



Thinfinity® Remote Desktop Server

HTML5 Remote Desktop Client

Administrator's guide

Table of Contents

About This Document	7
Introduction	8
What's new in 4.0	9
Architecture	9
Security	13
Upgrade from 3.0	14
Getting Started	14
1 Installing Thinfinity® Remote Desktop Server	15
2 Using Thinfinity® Remote Desktop Server for the First Time	17
Verifying the Communication Settings	18
Connecting to a desktop	19
3 Customizing Thinfinity® Remote Desktop Server	20
Setting the Access Security Level	21
No Login Required	23
User / Password	24
Access Profiles	25
RDP Profiles	27
Creating an RDP Profile	27
Editing an RDP Profile	29
Disabling an RDP Profile	31
Removing an RDP Profile	32
The "[any computer]" Profile	33
Weblink Profiles	35
Creating a Weblink Profile	35
Editing a Weblink Profile	37
Disabling a Weblink Profile	39
Removing a Weblink Profile	40
RD Web Access Profiles	41
Creating an RD Web Access Profile	41
Editing an RD Web Access Profile	43
Disabling an RD Web Access Profile	45
Removing an RD Web Access Profile	46
Testing Internal Access	47
Configuring Internet Access	48
Enabling Remote Sound	49
Mapping Remote Drives	50
Intermediate Disks	50
Shared Folders	53
4 After Customization	55
Connecting to a Desktop	56
Connecting to an Application	59
Performing a File Transfer	61
Navigating	63
File Options	64
Remote Folder Area Options	65
Downloading and Uploading files	66

5 Supported RDP Shortcut Keys.....	67
Advanced Settings	68
1 Thinfinity® Remote Desktop Server Manager.....	69
Gateways	71
Security	73
Access Profiles	75
RDP Profile Editor.....	77
General	79
Setting up a Hyper-V Profile.....	81
Setting up an RDS Collection Profile.....	83
Display	85
Resources	87
Program	89
Experience	92
Advanced	94
Printer	96
Permissions	97
Web Link Profile Editor.....	98
Web Link	100
Permissions	101
RD Web Access Editor.....	102
General	103
Permissions	104
Folders	105
Permissions	107
Authentication	110
OAuth/2.....	110
Methods	110
Settings	113
Mappings	116
Configure OAuth with Okta.....	119
Configure OAuth with Auth0.....	128
RADIUS.....	135
Settings	135
Mappings	137
External DLL Authentication Method Settings	140
Duo Authentication Method Settings	141
How to configure DUO.....	143
SAML Authentication Method Settings	149
Configure SAML with Okta.....	150
Configure SAML with Centrify.....	159
2 Gateway Manager.....	165
Configure HTTP Error Responses	168
Managing the SSL Certificate	170
The Default Embedded Certificate.....	172
A Self-Signed Certificate.....	173
A CA Certificate.....	175
3 License Manager.....	177
License Activation	177
Proxy Activation.....	179
Get a new Trial Serial Number.....	180

Activate a Serial Number Online.....	180
Activate a Serial Number Offline.....	182
Registering Your License With The License Server Manager.....	184
4 Custom Settings.....	188
Extend the Remote Desktop's Toolbar	190
5 Customizing the Toolbar.....	193
Using customsettings.js	194
Using the 'connect' Method	196
6 Remote FX.....	197
7 Save Session.....	198
Record a Session	198
Play Recorded Sessions	199
8 Multitouch Redirection.....	200
9 Enhanced Browser and DPI Support.....	201
Model Inheritance	202
Property Reference	203
The Calculation Process	206
Examples	206
10 Silent Install Options.....	207
11 Credentials Management.....	210
User-based Access Profiles	210
Credentials Management	212
Mobile Devices	213
1 Getting into Thinfinity® Remote Desktop Server.....	215
2 Mouse Control.....	216
3 Keyboards and Toolbars.....	218
4 Gestures.....	222
5 Disconnecting from Thinfinity® Remote Desktop Server.....	224
Scaling and Load Balancing	225
1 Scaling and Load Balancing Configurations.....	226
2 Installing Components.....	228
3 Configuring a Load Balancing Scenario.....	229
Integrating Thinfinity® Remote Desktop Server	233
1 SDK.....	234
Deploying	236
Using the SDK	237
SDK Login	240
Connect method	240
Placement.....	245
Destination and Authentication.....	245
Settings.....	248
kbdLayout Values.....	250
Features	255
Events	257
Toolbar Customization.....	261

Browser Resizing	264
Keystroke Methods	265
SSL Certificate	268
Demo	269
2 External Authentication	270
Apikey	271
3 Single Sign On	272
Facebook OAuth Authentication Example	274
Google OAuth/2	276
Google Client ID for Web Applications	278
RADIUS	283
4 Customizing the Web Interface	285
Changing the Logo	287
Customizing the Web Files	288
Files Location	289
5 Web Services API	291
Architecture	292
Installing the Web Service	293
Setting up the Communication Settings	295
Profiles Web Service	297
Methods	298
Types	300
The WSPProfile type	302
The Demo Applications	305
Analytics Web Service	306
Methods	307
Types	308
WSQueryInfo	310
WSQueryRange	311
WSDBLoginRecord	312
WSDBSessionRecord	313
WSDBConnectionRecord	314
WSDBBrowserRecord	315
The Demo Application	316
6 One-Time-URL	317
Configuring the Connection	319
Enabling Features	323
User guide	325
1 Logging In	326
2 Connecting	327
Connecting with Open Parameters	329
General	330
Display	331
Resources	333
Program	336
Experience	339
Advanced	341
Connecting with Profiles	342
3 Toolbar	343

Actions	344
File Transfer	345
Options	345
Disconnect	346
4 Features	347
File Transfer	347
Navigating.....	349
File Options.....	350
Remote Folder Area Options.....	351
Downloading and Uploading files.....	352
Remote Printer	353
Remote Sound	354
Share Session	355
Mapped Drives	357
Analytics	358
Logins	359
Sessions.....	360
Connections.....	361
Browsers.....	362
Filter	363
Configuring MS SQL Server.....	364
Analytics Tables Reference.....	367
5 Disconnecting	372

1 About This Document

In this help file you will find information about Thinfinity® Remote Desktop Server. This document is intended for administrators to set up and configure Thinfinity® Remote Desktop Server. Check the [Getting Started](#) section and follow the instructions to quickly install and configure Thinfinity® Remote Desktop Server. Look into the [Advanced Settings](#) section to learn how you can better take advantage of the many features Thinfinity® Remote Desktop Server 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 <https://www.cybelesoft.com>

2 Introduction

Thinfinity® Remote Desktop Server is a web application that allows users to **access** their **Windows Desktops remotely** from any device of their preference.

Why Thinfinity® Remote Desktop Server?

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 HTML5 compliant browser.
3. In a local area network (LAN), Thinfinity® Remote Desktop Server 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.

Thinfinity® Remote Desktop Server 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, Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server'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 Thinfinity® Remote Desktop Server](#)

[Advanced Settings](#)

[User's guide](#)

3 What's new in 4.0

Now Thinfinity® Remote Desktop Server includes many new options and features that enhance the user experience:

New in 4.0 :

- Support for OpenID Connect protocol.
- Support for [DUO](#) 2FA.
- Support for ForgeRock OAuth.
- User-based [Access Profiles](#).
- User-based [Credentials Management](#).

And all the features from previous versions :

- 40% faster than previous version.
- Support for Microsoft® RemoteFX™, enabling fast, enhanced visual experience of the Windows desktop. [Read more](#).
- Create shortcuts to any configured connection using Virtual Paths. [Read more](#).
- Record your remote desktop sessions and play them within the Thinfinity® Remote Desktop Server web interface. [Read more](#).
- Multi-touch input redirection. Send the input of up to ten simultaneous fingers to be interpreted in the remote OS. [Read more](#).
- Load Balancing for a better performance on large deployments. [Read more](#).
- RADIUS authentication. Integrate the Thinfinity® Remote Desktop Server authentication with the RADIUS system. [Read more](#).
- Populate Microsoft RD Web Access remote apps and desktops. [Read more](#).
- Customize the Thinfinity® Remote Desktop Server user access to toolbar buttons. [Read more](#).
- Use MS-SQL as the default backend database for storing the [Analytics](#) data. [Read more](#).
- OAuth/2 now configurable with any server that supports this functionality. [Read more](#).

4 Architecture

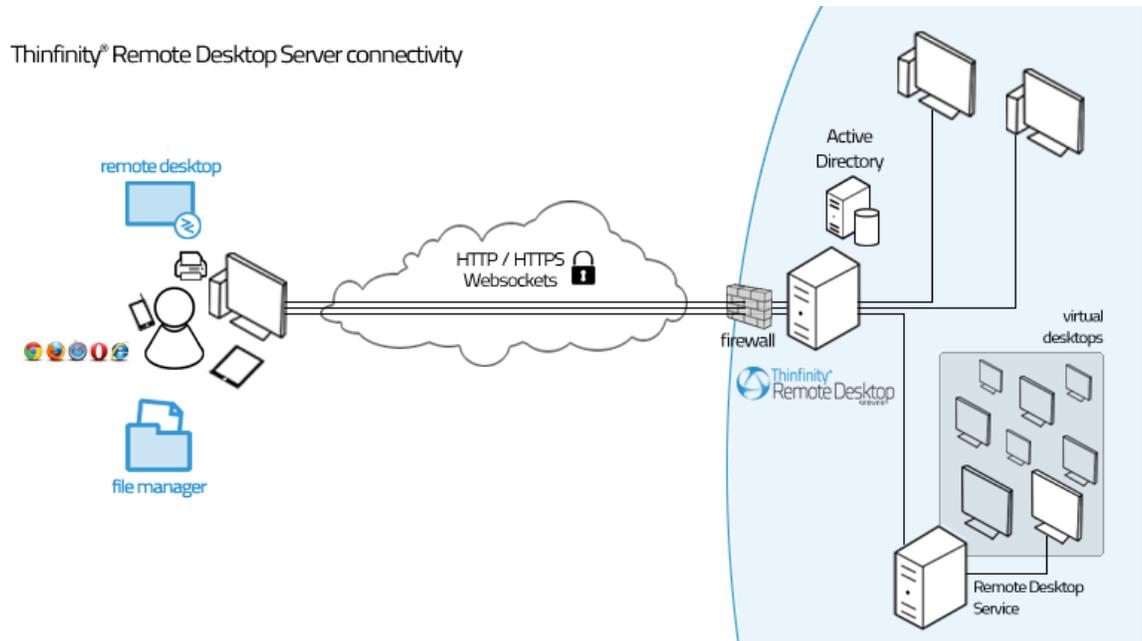
Thinfinity® Remote Desktop Server is composed of:

- a Server Machine running Thinfinity® Remote Desktop Server
- Thinfinity® Remote Desktop Web Client (*which loads on an HTML5 browser*)

Thinfinity® Remote Desktop Server is a secure, high-performance HTTP / WebSockets server, which serves the web pages needed to run the Thinfinity® Remote Desktop Web Client on the web browser.

When the end-user accesses the Thinfinity® Remote Desktop main page and enters the appropriate connection parameters, the Thinfinity® Remote Desktop Web Client communicates with the server, using Ajax and WebSockets (if available) to start the connection to the remote-end.

