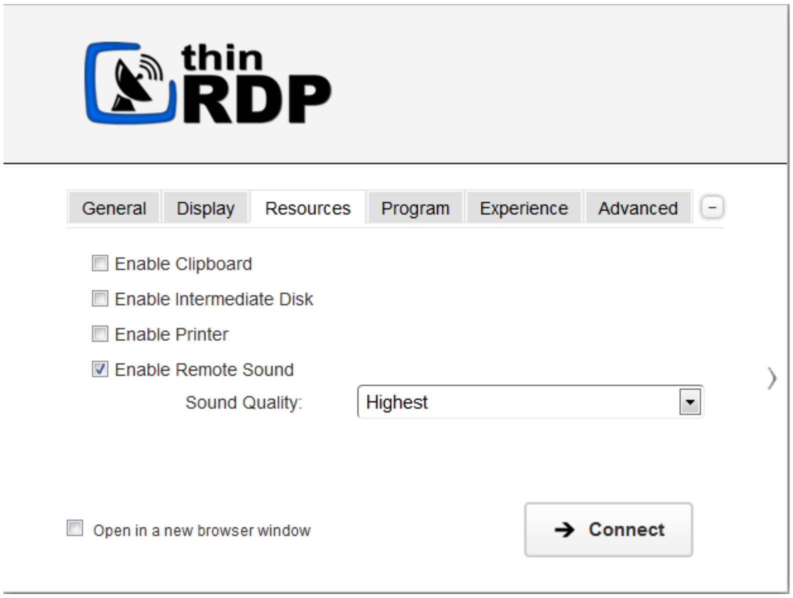
PostScript Printer Driver: HP Color LaserJet 8500 PS

☐ Enable Remote Sound

☐ Open in a new browser window

When you check the "Enable Printer" option, the interface will be seen as the image above. Learn below how each printer option works.

Enable a Remote Printer	Uncheck this option to disable ThinRDP PDF printer.
Printer name	Specify the printer name that you want to be shown on the remote machine's printer list.
PostScript printer driver	This is the driver to be used by ThinRDP in order to print the remote documents. The "*HP Color Laser Jet 2800 Series PS*" driver is compatible with 2008 Windows versions. The "*HP Color LaserJet 8500 PS*" driver is compatible with 2003 Windows versions. The "*Microsoft XPS Document Writer V4*" driver is compatible with Windows Server 2012 and Windows 8. Despite the fact this field is a drop-down menu, you can still type in any other driver that is not listed on the menu. So, if you are not using 2003 or 2008 Windows versions, look for a driver that is already installed on the OS and inform this driver name in this field.
Set as default printer	Mark this option to make ThinRDP printer the remote machine default printer.



□ Enable Clipboard
□ Enable Intermediate Disk
□ Enable Printer
☑ Enable Remote Sound
Sound Quality: Highest

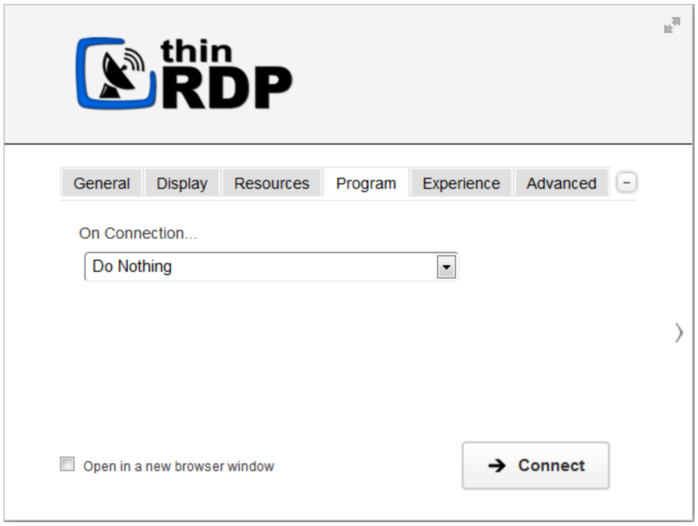
□ Open in a new browser window

When you mark the "Enable Remote Sound" option, the interface will be seen as the image above. Learn below how each sound option works.

Enable Sound	Check this option to enable the remote sound to be reproduced within the browser. The remote sound only works with Firefox and Chrome web browsers.
Sound quality	Determines what quality ThinRDP will use to reproduce the remote sound. The highest quality, the most resources will be required.

11.2.1.4 Program

This tab allows users to configure the connection to open a specific application. By default ThinRDP comes with the "Do nothing" option marked. This option will show the whole remote desktop.



On Connection...

Do Nothing

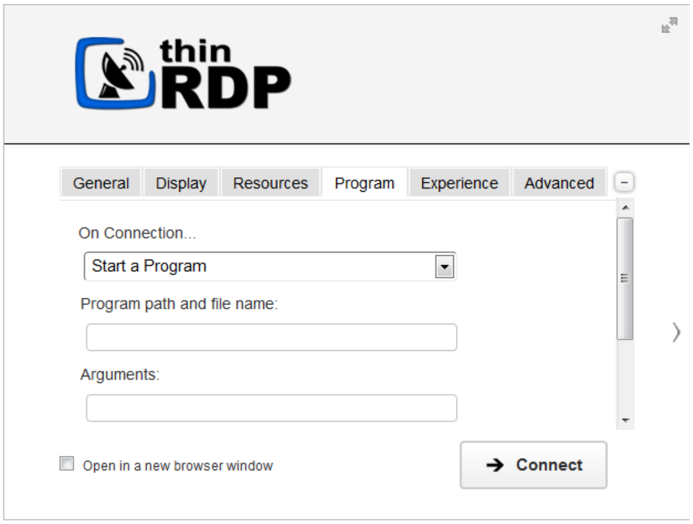
□ Open in a new browser window

Start a Program:

If you want to set a specific application to start with the connection. Select the "Start a Program" option.

This feature is only available within Windows Server versions.

Once you close the program, the remote session will get disconnected.



On Connection...

Start a Program

Program path and file name:

Arguments:

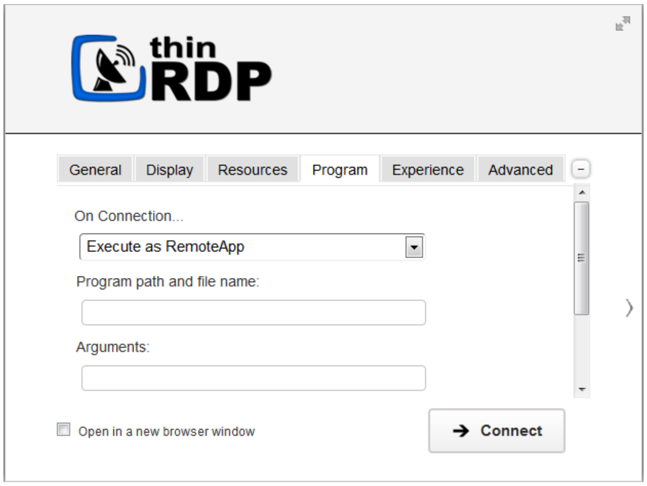
□ Open in a new browser window

When the "Start a Program" option is selected, you will be presented with the following options:

Program path and file name	Specify the complete path to give access the application you want to start with the connection. Right after the path you should also inform the application arguments, if they exist.
Arguments	Applications arguments.
Start in the following folder	Inform a context directory for the program set on the field "Program path and file name"

Execute as RemoteApp:

The RemoteApp is a Terminal Services feature that allows Windows®-based application publishing. You can connect to an application using RemoteApp through ThinRDP, by selecting the "Execute as RemoteApp" on the Program tab.



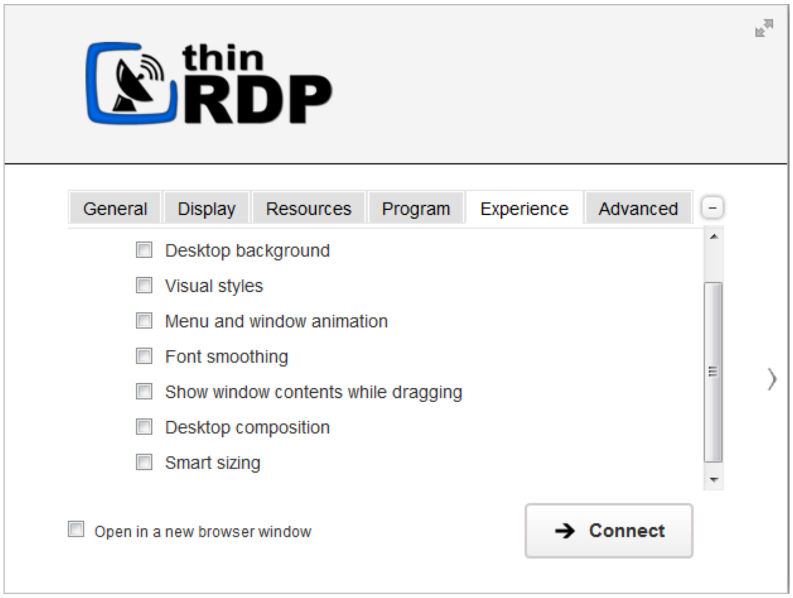
On Connection...