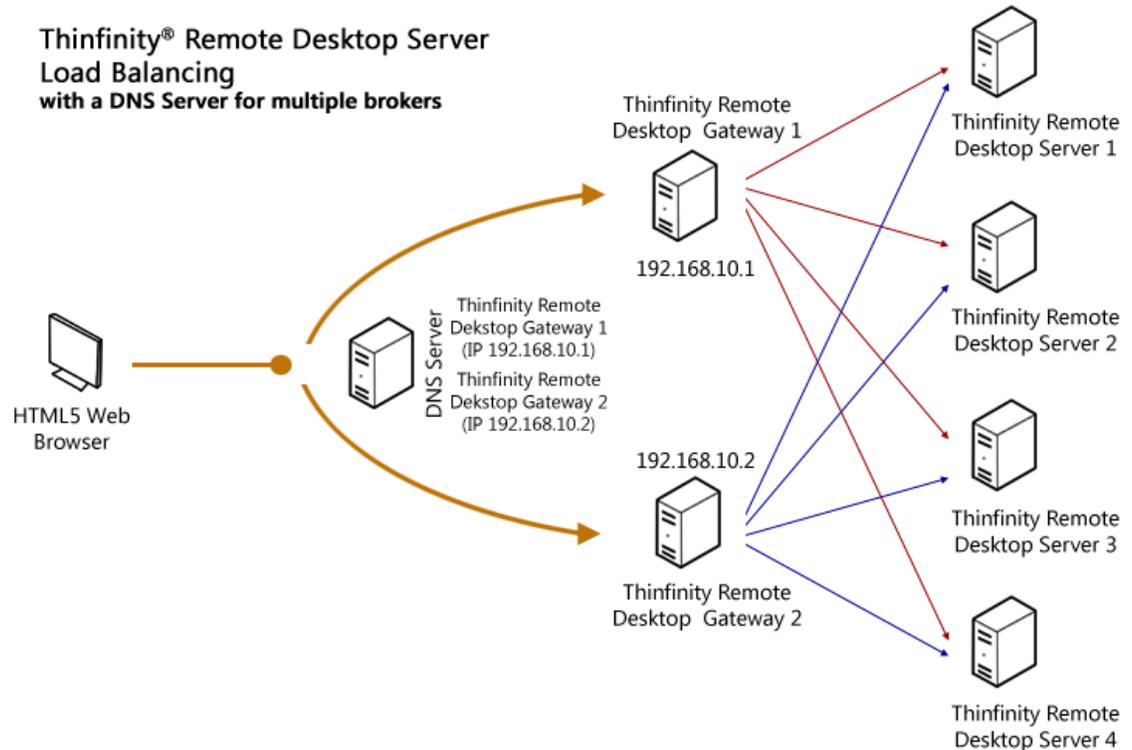
Once the connection is established, the server will receive RDP commands, optimize them for the web, and send the resulting data stream to the Thinfinity® Remote Desktop Web Client.



Load Balancing Architectures for Thinfinity® Remote Desktop Server:

Thinfinity® Remote Desktop Server can be configured in two different load balancing architectures:

- Thinfinity® Remote Desktop Server Load Balancer
- Thinfinity® Remote Desktop Server Load Balancer with a DNS for multiple brokers



[Read more about load balancing.](#)

Requirements:

Using Thinfinity® Remote Desktop Server, any Windows, Mac OS X, Linux, Android and iOS user can remote into a Windows desktop or work with a single Windows application.

Web Client

- OS independent
- HTML5-compliant Web Browser
 - Internet Explorer 9.0, 10.0, 11.0
 - Firefox 17+
 - Chrome 22+
 - Safari 6.0.1+
 - iOS 5.1.1+
 - Android 2.3, 4.0+
 - Edge 38+

Server Machine

- Windows XP 32 and 64 bit
- Windows Vista 32 and 64 bit
- Windows 7 32 and 64 bit
- Windows 8 32 and 64 bit
- Windows 10 32 and 64 bit
- Windows Server 2003 32 and 64 bit

- Windows Server 2008 32 and 64 bit
- Windows Server 2012 and 2012 R2
- Windows Server 2016

5 Security

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

Secure connections

All the connections to Thinfinity® Remote Desktop Server from the browser are performed over HTTPS. Thinfinity® Remote Desktop Server provides you with the means to install your own 256-bit SSL certificate.

Authentication levels

Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server authentication with external applications, read the [External Authentication](#) and [Single-Sign-On](#) topics.

6 Upgrade from 3.0

If you are upgrading from Thinfinity Remote Desktop Server 3.0 , you'll have to perform the following steps :

1. Download the installer from this link:

<http://www.cybelesoft.com/downloads>

2. Make sure your license was updated to Thinfinity Remote Desktop Server 4.0 (please contact sales@cybelesoft.com in regards to this).
3. Uninstall Thinfinity Remote Desktop Server 3.0.
4. Install Thinfinity Remote Desktop Server 4.0.

Don't worry about your configuration. By default this is stored in "C:\ProgramData\Cybele Software \Thinfinity\Remote Desktop Server\" and won't be deleted.

7 Getting Started

Use this section to cover the fundamental aspects of Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server in a matter of minutes:

1. [Installing Thinfinity® Remote Desktop Server](#)
2. [Using Thinfinity® Remote Desktop Server for the first time](#)
3. [Customizing Thinfinity® Remote Desktop Server](#)
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 Thinfinity® Remote Desktop Server](#)

[User's Guide](#)

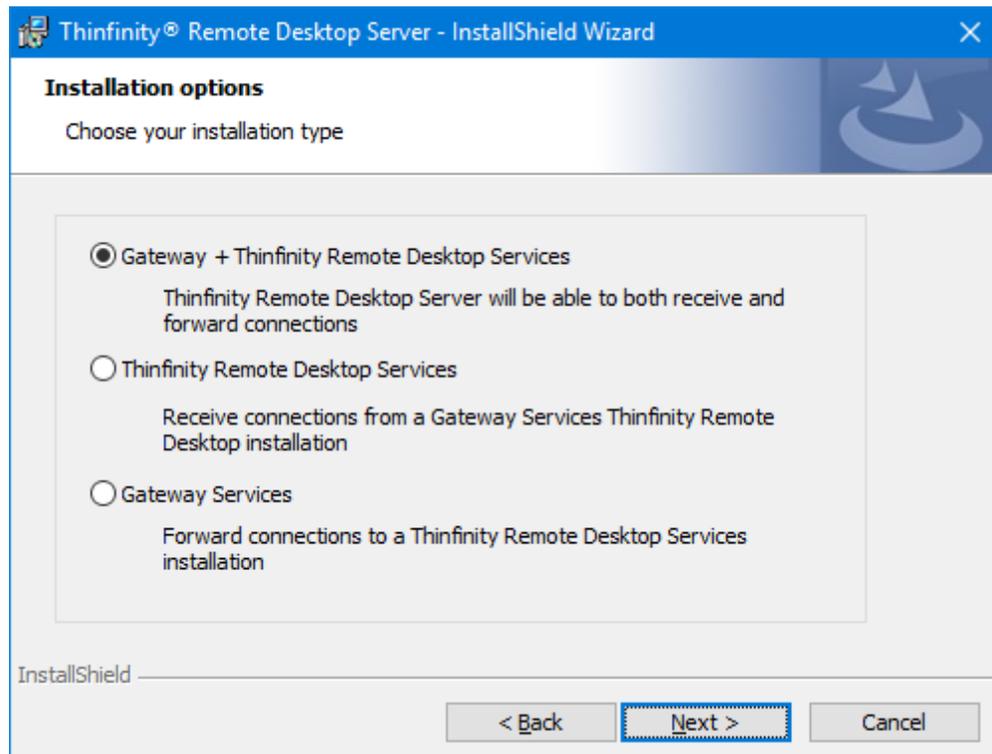
7.1 Installing Thinfinity® Remote Desktop Server

Thinfinity® Remote Desktop Server 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>

2. Execute the installer on the target machine.
You will be presented with these options:



Gateway + Thinfinity Remote Desktop Services

Choose this option for a standalone installation. Both a Thinfinity Remote Desktop Services and Gateway Services installation coexist in the same computer. Also, this installation can work together with others in a [Scaling and Load Balancing](#) configuration.

Thinfinity Remote Desktop Services

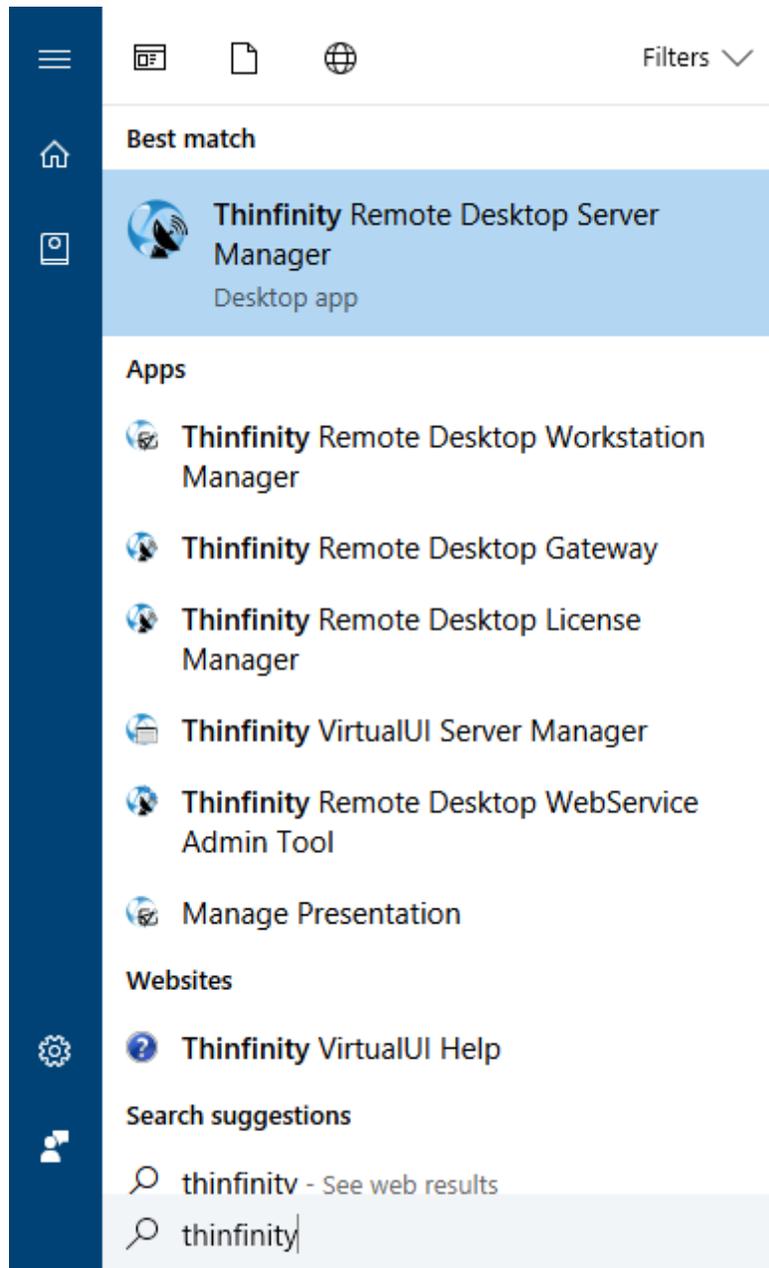
Choose this option only if you are using a [Scaling and Load Balancing](#) configuration. A Thinfinity Remote Desktop Services installation works together with at least one gateway installation and other Thinfinity Remote Desktop Services installation(s).

Gateway Services

Choose this option only if you are using a [Scaling and Load Balancing](#) configuration. A Gateway Services installation works together with two or more Thinfinity Remote Desktop

Services installations.

3. Look for the "*Thinfinity® Remote Desktop Server Manager*" in the Start Menu.



7.2 Using Thinfinity® Remote Desktop Server for the First Time

Connecting to a remote desktop for the first time with Thinfinity® Remote Desktop Server is really easy:

[Verify the communications settings](#)

Once Thinfinity® Remote Desktop Server is installed and RDP is enabled in the remote machine, 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](#).

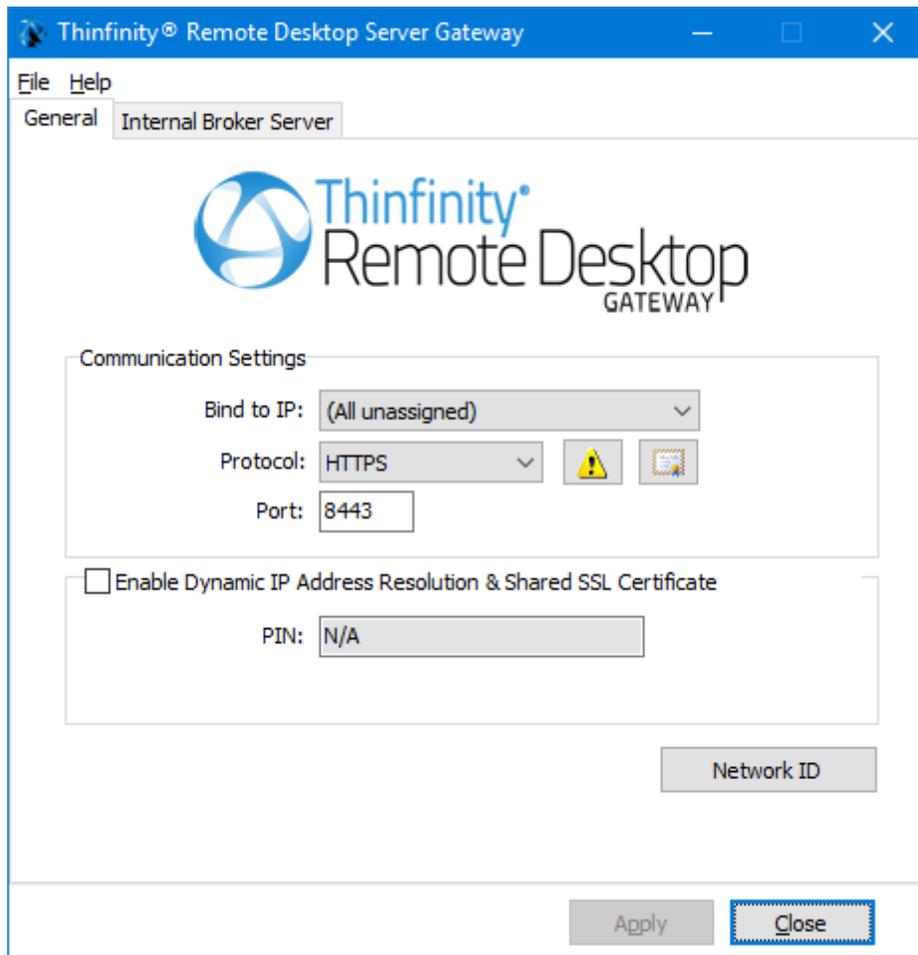
When all of this is ready, [Connect to a desktop](#) for the first time with Thinfinity® Remote Desktop Server.

7.2.1 Verifying the Communication Settings

Check whether Thinfinity® Remote Desktop Gateway is running by looking at the status message located on the bottom of the window. It should say "Registered on https...".

Thinfinity® Remote Desktop Gateway listens by default on port 8443. 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 yet in use in the computer where Thinfinity® Remote Desktop Gateway is installed.

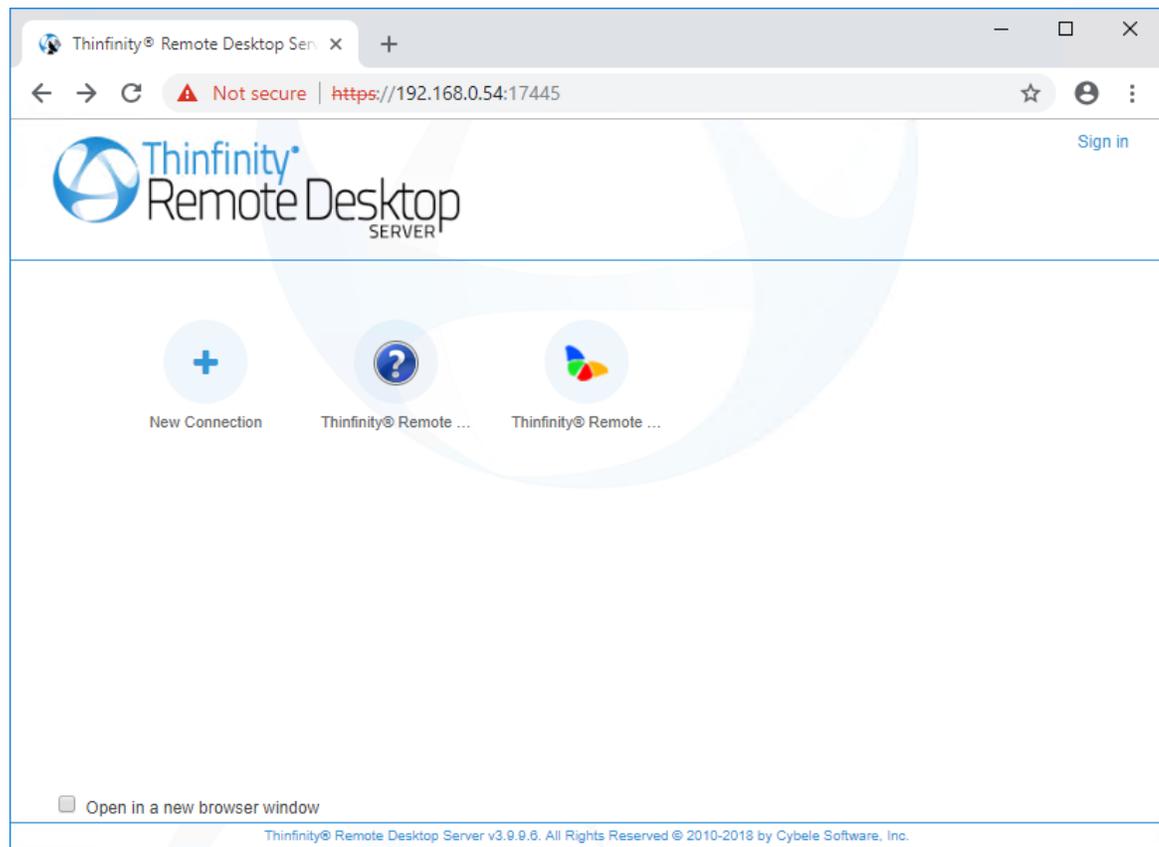


2. Change the port number in Thinfinity® Remote Desktop Gateway.
3. Press "Apply". Wait for a couple of minutes.
4. Verify whether Thinfinity® Remote Desktop Gateway is running in the status message.

7.2.2 Connecting to a desktop

1. Open your preferred HTML5-enabled web browser in the computer where Thinfinity® Remote Desktop Server was installed.
2. Type the following url: <https://127.0.0.1:8443/> into the address bar. If you have changed the port number in the [previous step](#), replace the port number in this url. When you access from a different computer, replace [127.0.0.1](#) with the server IP address or DNS name.

You will be presented with the following screen:



3. In the 'Computer' field, enter the remote desktop IP you want to connect to.
4. Enter the Username and Password for the remote machine.
5. Press 'Connect'.
6. The remote desktop will show inside the browser and you can use it like a regular remote desktop session.

If you want to change the RDP connection settings, press the plus (+) sign on the right upper corner before connecting and the [Display](#), [Program](#), [Experience](#), [Advanced](#) and [Resources](#) options will show.

To set up different options and make Thinfinity® Remote Desktop Server suit better your needs, read the [Customizing Thinfinity® Remote Desktop Server](#) topic.

7.3 Customizing Thinfinity® Remote Desktop Server

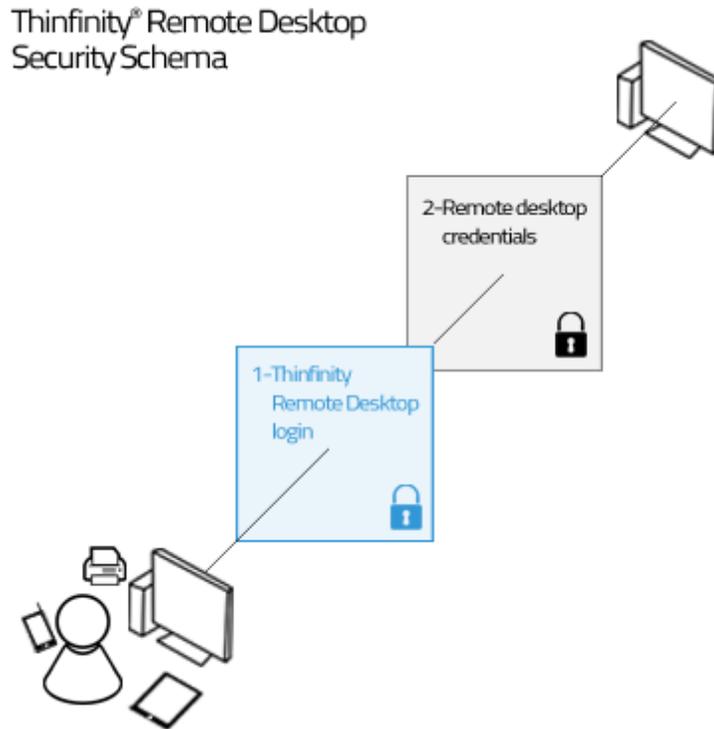
Once you have installed Thinfinity® Remote Desktop Server and connected for the first time, you can tailor it to serve your specific needs:

Read more:

- [Setting the Access Security Level](#)
- [Testing Internal Access](#)
- [Configuring Internet Access](#)
- [Enabling Remote Sound](#)
- [Mapping Remote Drives](#)

7.3.1 Setting the Access Security Level

The application administrator can set two user access security levels.