Execute as RemoteApp

When the "Execute as RemoteApp" option is selected, you will be presented with the following options:

Program path and file name	Application published name or the direct path to the application file.
Arguments	Applications arguments.
Start in the following folder	Specify a context directory for the program set on the field "Program or file"

11.2.1.5 Experience



□ Desktop background
□ Visual styles
□ Menu and window animation
□ Font smoothing
□ Show window contents while dragging
□ Desktop composition
□ Smart sizing

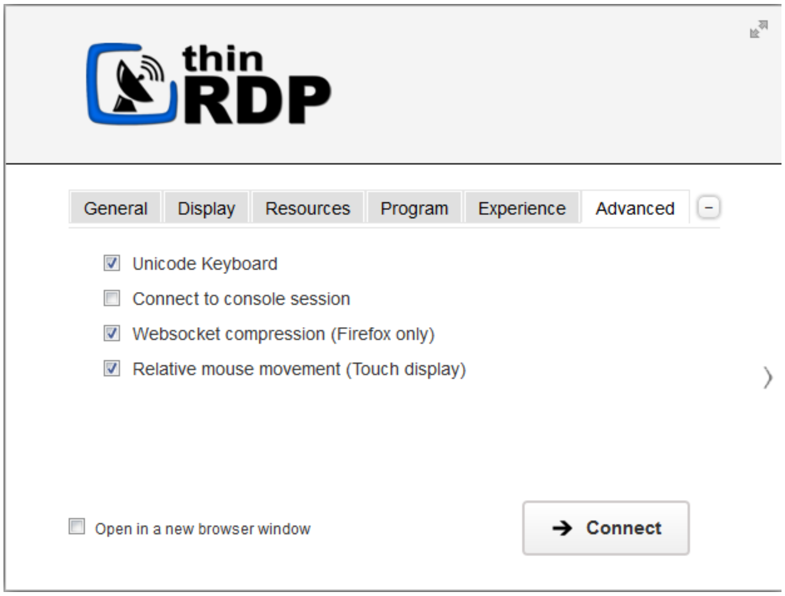
□ Open in a new browser window

The web interface "Experience" tab presents you with these following options:

Desktop Background	Check this option to show the desktop background.
Visual Styles	Check this option to show Windows Visual Styles: the appearence of common controls, colors, bordes, and themes.
Menu and Windows Animation	Check this option to show menu and windows animation when you scroll or expand a drop down menu.
Font Smoothing	Check this option to allow "Clear Type", a font smoothing option added to Windows Server 2008.
Show Window Content While Dragging	Check this option to show the contents of the window while being dragged. Otherwise a transparent border is dragged.
Desktop Composition	Check this option to configure the DWM to redirected the desktop drawing to off-screen surfaces in video memory. Also, the desktop will present many visual effects.
Smart sizing	By checking this option, you will have the connection image, scaled. The smart stands for a behaviour in which the maximum size of the connection will be the original desktop size.

All of these options enhance the look of the remote desktop and use more bandwidth.

11.2.1.6 Advanced



☑ Unicode Keyboard

□ Connect to console session

☑ Websocket compression (Firefox only)

☑ Relative mouse movement (Touch display)

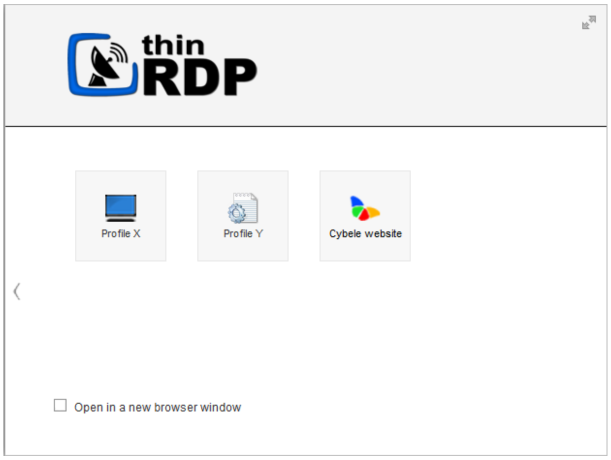
□ Open in a new browser window

The web interface "Advanced" tab presents you with these following options:

Unicode Keyboard	Uncheck this option to connect to Unix computers through xRDP.
Connect to console session	Check this option to connect to the console session. This require confirmation from the logged on user and log out the current session.
Websocket compression	Check this option to enable the compression for the exchanged Websocket data and have the application performance improved.
Relative mouse movement	The relative mouse movement is a mouse behaviour encountered in touch screen mobile devices, in which the screen cursor moves relatively to the touch. Uncheck this option to have a mouse behaviour similar to the real desktop mouse in which the cursor will be always positioned under the touch.

11.2.2 Connecting with Profiles

An Access Profile is a easiest and faster way to establish a connection or connect to a weblink.
An RDP profile will have all the connection settings already set by system administrator.
Each user will have as many profiles as the System Administrator has assigned to his/her user profile.
The Profiles page looks like the image bellow:



1. Check the option "Open in a new browser window" if you want the connection to be placed on a new browser tab.

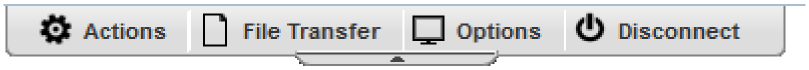
2. Click on the profile you want to connect through.

3. At this moment you are already connected remotely to the desktop or have been redirected to the website that profile points to.

11.3 Toolbar

Once a connection is established you will see on the top of the screen a small arrow, that will give you access to the connection toolbar.

Click on the connection middle top arrow, and the toolbar below will appear. If you want this toolbar to start expanded, ask the system administrator to configure it on the Permissions tab.



Actions menu

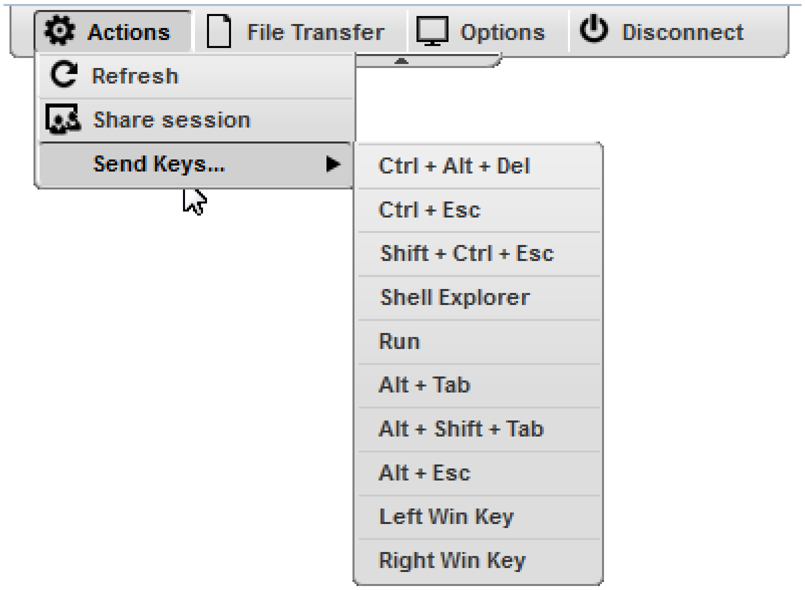
File Transfer menu

Options menu

Disconnect menu

11.3.1 Actions

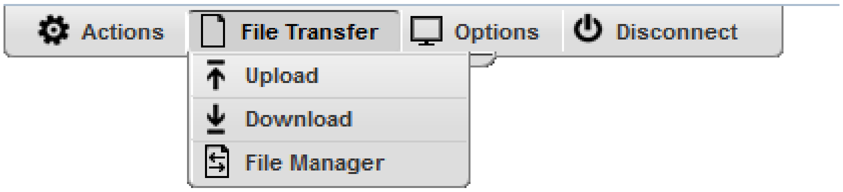
Click on the "Actions" button and its menu will open:



Refresh	The Refresh button performs a reconnection with the server, using the same parameters as the current connection, except for the screen size values, that will be updated to the current screen size (only if scale is on).
Share session	The Share session feature, allows you to share the current desktop connection with someone else. Click on the button and you will be presented with an URL and a password that should be sent to the user who you want to share the desktop with.
Send Keys	On this option you will be able to send determined keys combinations to the server. The keys will be shown as soon as you click on this option.

11.3.2 File Transfer

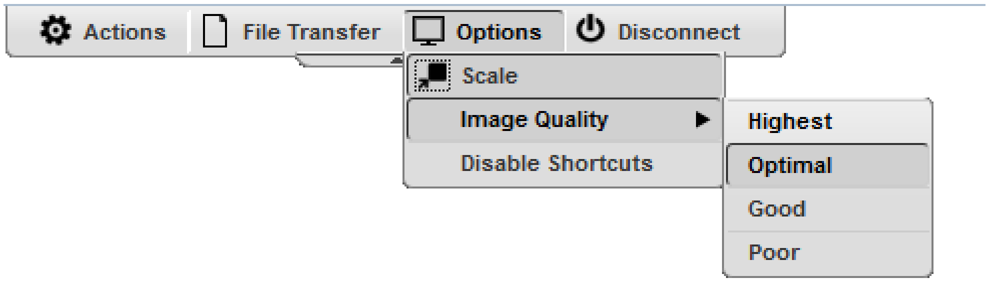
Click on the "File Transfer" button and its menu will open:



Upload	This option allows you to upload a file located on the local computer into the remote desktop.
Download	This option enables you to download any file located inside the Intermediate disk.
File Transfer	This option will open the File Transfer Manager. If the button is not available ask the system administrator to set you the permissions for it.

11.3.3 Options

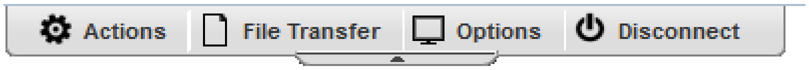
Click on the "Options" button and its menu will open:



Scale	By setting this option, you will have the connection image scaled. The original desktop size will be the maximum limit size applied to the connection.

Image Quality	The connection image quality is a lot related with the application performance (higher quality=lower performance). The default Image quality is Optimal, because it presents the best cost benefit between quality and performance cost. If you need to have more quality or better performance, take a look on the other options below: Highest - Works only with PNG images and has no compression (0% compression) Optimal - Combines PNG and JPEG images (20% compression). Good - Works only with JPEG images (40% compression) Faster - Works only with JPEG images (50% compression).
Disable shortcuts	When you mark this option, ThinRDP will stop interpreting keyboard shortcuts. All the shortcut combinations will be redirected to the remote desktop exactly as they where typed in.

11.3.4 Disconnect



The disconnect button will close the connection with the remote desktop.

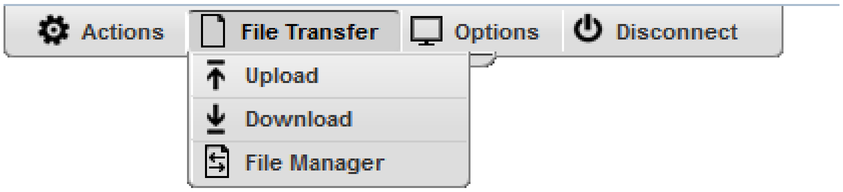
11.4 Features

11.4.1 File Transfer

Once a connection is established you have the possibility to perform File Transfers operations between the remote machine and the local computer:

1. Click on the connection middle top arrow, and the toolbar will be presented.

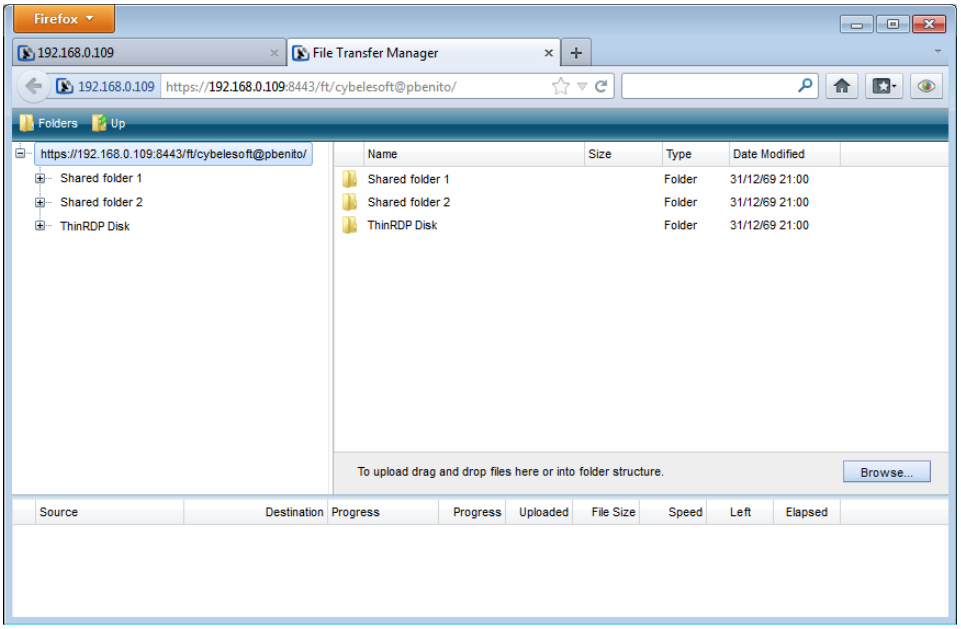
2. Click on the "File Manager" option, located inside the File Transfer toolbar option. If the button is not available ask the system administrator to set you the permissions for it.



Upload	Click on this option to upload a file located on the local computer into the remote desktop. A window will be opened so that you can select the file to be uploaded.
Download	This option enables you to download any file located inside the Intermediate disk. Select the file on the presented list and press the "Download" button.
File Transfer	This option will give you access to the File Transfer Manager.

See also, the option to Download automatically any newly-added file.

3. This is the screen where you can manage files and also transfer them.



- https://192.168.0.109:8443/ft/cybelesoft@pbenito/
  - Shared folder 1
  - Shared folder 2
  - ThinRDP Disk

Name	Size	Type	Date Modified
Shared folder 1		Folder	31/12/69 21:00
Shared folder 2		Folder	31/12/69 21:00
ThinRDP Disk		Folder	31/12/69 21:00

To upload drag and drop files here or into folder structure.

4. Observe that the "Shared Folders" and the "Intermediate disk" are the only remote directories available to exchange files with. If you need to download or upload remote files from the file manager, you should always move them first into these directories (they are going to be mapped drives also), and after that transfer to the desired location.

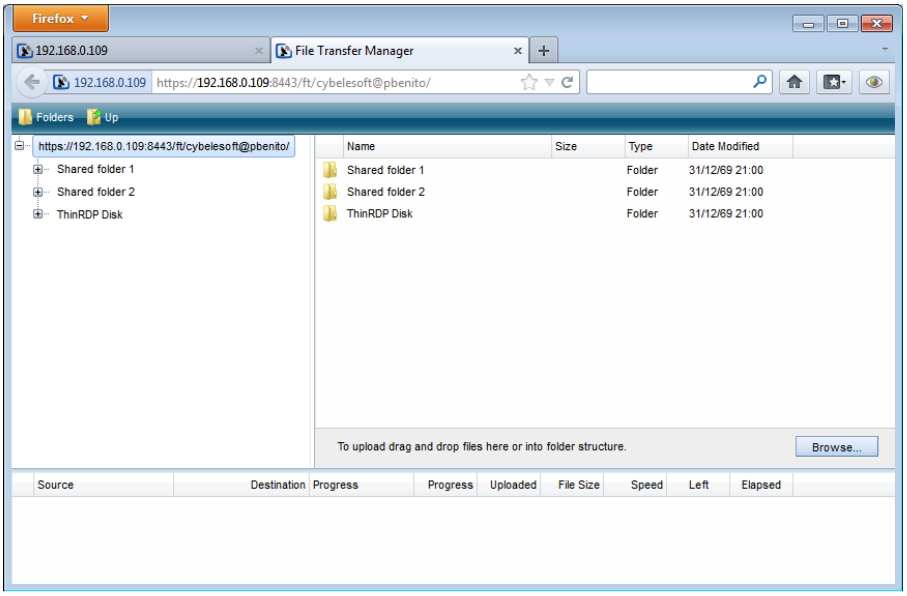
5. Read also, the following sections:

Navigating on the File Transfer Screen
File Options
Folder Area Options

11.4.1.1 Navigating

On the upper part of the screen you will see your remote files and folders. Browse to the remote location by double clicking on the folders on the right, or expanding the tree structure on the left.

In order to upload files, drag them from your local PC and paste them into the remote view area, or press the 'Browse' button.
The lower part of the screen shows the status of the files to be transferred.