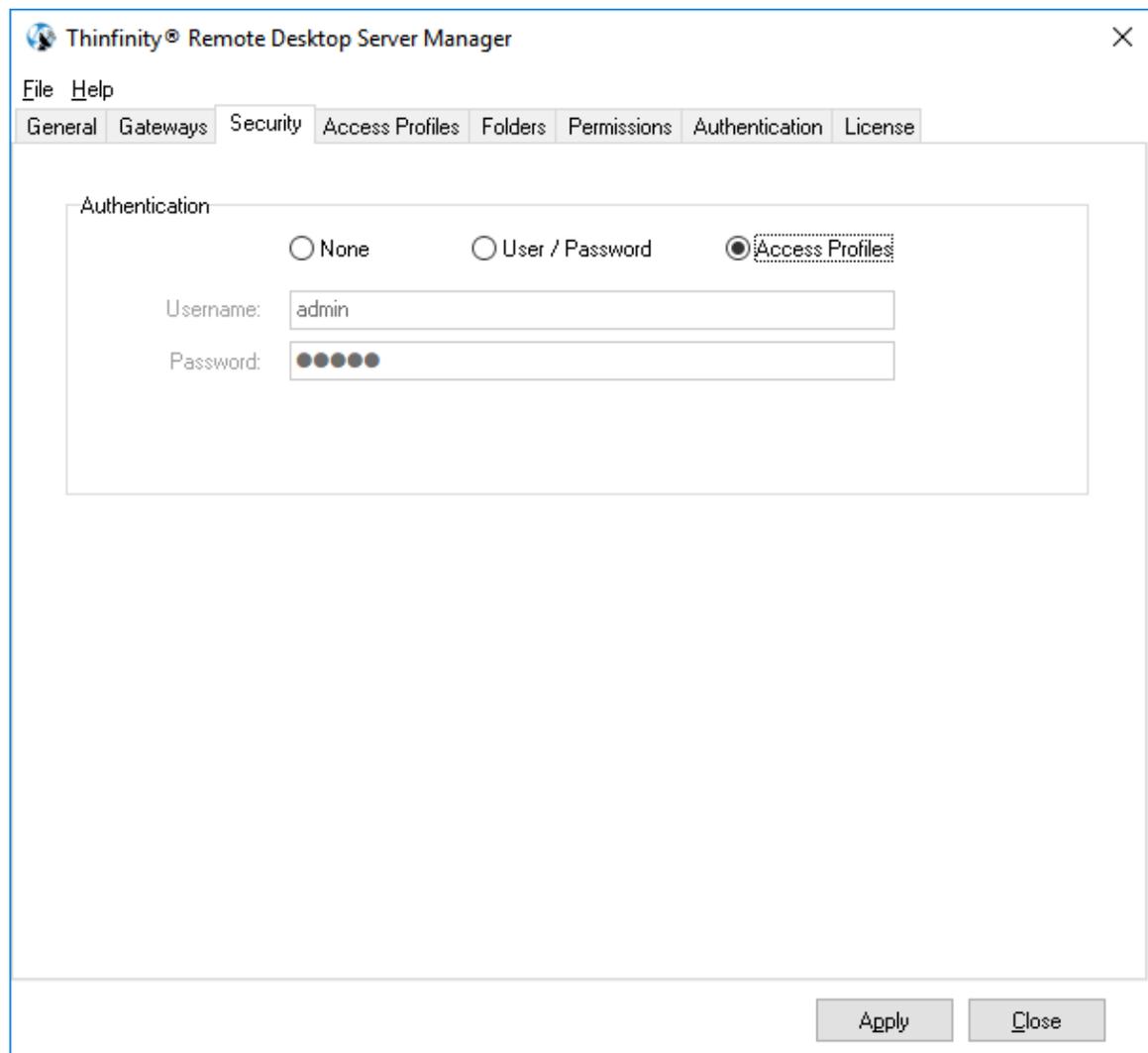
1. Application Login:

The first level provides access to users into the Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server Manager:

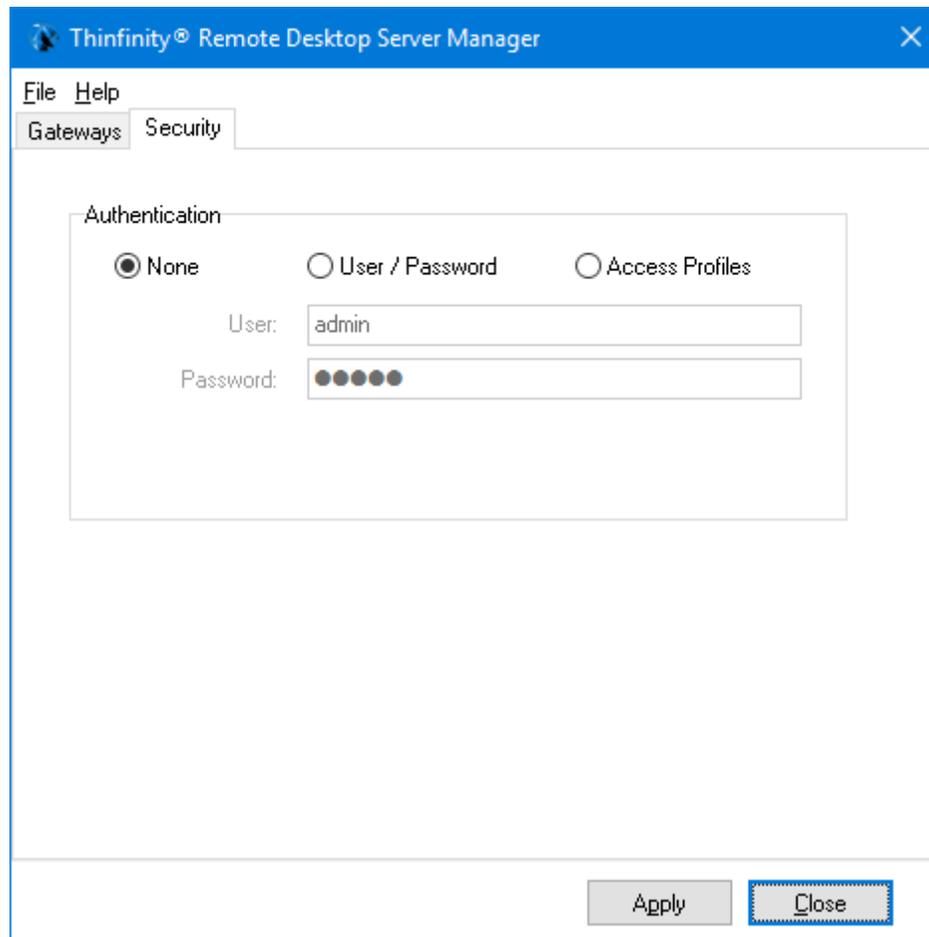


7.3.1.1 No Login Required

When you first install Thinfinity® Remote Desktop Server, the authentication will be set to "None", in other words it will have no login required.

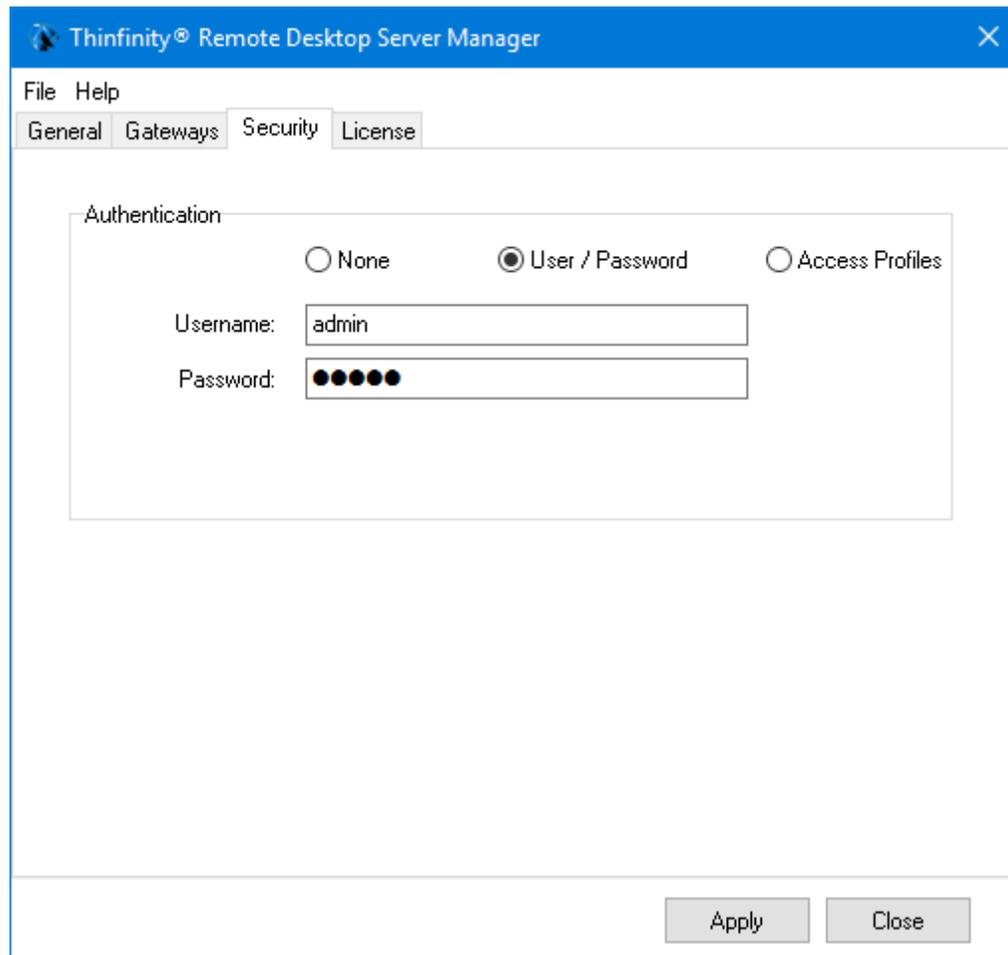
When you set the security to None, it means that everyone will have access into the Thinfinity® Remote Desktop Server application without identifying themselves and so the first security level will be disabled.

This option is only recommended for local use.



7.3.1.2 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.



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 Thinfinity® Remote Desktop Server.

7.3.1.3 Access Profiles

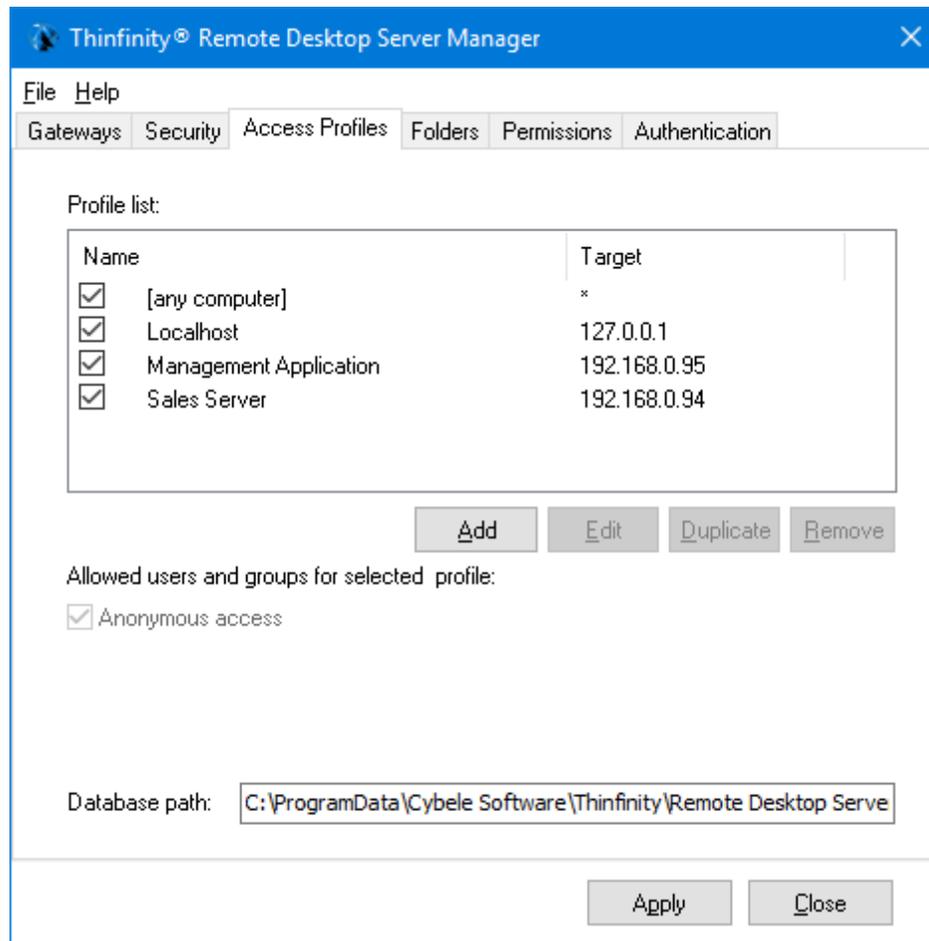
This option enables you to tailor access profiles and let users seamlessly and safely connect their desktop, applications and weblinks, using the current company's security policy.

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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server Manager's "Security" tab.

This will enable the "Access Profiles" tab, as shown below.



The following topics will teach you how to manage [RDP profile](#), [Weblink profiles](#) and [RD Web Access Profiles](#) from this Access Profiles window.

7.3.1.3.1 RDP Profiles

An RDP profile is a profile that safely connects users to their desktop and applications.

Read More:

- [Create an RDP Profile](#)
- [Edit an RDP Profile](#)
- [Disable an RDP Profile](#)
- [Remove an RDP Profile](#)
- [Get to know the "any computer" profile](#)

7.3.1.3.1.1 Creating an RDP Profile

1. Go to the Thinfinity Remote Desktop Server 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:

Thinfinity Remote Desktop Server - Profiles Editor

Name: New RDP Profile

Virtual Path: New_RDP_Profile

Access Key: LTSFAENHVqVSiuwsunLgttPbHrAuJwkW@bZx4-0eRJ\$zEwV New Key

Icon: None RDP Profile Web Link RD Web Access

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 an RDS Collection

Credentials:

Use the authenticated credentials

Ask for new credentials

Use these credentials:

User name:

Password:

Ok Cancel

3. Read the next topic ([Edit a profile](#)) to learn how to configure this profile.

Read More:

- [Edit an RDP Profile](#)
- [Disable an RDP Profile](#)
- [Remove an RDP Profile](#)
- [Get to know the "any computer" profile](#)

7.3.1.3.1.2 Editing an RDP 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 Thinfinity® Remote Desktop Server 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:

The screenshot shows the "Profiles Editor" window for Thinfinity Remote Desktop Server. The "Name" field is set to "Notepad" and the "Virtual Path" is also "Notepad". The "Access Key" is a long alphanumeric string. The "Icon" is a notepad icon, and the "RDP Profile" radio button is selected. The "General" tab is active, showing the "Computer" field set to "127.0.0.1". Under "Credentials", the "Use the authenticated credentials" radio button is selected. The "User name" and "Password" fields are empty. The "Ok" and "Cancel" buttons are at the bottom right.

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 <i>Single sign-on</i> 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 Thinfinity® Remote Desktop Server, 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 Thinfinity® Remote Desktop Server will see this profile. Checking this option will disable the user selection.
Group or users access	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. (*)

(*) Thinfinity Remote Desktop supports a user changing the password at his next logon within the Thinfinity Remote Desktop web interface. Make sure to [uncheck the 'Use standard browser authentication dialog'](#) to enable this option

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.

Read More:

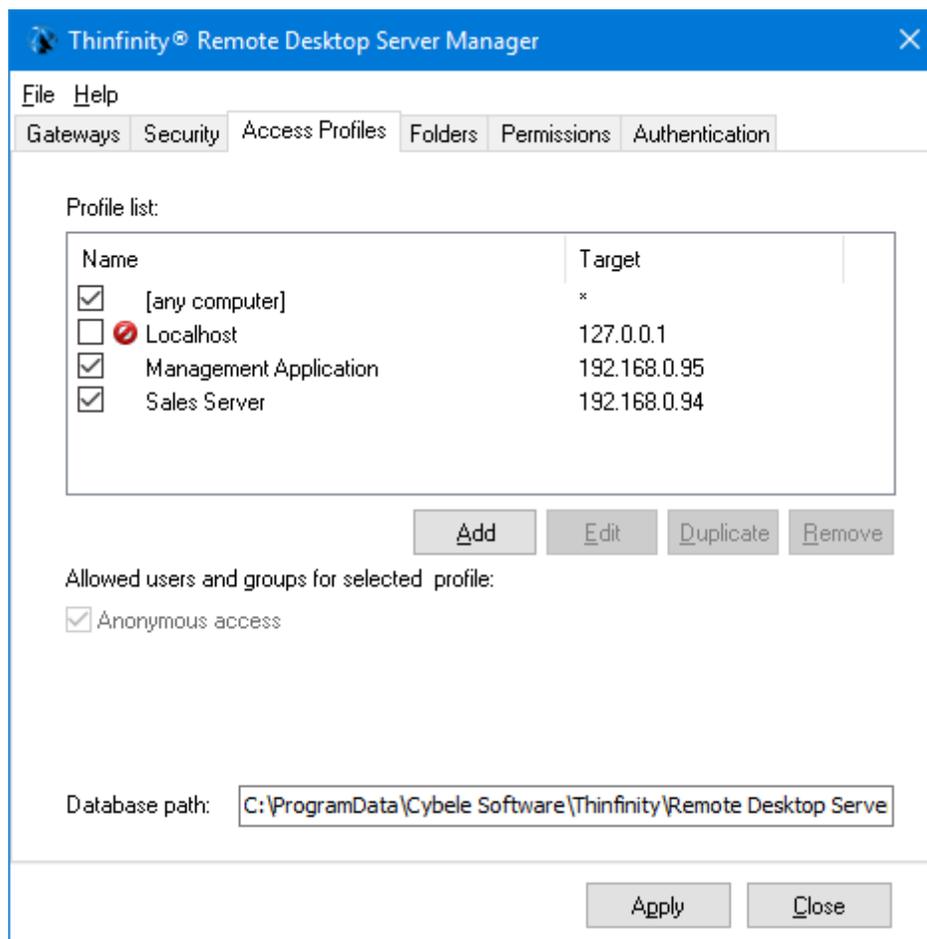
- [Disable an RDP Profile](#)
- [Remove an RDP Profile](#)
- [Get to know the "any computer" profile](#)

7.3.1.3.1.3 Disabling an RDP 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 Thinfinity® Remote Desktop Server Manager's "Access Profile" tab. If it is not there, read the [Access Profiles](#) topic first.
2. Select the profile you want to 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.



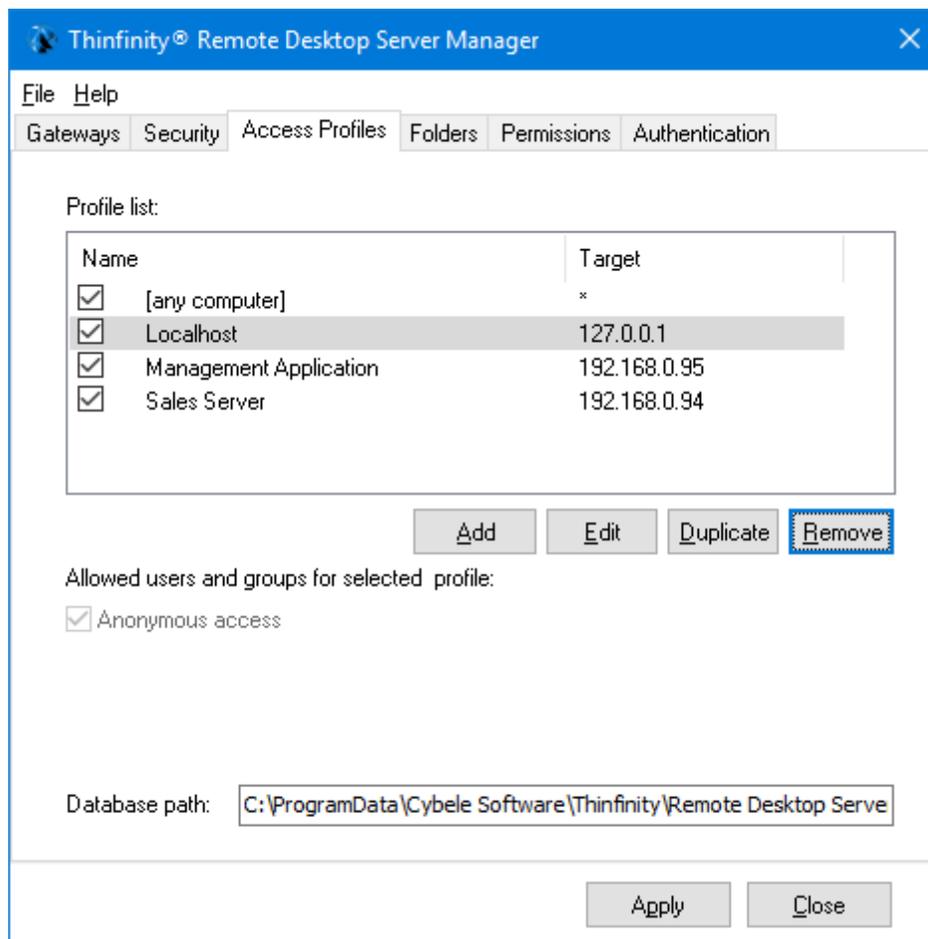
Read More:

- [Remove an RDP Profile](#)
- [Get to know the "any computer" profile](#)

7.3.1.3.1.4 Removing an RDP Profile

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

1. Go to Thinfinity® Remote Desktop Server 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.



Read More:

- [The "\[any computer\]" profile](#)

7.3.1.3.1.5 The "[any computer]" Profile

The "[any computer]" profile is the default profile for Thinfinity® Remote Desktop Server.