Firefox
192.168.0.109
File Transfer Manager
192.168.0.109 https://192.168.0.109:8443/ft/cybelesoft@pbenito/
Folders
Up
https://192.168.0.109:8443/ft/cybelesoft@pbenito/
Shared folder 1
Shared folder 2
ThinRDP Disk
Browse...

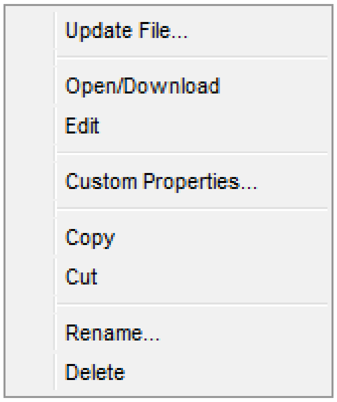
Name	Size	Type	Date Modified
Shared folder 1		Folder	31/12/69 21:00
Shared folder 2		Folder	31/12/69 21:00
ThinRDP Disk		Folder	31/12/69 21:00

To upload drag and drop files here or into folder structure.

Source	Destination	Progress	Progress	Uploaded	File Size	Speed	Left	Elapsed

11.4.1.2 File Options

Right click on a remote file to access these options:



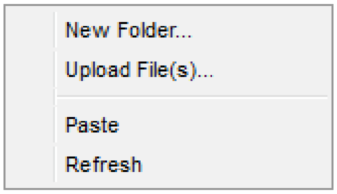
Find the behaviour for each one of these options below:

Update File	Choose this option to replace the selected remote file with a local file.

Open/Download	Choose this option to open or download the selected file.
Custom Properties	Choose this option to see the remote file's properties.
Copy	Choose this option to copy the file into the remote clipboard. You can paste it into another remote folder.
Cut	Choose this option to cut the file into the remote clipboard. You can paste it into another remote folder.
Rename	Choose this option to change the name for the remote file.
Delete	Choose this option to delete the selected file.

11.4.1.3 Remote Folder Area Options

Right click on the blank remote folder area any time to access the following options:



Find the behaviour for each one of these options below:

New Folder	Choose this option to create a new folder in the remote location.
Upload File(s)	Choose this option to upload one or more files to the remote location.
Paste	Choose this option to paste a remote file that is in the clipboard into the remote location. It will be enabled only after you have copied a file into the clipboard.
Refresh	Choose this option to refresh the view of the remote folder.

11.4.1.4 Downloading and Uploading files

1. Downloading remote files:

1. Connect to the remote machine.
2. Open the remote machine Windows Explorer and copy the remote files to be downloaded into a "Shared Folder" or an "Intermediate Disk".
3. Open the "File Transfer" Manager from the upper connection toolbar.
4. Download the remote file to any local directory of your preference.

See also, the option to Download automatically any newly-added file.

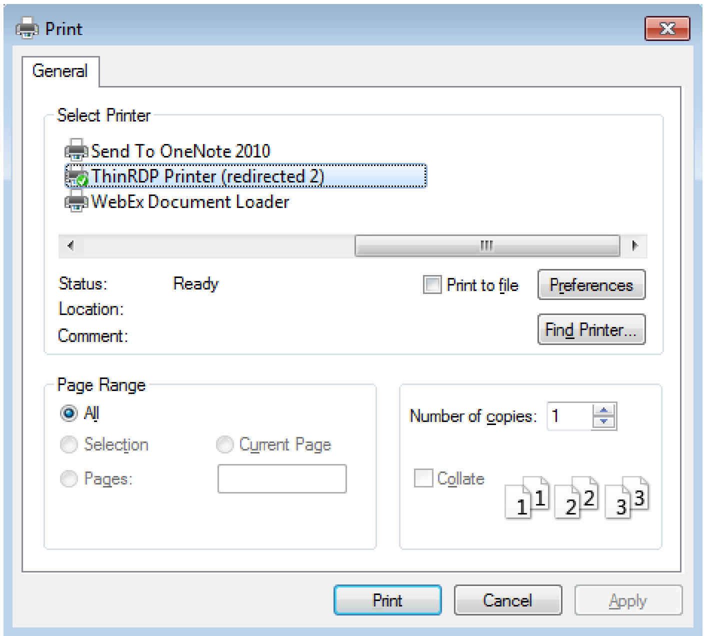
2. Uploading local files:

1. Connect to the remote machine.
2. Open the "File Transfer" Manager from the upper connection toolbar.
3. Upload the file you want to transfer to the remote machine into a "Shared Folder" or an "Intermediate Disk".
4. Go back to the connection screen and open the remote machine Windows Explorer.
5. Copy the file from the "Shared Folder" or "Intermediate Disk" drive into the remote directory of your preference.

11.4.2 Remote Printer

The ThinRDP Remote Printer allows you to print any remote document locally. If the Remote Printer is enabled to a connection, every time you print a document, the ThinRDP Printer will be shown among the list of available printers.

1. Open a remote document and try to print it.



Select Printer

- Send To OneNote 2010
- ThinRDP Printer (redirected 2)
- WebEx Document Loader

Status: Ready

Location:

Comment:

□ Print to file

Page Range

● All

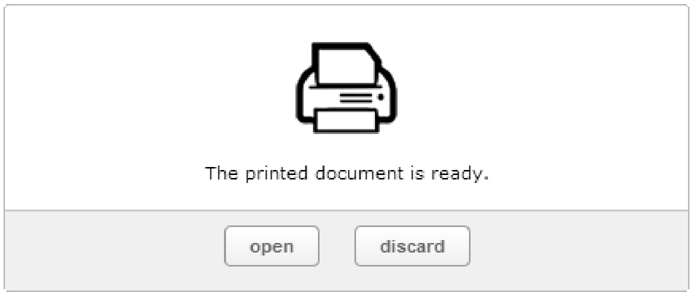
○ Selection ○ Current Page

○ Pages:

Number of copies: 1

□ Collate

2. Select ThinRDP printer and press "Print".
3. A message will be presented to let you know that the document is ready to be printed.



The printed document is ready.

a. Click on "open" and the document will be open on a new browser tab in a PDF format. From there you can print it as you may print any other PDF document.

b. Click on "discard" if you want to cancel the printing.

11.4.3 Remote Sound

With ThinRDP you can listen to the sound that is playing on the remote machine.
Try playing any sound on an open connection and check out if you can listen to it locally.

If you are having problems playing the remote sound locally, verify if some of the following conditions are taking place:

1. The remote sound is not enabled for your connection. If you are using profiles ask to the system administrator to enable it. If not, learn how to enable it on Resources tab topic.

2. You are using a non supported browser for remote sound. The only supported browsers so far are Firefox and Google Chrome.

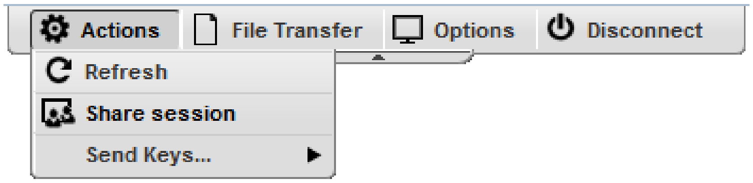
3. The speakers of your local machine are not connected or do not work correctly at the moment.

11.4.4 Share Session

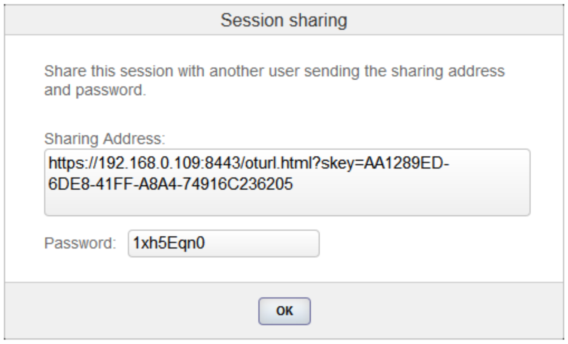
The "Share Session" feature allows users to share an active desktop connection with other users, so that they can see and interact with it in many ways.
The shared session will present the remote user exactly what is being shown on the local connection. It replicates the remote desktop image on the remote user browser and is updated continuously.
Follow the next steps and learn how to share your desktop connection with other users:

1. Open the desktop connection you want to share.

2. On the connection toolbar click on the Actions button and then on the "Share Session". If the button is not available ask the system administrator to set you the permissions for it.



3. A dialog will present you with the Sharing Address and password that should be used to access this same connection remotely.


Session sharing

Share this session with another user sending the sharing address and password.

Sharing Address:
https://192.168.0.109:8443/oturl.html?skey=AA1289ED-6DE8-41FF-A8A4-74916C236205

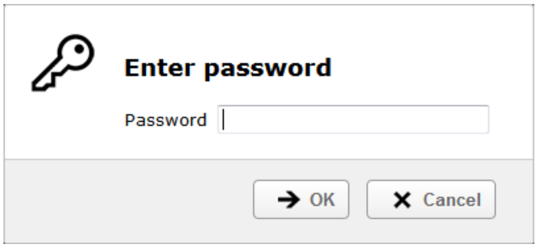
Password: 1xh5Eqn0

4. The connection is now available to be accessed remotely. Send the URL and password information to the person you want to share the connection with.