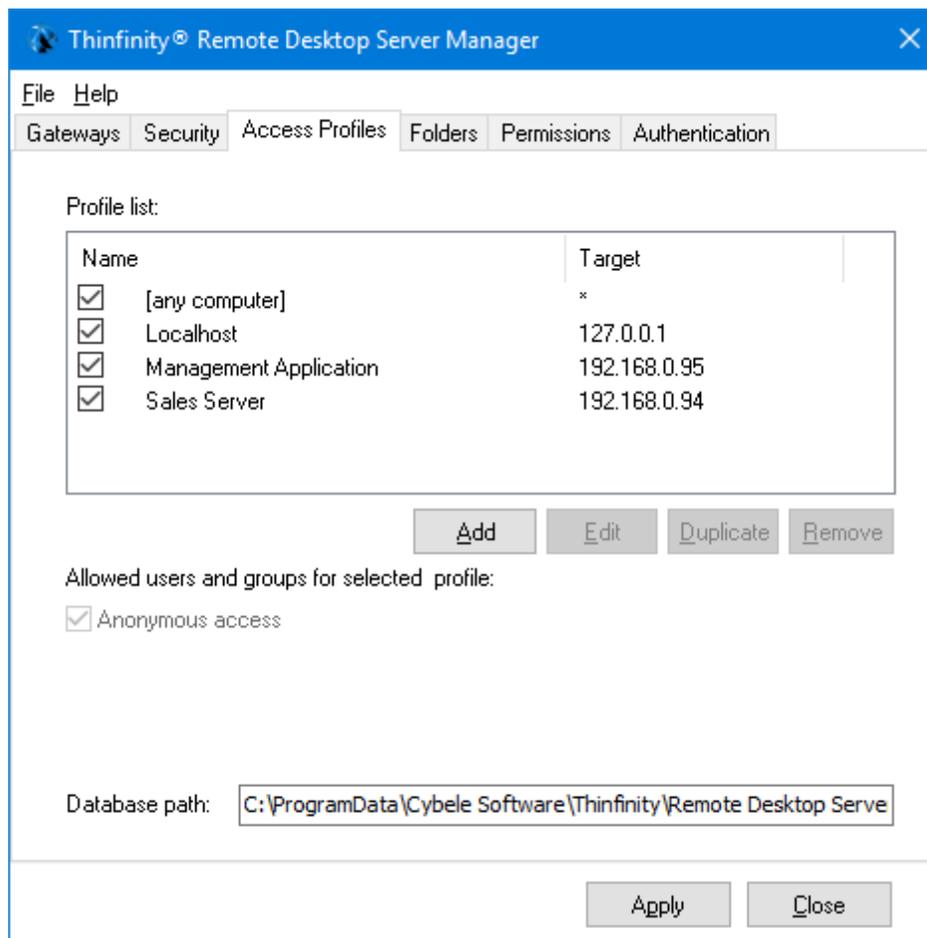
It has two special behaviors:

- 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.



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

The screenshot shows the 'Thinfinity Remote Desktop Server - Profiles Editor' window. It contains the following fields and controls:

- Name:** [any computer]
- Virtual Path:** (empty text box)
- Access Key:** -aOYndjQfsHQCjUVsyZtj\Xz-MtmTxko105borIG\$t4fd-c1. A **New Key** button is located to the right of this field.
- Icon:** None

The **Permissions** section includes:

- Allow anonymous access
- Group or user names:** (empty list box)
- Add** and **Remove** buttons at the bottom right of the list box.

At the bottom of the window are **Ok** and **Cancel** buttons.

Read More:

- [Weblink Profiles](#)

7.3.1.3.2 Weblink Profiles

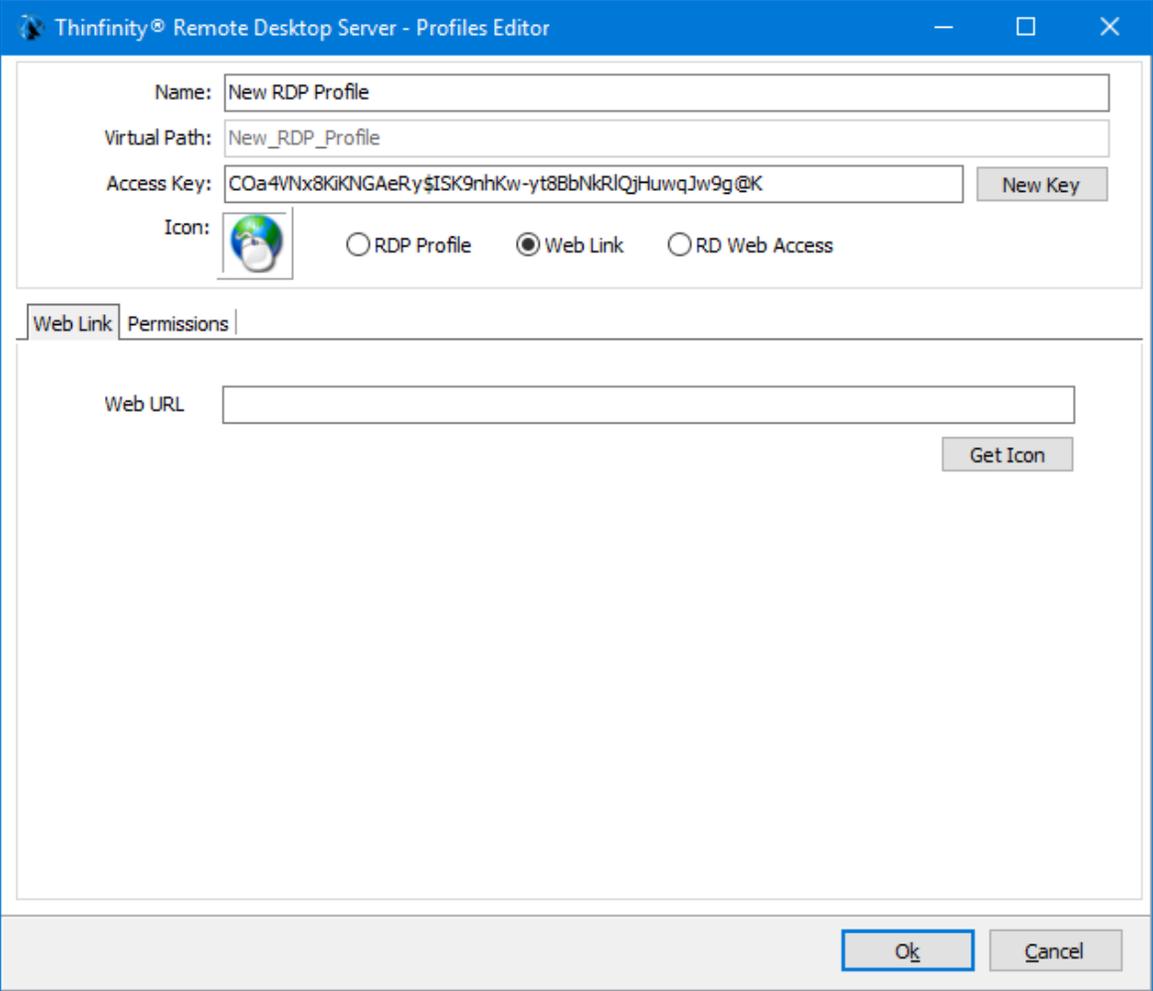
A Weblink profile is a profile that gives the users access to informed URL. These profiles will be presented along with the RDP profiles within the Web Interface.

Read More:

- [Creating a Weblink Profile](#)
- [Editing a Weblink Profile](#)
- [Disabling a Weblink Profile](#)
- [Removing a Weblink Profile](#)

7.3.1.3.2.1 Creating a Weblink Profile

1. Go to the Thinfinity Remote Desktop Server 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.



The screenshot shows the "Thinfinity Remote Desktop Server - Profiles Editor" dialog box. The "Name" field is set to "New RDP Profile" and the "Virtual Path" is "New_RDP_Profile". The "Access Key" field contains a long alphanumeric string, with a "New Key" button to its right. Under the "Icon" section, there is a globe icon and three radio buttons: "RDP Profile", "Web Link" (which is selected), and "RD Web Access". Below this, there are two tabs: "Web Link" and "Permissions". The "Web Link" tab is active, showing a "Web URL" field and a "Get Icon" button. At the bottom of the dialog are "Ok" and "Cancel" buttons.

3. Read the next topic ([Edit a profile](#)) to learn how to configure this profile.

Read More:

- [Editing a Weblink Profile](#)
- [Disabling a Weblink Profile](#)
- [Removing a Weblink Profile](#)

7.3.1.3.2.2 Editing a Weblink Profile

1. Go to Thinfinity® Remote Desktop Server 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.

The screenshot shows the 'Profiles Editor' window for Thinfinity Remote Desktop Server. The 'Name' field is set to 'New RDP Profile', the 'Virtual Path' is 'New_RDP_Profile', and the 'Access Key' is 'COa4VNx8KIKNGAeRy\$ISK9nhKw-yt8BbNkRIQjHuwqJw9g@K'. The 'Web Link' radio button is selected. The 'Web URL' field is empty, and there is a 'Get Icon' button next to it. The 'Permissions' tab is also visible but not active.

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 Thinfinity® Remote Desktop Server 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.(*)
------------------------	--

(*) Thinfinity Remote Desktop supports a user changing the password at his next logon within the Thinfinity Remote Desktop web interface. Make sure to [uncheck the 'Use standard browser authentication dialog'](#) to enable this option

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

Read More:

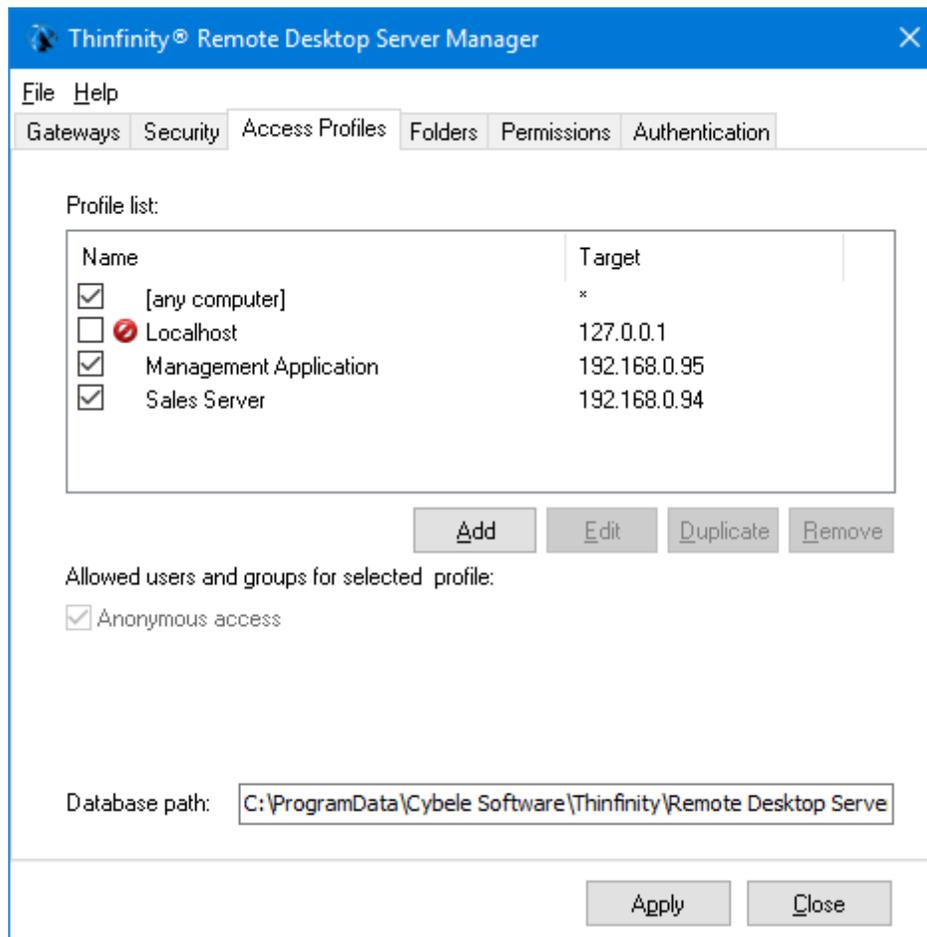
- [Disabling a Weblink Profile](#)
- [Removing a Weblink Profile](#)

7.3.1.3.2.3 Disabling a Weblink 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 Thinfinity® Remote Desktop Server Manager's "Access Profile" tab. If it is not there, read the [Access Profiles](#) topic first.
2. Select the profile you want to 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.