Access the shared connection remotely:

1. Open your preferred browser from any computer/location of your preference and paste the sharing address (URL).

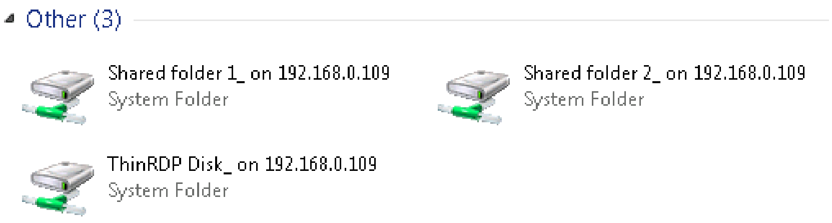
2. The password will be required. Type it in the dialog that you be presented and press the OK button



3. You should now be able to see and interact with the previously shared connection.

11.4.5 Mapped drives

In order to exchange files with the remote machine, ThinRDP maps disk drives on the connection, so that users can manipulate their files remotely and exchange them with the local machine.
You can find the mapped drives on the connection's Windows Explorer.



Other (3)

Shared folder 1_ on 192.168.0.109
System Folder

Shared folder 2_ on 192.168.0.109
System Folder

ThinRDP Disk_ on 192.168.0.109
System Folder

ThinRDP maps two kinds of directories:

Intermediate disks

The intermediate disks are directories created by ThinRDP and they are user exclusive, which means that the files saved on this directory won't be accessible by other users.
If you are establishing connections through Profiles, you would have to ask to the system administrator what is the name of the profile intermediate disk. Otherwise, if you are configuring the connection settings yourself, you will be able to set your own drive name.
Be cautious: The files will be deleted right after you close the connection, if you log into ThinRDP as an "anonymous user".

Shared Folders

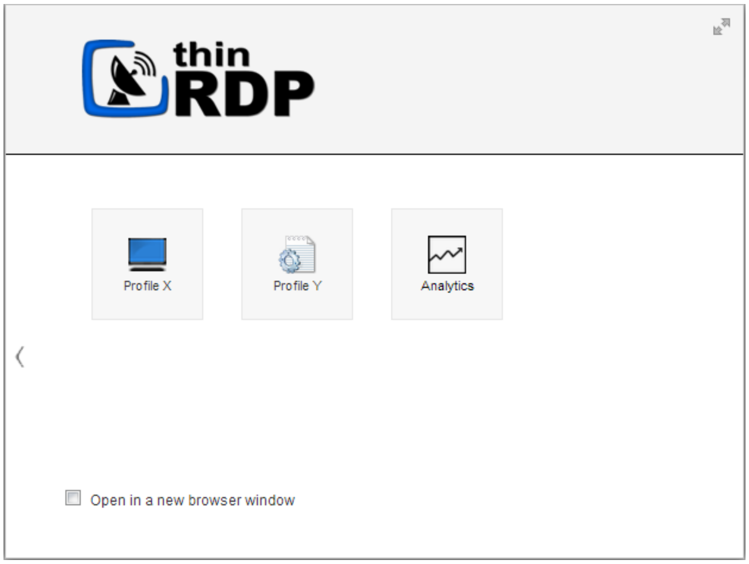
The Shared Folders are network directories accessible by all ThinRDP users and connections. Besides the file transfer utility, they are also useful to exchange files with other users.
The name of the Shared Folder drives are defined by the System Administrator. Find out what is the name of the Shared Folders, so that you can use them to manipulate your remote files, perform file transfers and exchange files with other users.

The "Intermediate disks" and "Shared Folders" will be the only remote locations available on the File Transfer Manager.
If you need to download or upload remote files you should always move them first into these directories (they are going to be mapped drives also), and after that transfer to the desired location.

11.4.6 Analytics

The analytics feature allows assigned users to view historical data regarding Logins, Sessions and Connections established within ThinRDP in a period of time. It also has the Browsers descriptions used to make this connections from. The users permissions to access the Analytics data should be assigned on the ThinRDP Manager Permissions tab.

If you have access to the Analytics feature, your Web profile page will have a "Analytics" button, like the one on the image below:

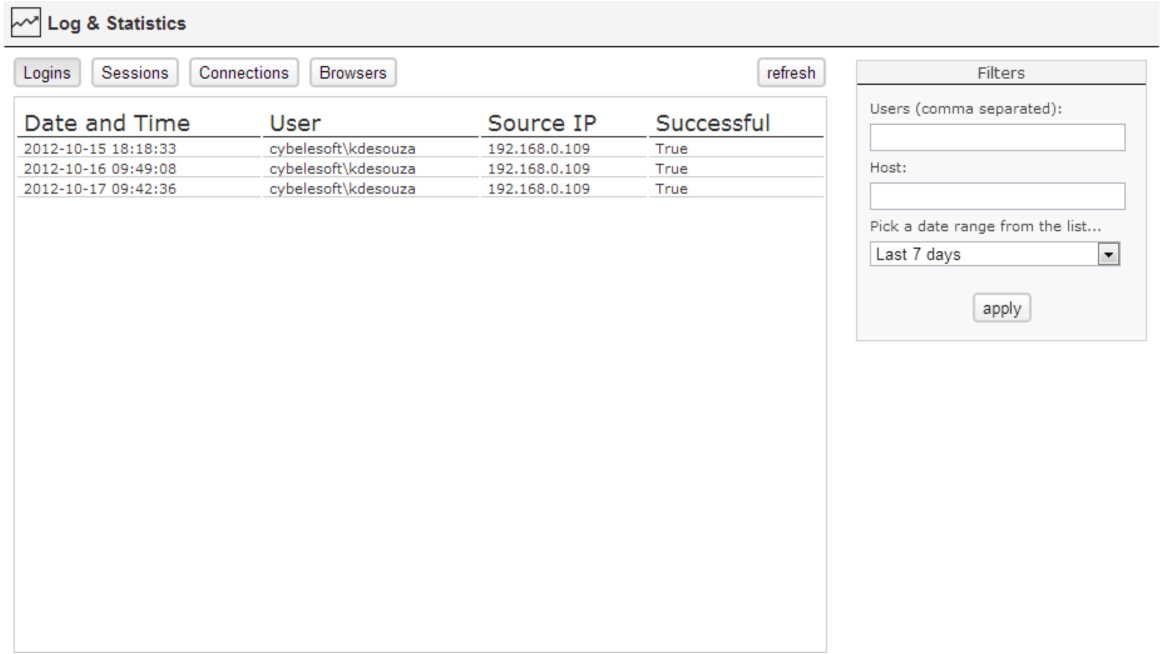


Click on the Analytics button to have the "Log & Statistics" window opened on a new window and find inside the "Log & Statistics" window the following tabs/options:

- Logins
- Sessions
- Connections
- Browsers
- Filter

11.4.6.1 Logins

The Logins View mode shows all the logins performed through the application within a determined period of time (default filter: Last hour).



Date and Time	User	Source IP	Successful
2012-10-15 18:18:33	cybelesoft\kdesouza	192.168.0.109	True
2012-10-16 09:49:08	cybelesoft\kdesouza	192.168.0.109	True
2012-10-17 09:42:36	cybelesoft\kdesouza	192.168.0.109	True

Users (comma separated):

Host:

Pick a date range from the list...