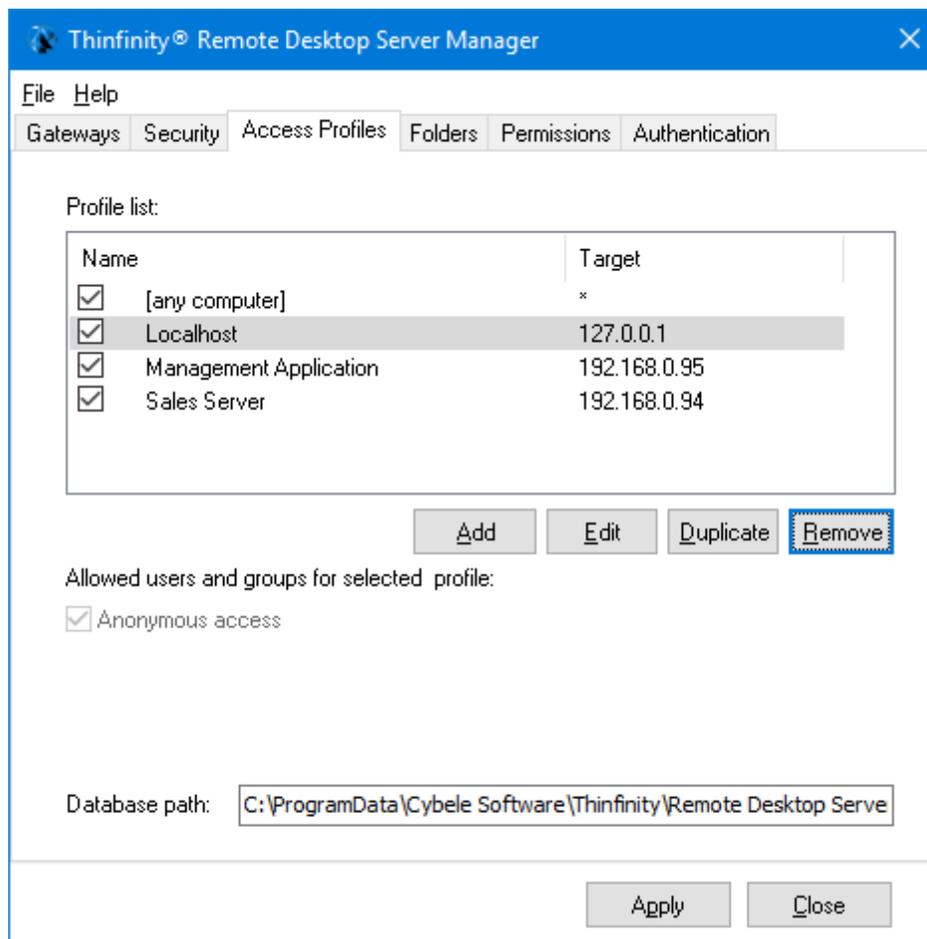
Read More:

- [Removing a Weblink Profile](#)

7.3.1.3.2.4 Removing a Weblink Profile

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

1. Go to Thinfinity® Remote Desktop Server 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.



Read more:

- [Testing Internal Access](#)

7.3.1.3.3 RD Web Access Profiles

An RD Web Access profile allows you to show Microsoft RD Web Access connections as regular Thinfinity Remote Desktop Server profiles.

Read More:

- [Creating an RD Web Access Profile](#)
- [Editing an RD Web Access Profile](#)
- [Disabling an RD Web Access Profile](#)
- [Removing an RD Web Access Profile](#)

7.3.1.3.3.1 Creating an RD Web Access Profile

1. Go to the Thinfinity Remote Desktop Server 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:

Thinfinity Remote Desktop Server - Profiles Editor

Name:

Virtual Path:

Access Key:

Icon: RDP Profile Web Link RD Web Access

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

Computer:

Connect to a Hyper-V Virtual Machine

Connect to a Virtual Desktop on an RDS Collection

Credentials:

Use the authenticated credentials

Ask for new credentials

Use these credentials:

User name:

Password:

3. Read the next topic ([Edit a profile](#)) to learn how to configure this profile.

Read More:

- [Editing an RD Web Access Profile](#)
- [Disabling an RD Web Access Profile](#)
- [Removing an RD Web Access Profile](#)

7.3.1.3.3.2 Editing an RD Web Access 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 Thinfinity® Remote Desktop Server Manager's "Access Profile" tab. If it is not there, read the topic [Access Profiles](#) first.
2. Press "Edit" to configure the profile.
3. First of all, type in a descriptive name for the profile in the "Name" field.
4. Select the 'RD Web Access' Option.

The screenshot shows the 'Profiles Editor' window for Thinfinity Remote Desktop Server. The 'Name' field is set to 'RDWebAccessServer', and the 'Virtual Path' is also 'RDWebAccessServer'. The 'Access Key' is a long alphanumeric string, and there is a 'New Key' button next to it. The 'Icon' field is empty. There are three radio buttons: 'RDP Profile', 'Web Link', and 'RD Web Access', with 'RD Web Access' selected. Below this is a tabbed interface with 'General' and 'Permissions' tabs. The 'General' tab is active, showing 'RD Web URL' and 'Credentials' sections. The 'RD Web URL' field is empty. The 'Credentials' section has two radio buttons: 'Use the authenticated credentials' (selected) and 'Use these credentials:'. Below these are 'User name' and 'Password' fields, both empty. At the bottom right are 'Ok' and 'Cancel' buttons.

5. Complete the 'RD Web URL' field with the Microsoft RD Web Access URL

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

Use the authenticated credentials	Sets a <i>Single sign-on</i> 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 Thinfinity® Remote Desktop Server, 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 Thinfinity® Remote Desktop Server 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.(*)

(*) Thinfinity Remote Desktop supports a user changing the password at his next logon within the Thinfinity Remote Desktop web interface. Make sure to [uncheck the 'Use standard browser authentication dialog'](#) to enable this option

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.

Read More:

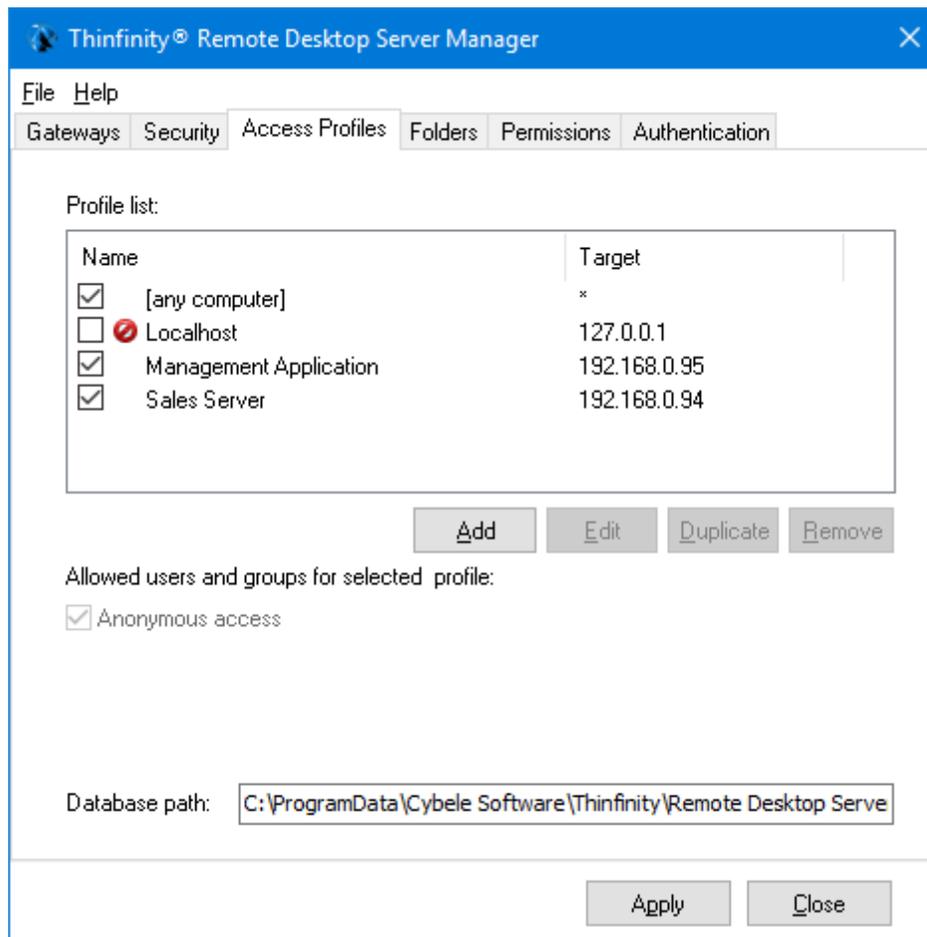
- [Creating an RD Web Access Profile](#)
- [Disabling an RD Web Access Profile](#)
- [Removing an RD Web Access Profile](#)

7.3.1.3.3 Disabling an RD Web Access 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 Thinfinity® Remote Desktop Server Manager's "Access Profile" tab. If it is not there, read the [Access Profiles](#) topic first.
2. Select the profile you want to 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.