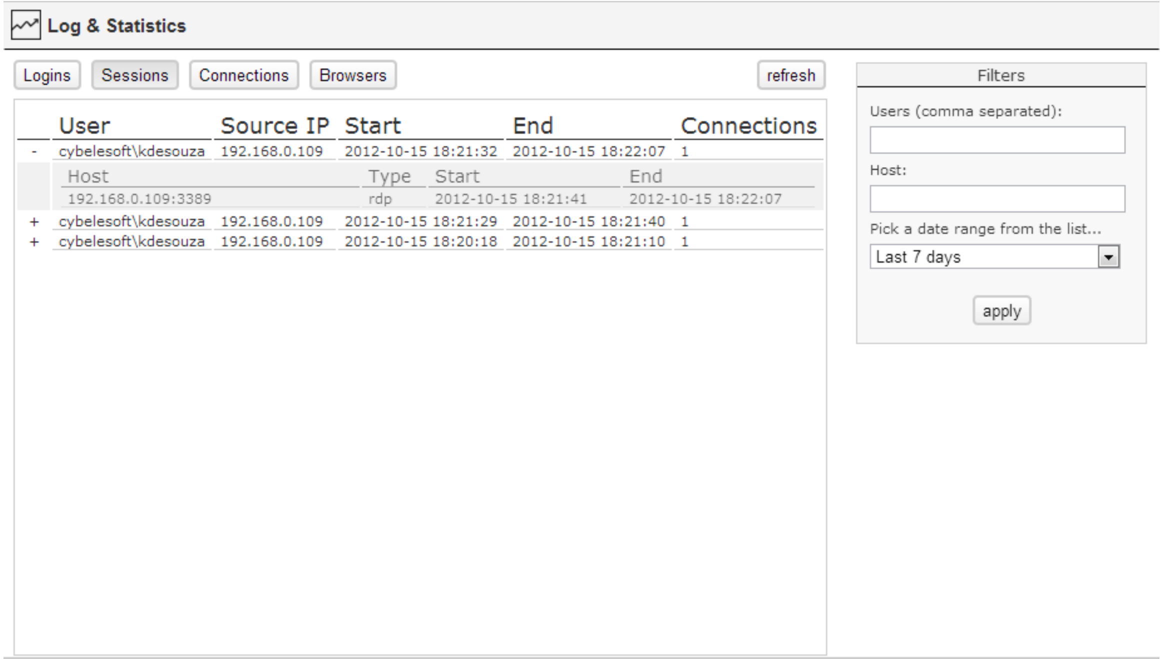
Last 7 days

This is the information shown on the Logins table:

Date and Time	Date and Time when the Login was performed.
User	User that logged in.
Source IP	IP Address from which the login was done.
Successful	Indicates whether the login was successful or failed

11.4.6.2 Sessions

The Session View mode shows all the sessions created through the application within a determined period of time (default filter: Last hour).



	User	Source IP	Start	End	Connections
-	cybelesoft\kdesouza	192.168.0.109	2012-10-15 18:21:32	2012-10-15 18:22:07	1
+	cybelesoft\kdesouza	192.168.0.109	2012-10-15 18:21:29	2012-10-15 18:21:40	1
+	cybelesoft\kdesouza	192.168.0.109	2012-10-15 18:20:18	2012-10-15 18:21:10	1

Host	Type	Start	End
192.168.0.109:3389	rdp	2012-10-15 18:21:41	2012-10-15 18:22:07

Users (comma separated):

Host:

Pick a date range from the list...

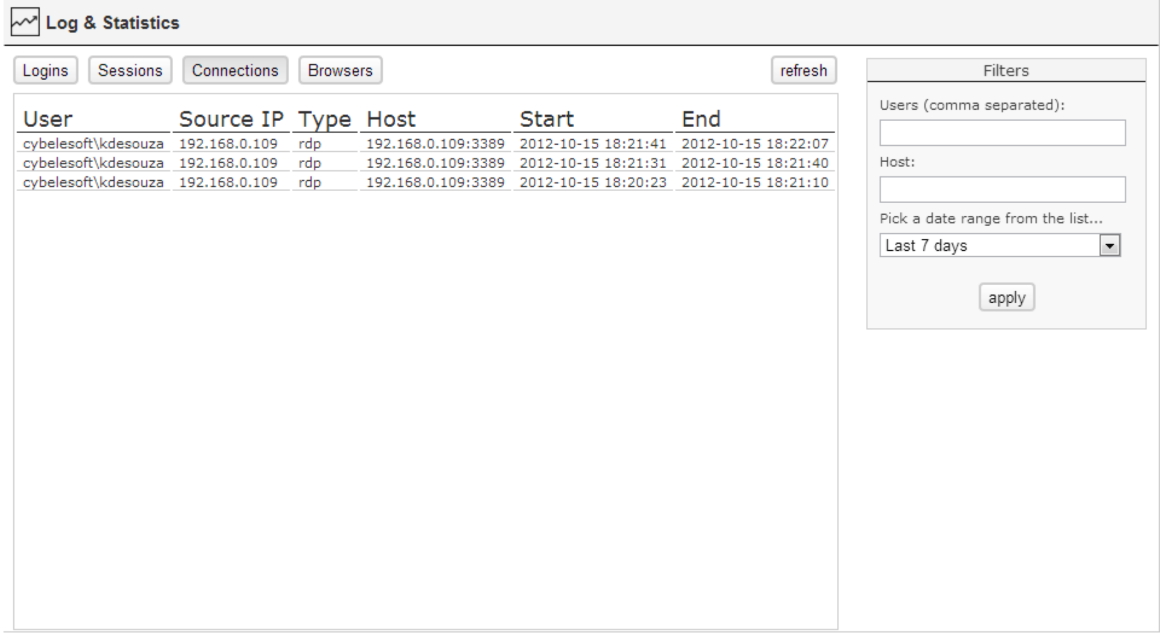
Last 7 days

This is the information shown on the Sessions table:

User	User that started the new session.
Source IP	IP Address from which the session was started.
Start	Date that the Session Ended.
End	Date that the Connection Started.
Connections	Counter of the Connections established within the Session.
(+)	By clicking on the plus (+) sign on the left side of each line, you will be able to see all the connections that were made within that session.

11.4.6.3 Connections

The Connection View mode shows all the connections established in a determined period of time (default filter: Last hour).



User	Source IP	Type	Host	Start	End
cybelesoft\kdesouza	192.168.0.109	rdp	192.168.0.109:3389	2012-10-15 18:21:41	2012-10-15 18:22:07
cybelesoft\kdesouza	192.168.0.109	rdp	192.168.0.109:3389	2012-10-15 18:21:31	2012-10-15 18:21:40
cybelesoft\kdesouza	192.168.0.109	rdp	192.168.0.109:3389	2012-10-15 18:20:23	2012-10-15 18:21:10

Users (comma separated):

Host:

Pick a date range from the list...

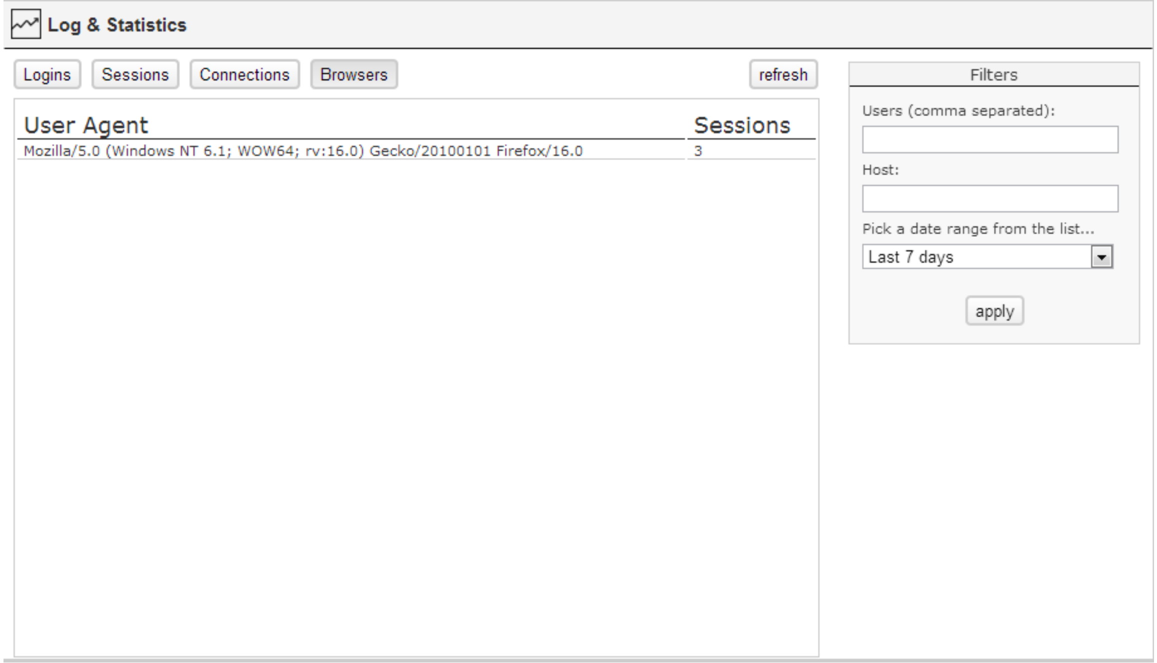
Last 7 days

This is the information shown on the Connections table:

User	User that established the Connection
Source IP	IP Address from which the Connection was established.
Type	Type of the Host
Host	Host (Name or Address) to which the Connection was established.
Start	Date the Connection Started
End	Date the Connection Ended

11.4.6.4 Browsers

The Browsers View mode shows all the kinds of browsers used to access ThinRDP.



User Agent	Sessions
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0	3

Users (comma separated):

Host:

Pick a date range from the list...

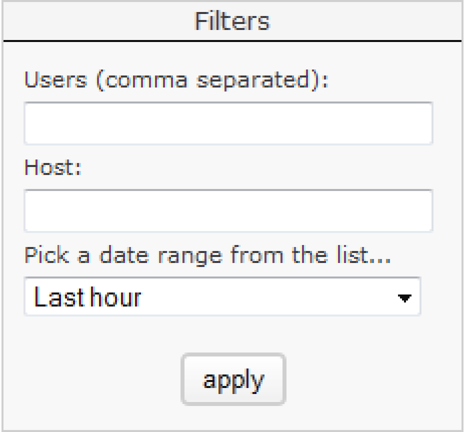
Last 7 days

This is the information shown on the browsers table:

User Agent	Browser User Agent.
Sessions	Counter of Sessions established within the Same Browser User Agent kind.

11.4.6.5 Filter

The Filters column allows you to filter the historical data of each one of the tabs. You can select the data filtering by Users, Host and a Date Range.



Users	Type in the usernames of the users you want filter, separated by commas.
Host	Type in a host name or IP Address.
Pick a date range from the list	Select one of the date range options, or select "Custom Range" to inform a custom period to filter the data.

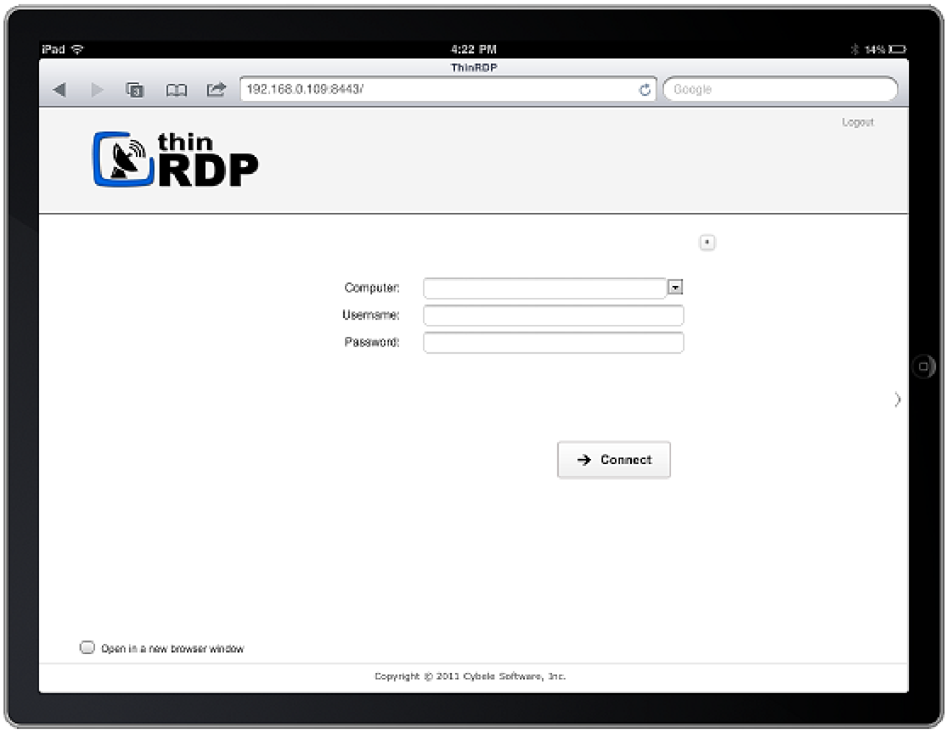
Always remember to press "apply" in order to have the records filtered by the selected parameters.

11.5 Acessing from Mobile devices

A great advantage you have using ThinRDP Server is the possibility to access remote desktops and applications from many different devices.

Any HTML5 compliant device can became a client of the application: iPhone, iPad, Android tablet, Chrome Book and many more.

Access the ThinRDP URL from a mobile or tablet and you will have a fully adapted interface to make the connection easier, as well as good performance and usability options specially designed for mobile devices.



Most of the mobiles and IPads are Touch Screen and it is through this screen touch you are going to control both remote desktop mouse and keyboard. Learn also about the available mobile Gestures.

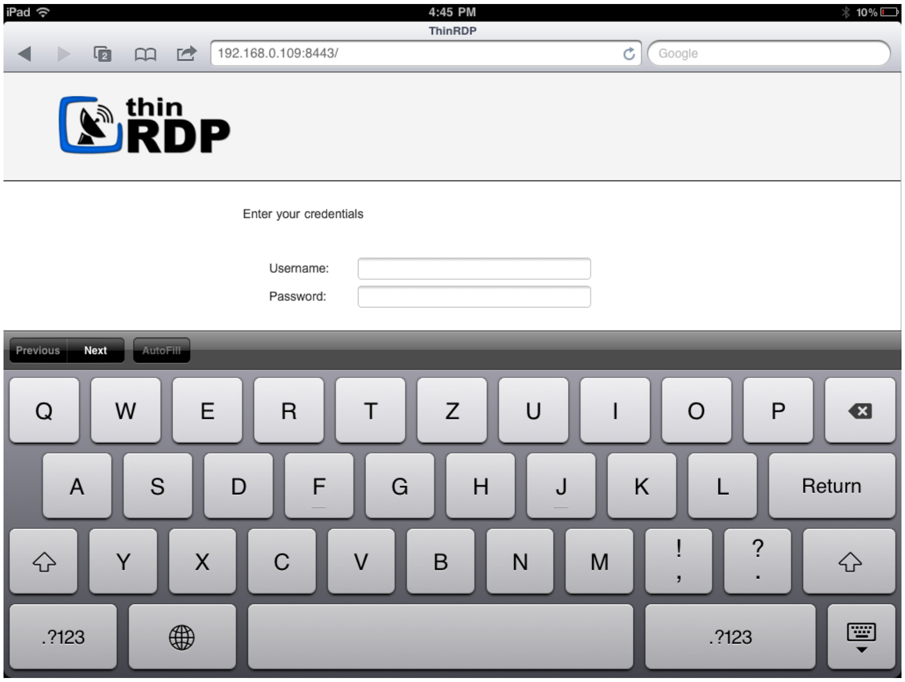
11.5.1 Getting into ThinRDP

When you access ThinRDP from a web browser, you will have two dialogs to fill. The first one is the application login and the second one has the connections settings you will be able to customize.

1. In order to navigate on both "Login" and "Settings" interfaces, the only thing you need to do is touch the control you want to select or enter. The "Login" and the "Settings" interfaces don't provide any kind of moving or dragging control, since there are no elements with these behavior.

2. The regular keyboard will get enabled every time you enter into a text field, so you can type in the connection information.

On the image below you can see the login interface along with the enabled keyboard.



Once you get connected with a desktop or an application, you will have many other navigability options and controls available.

Read the next topics and learn how to use these controls inside the connection.

Mouse Control

Keyboards

Gestures

Disconnecting

11.5.2 Mouse Control

Right after you get connected to a remote desktop or application you will have available the remote desktop mouse.
Take a look on the table below how you are going to control this mouse through a mobile screen.
The third column relates the mobile gesture that corresponds to the described mouse action.

Moving the mouse around	In order to move the remote desktop mouse you should drag your finger softly touching the mobile screen. You don't need to drag your finger exactly on the mouse draw position in order to make it move. Wherever the mouse is, it will start moving. Sometimes the mouse is hidden. In that case, keep dragging the finger towards different directions until you can see it on the screen.	-
Regular click	In order to click some element on the remote desktop you need to first position the mouse draw over this element (a icon, or a menu for example). Once you have position the mouse draw over the element, give a quick touch on the element.	Tap gesture
Double click	Just like on the regular click you need to first position the mouse draw over this element you want to double click. After that give two quick touches on the element.	Double-tap
Right click	When you open a connection through a mobile, ThinRDP provides a especial side menu. The second button is used exactly to right click an element of the remote desktop. As for the regular and double click, first of all you need to position the mouse over the element you want to right click. After that touch the second side menu button (the button has a mouse picture with the right button highlighted in red).	-
Drag and drop	To drag and drop elements of the remote desktop to the following: a. Touch the element you want to drag. Do not release your finger. b. Drag the finger towards the position you want to take the element to. c. When you get to the position you wanted, release the finger from the screen.	Press and drag

11.5.3 Keyboards

1. Regular Mobile Keyboard

Along with most mobile device comes a logical keyboard composed by the main used keys for mobile applications.
With ThinRDP you can use any kind of application located on a remote desktop and that is why ThinRDP has two additional keyboards with all the keys the device keyboard might not support.

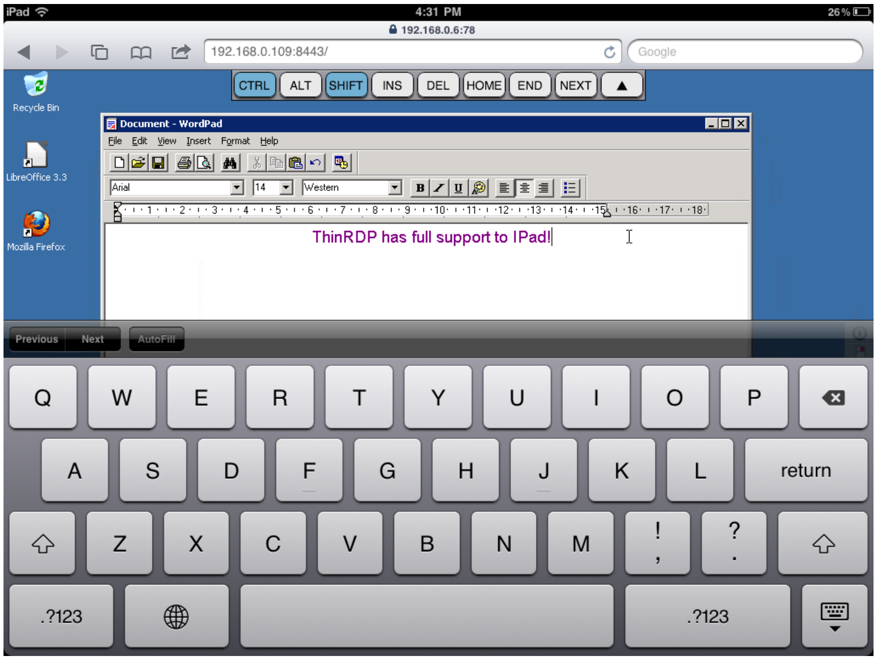
a. Enabling the regular keyboard:

I. If you are on the "Login" or on the "Settings" screen, this keyboard will get automatically enabled every time you enter a text field.
II. Once you get connected to a remote desktop or application, you should touch the last ThinRDP side menu button, in order to enable the regular keyboard.

o

b. Using the regular keyboard:

The keyboards use is very intuitive. You just have to touch the keys you want to type in.
To use numbers and special caracters, touch the "*.?123*" key.

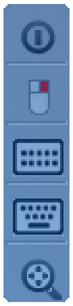


ThinRDP has full support to IPad!

If you want to make the regular keyboard invisible, press the last button (the one with a keyboard and a down arrow draw).

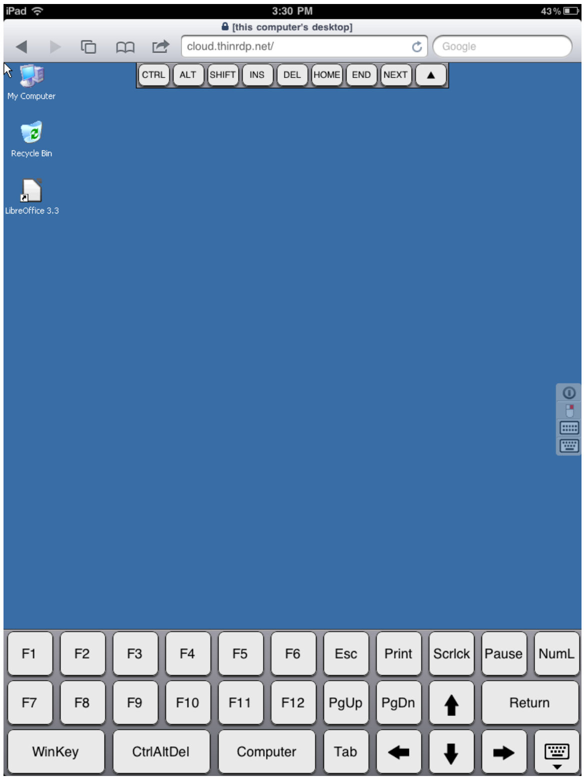
2. ThinRDP Extended Keyboard

ThinRDP has two additional keyboards.
In order to enable them you should touch the first up-down keyboard button, on the ThinRDP side menu.



a. Upper keyboard

The upper ThinRDP keyboard has the keys CTRL, ALT, SHIFT, INS, DEL, HOME, END and NEXT. This keyboard leaves the keys on until you have pressed a valid combination of them, for example, CTRL+ALT+DEL.



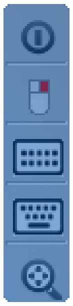
b. Bottom keyboard

The bottom ThinRDP keyboard has the F1-F12 keys, the arrow keys and few more, as you can check out on the up image.

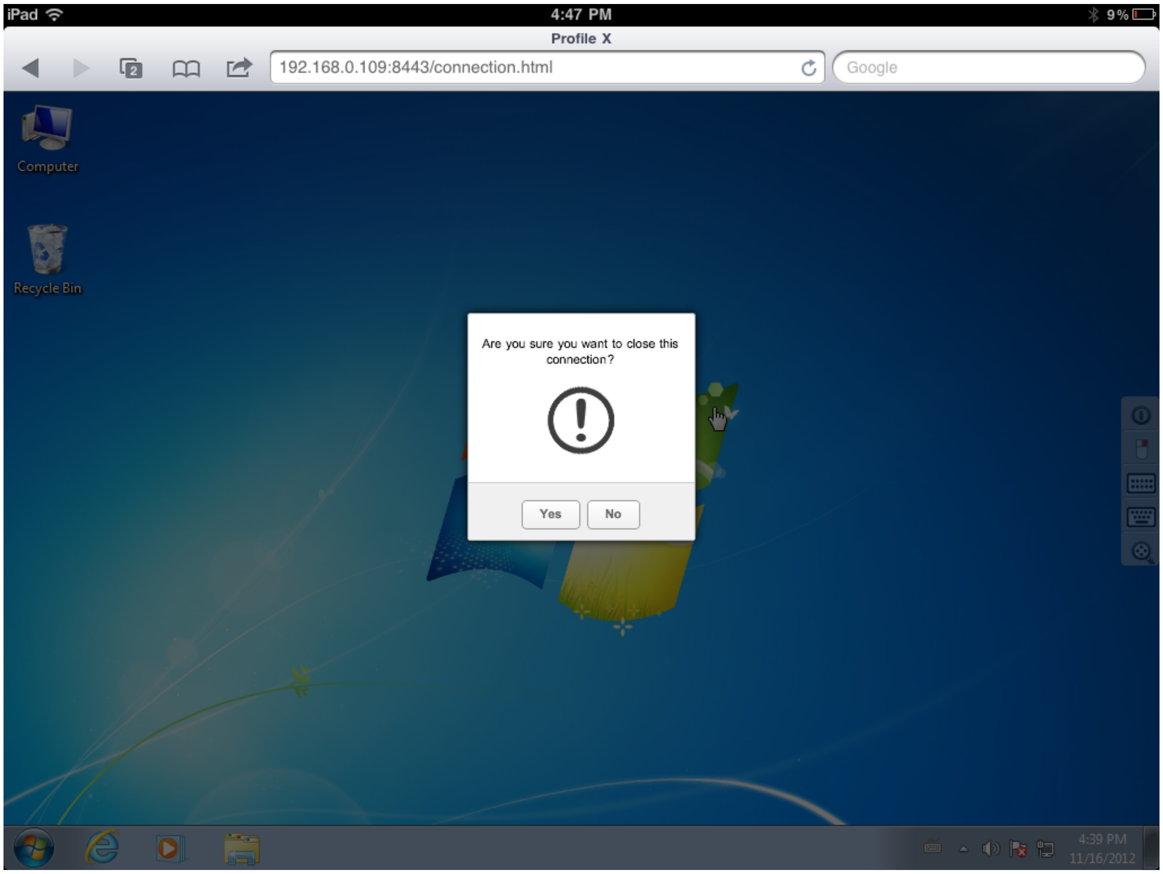
If you need to disable both ThinRDP additional keyboards, press the last bottom keyboard key (the one with a keyboard and a down arrow below draw).

11.5.6 Disconnecting from ThinRDP

1. In order to disconnect from the remote desktop touch the upper button located on the ThinRDP right side menu.



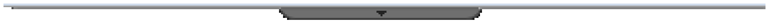
2. After touching the disconnect option you will receive a confirmation message. Touch "Yes" if you really want to disconnect from the remote desktop, otherwise touch "No".



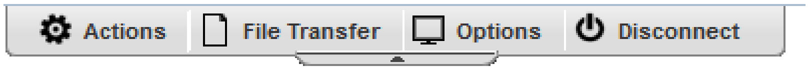
Are you sure you want to close this connection?

11.6 Disconnecting

1. Click on the connection middle top arrow, and the toolbar will be presented.



2. Click on the "Disconnect" button.



You can disconnect an active connection by closing the browser tab or performing a Windows logoff as well.