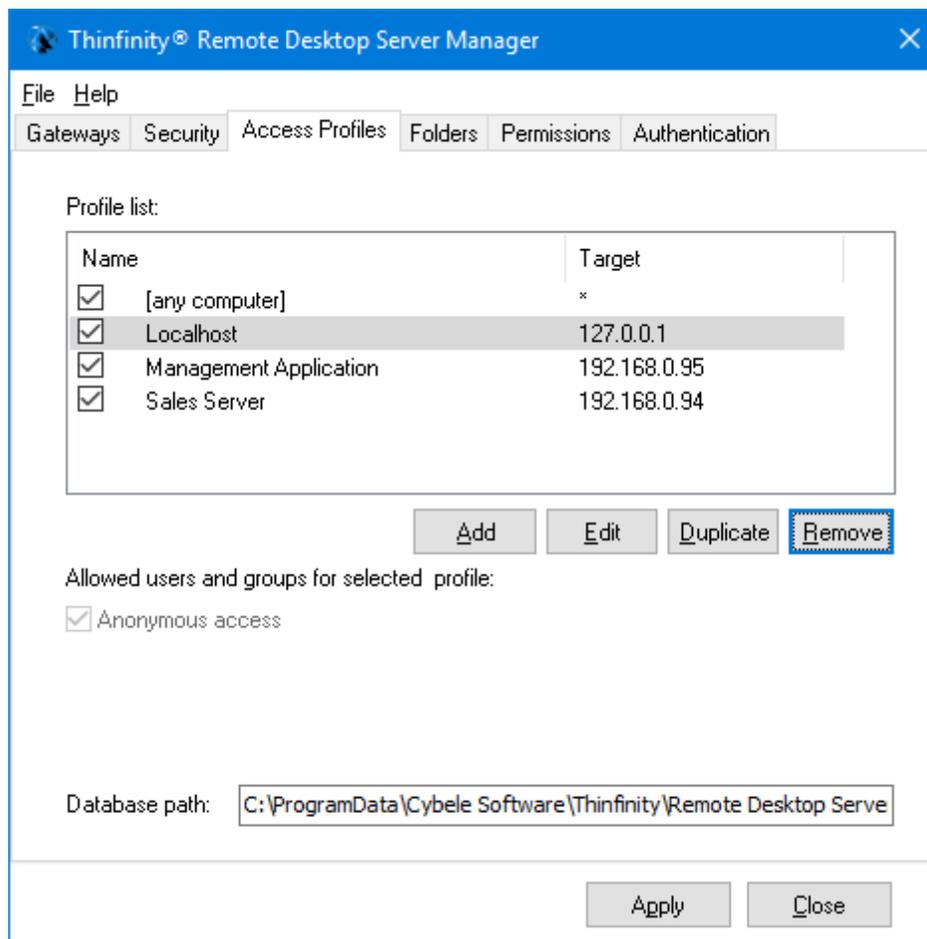
Read More:

- [Creating an RD Web Access Profile](#)
- [Editing an RD Web Access Profile](#)
- [Removing an RD Web Access Profile](#)

7.3.1.3.3.4 Removing an RD Web Access Profile

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

1. Go to Thinfinity® Remote Desktop Server 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.



Read More:

- [Creating an RD Web Access Profile](#)
- [Editing an RD Web Access Profile](#)
- [Disabling an RD Web Access Profile](#)
- [Testing Internal Access](#)

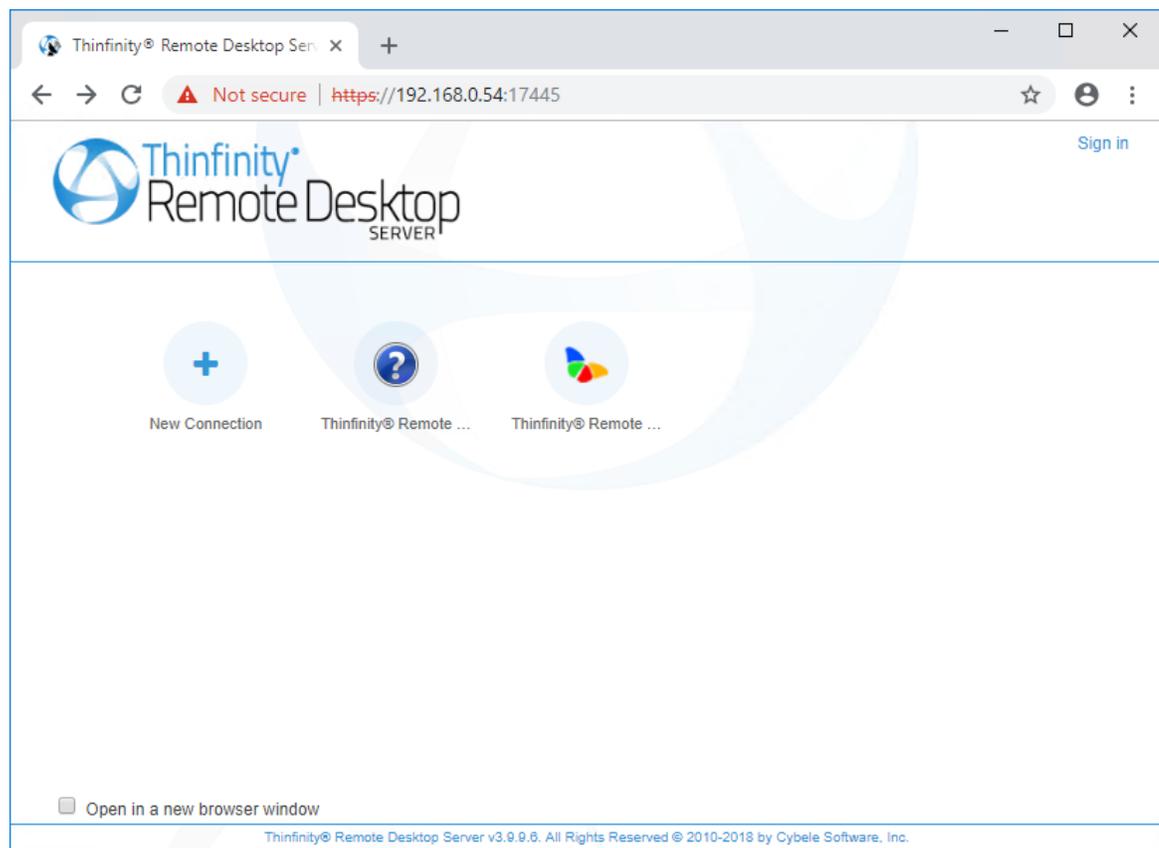
7.3.2 Testing Internal Access

Although Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server, 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 the Thinfinity® Remote Desktop Server main web interface:



This means that Thinfinity® Remote Desktop Server is running and you can use it within the LAN.

Read more:

- [Configuring Internet Access](#)
- [Enabling Remote Sound](#)
- [Mapping Remote Drives](#)

7.3.3 Configuring Internet Access

After you verified that Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server is running on, or a different one.
- d. Forward the internet port to the machine internal IP where you have installed Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server provides you on the Public Access section.

Read more:

- [Enabling Remote Sound](#)
- [Mapping Remote Drives](#)

7.3.4 Enabling Remote Sound

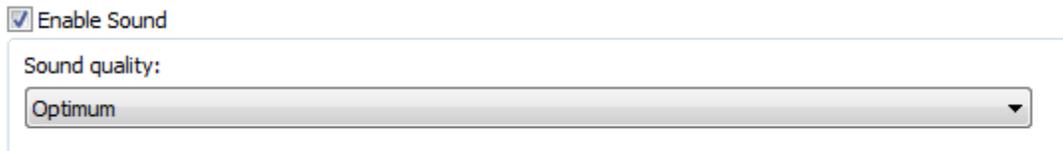
The remote sound feature allows you to listen to the sound playing on the remote machine. This feature is only available for Chrome and Firefox browsers for the moment.

Follow the next steps to enable the remote sound on Thinfinity® Remote Desktop Server.
If you are using:

a. Access Profiles:

Enable the remote sound on Thinfinity® Remote Desktop Server 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.



The screenshot shows a user interface element with a checked checkbox labeled "Enable Sound". Below it is a dropdown menu labeled "Sound quality:" with "Optimum" selected.

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".



The screenshot shows a user interface element with a checked checkbox labeled "Enable Remote Sound". Below it is a dropdown menu labeled "Sound Quality:" with "Optimum" selected.

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

Read more:

- [Mapping Remote Drives](#)

7.3.5 Mapping Remote Drives

Thinfinity® Remote Desktop Server allows you to map remote drives that enable you to interchange files between the remote environment and the local one.

You can map remote drives using two different features:

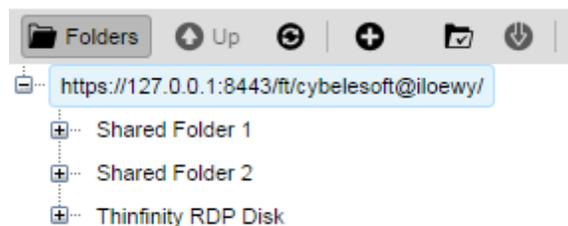
1. [Intermediate Disks](#)
2. [Shared Folders](#)

7.3.5.1 Intermediate Disks

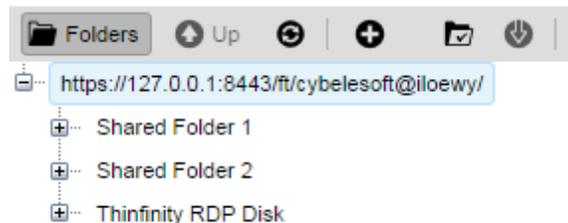
An intermediate disk is a directory created by Thinfinity® Remote Desktop Server to keep files that users will exchange between the remote computer and the browser.

The intermediate files will be available to Thinfinity® Remote Desktop Server users on two places:

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



- 2) On the [File Transfer](#) Manager as a remote directory to exchange files with.



Configuring an Intermediate disk is very easy:

If using Access Profiles:

1. On Thinfinity® Remote Desktop Server 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.

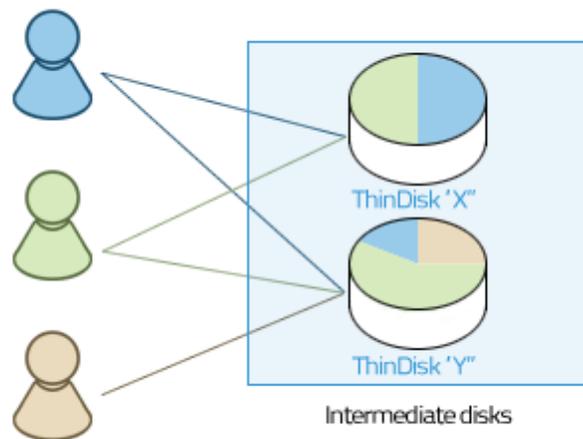
If using other authentication methods:

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.

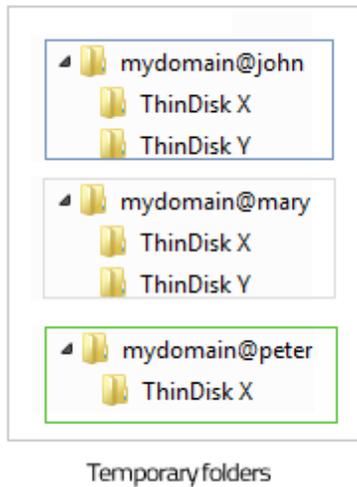
Intermediate physical files location:

The location where these files are kept physically is called "[Temporary Folders](#)" and can be also customized on Thinfinity® Remote Desktop Server 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:

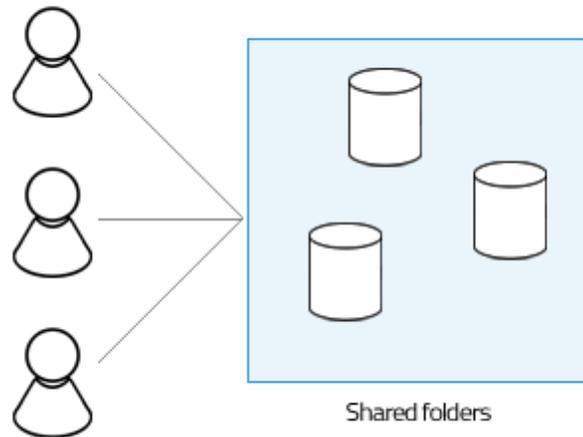


A user will have access to an intermediate disk, if he/she has access to any profile associated with this disk.

When a profile is set to anonymous, all users that connect through it will also have access to the disk associated with this profile.

7.3.5.2 Shared Folders

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



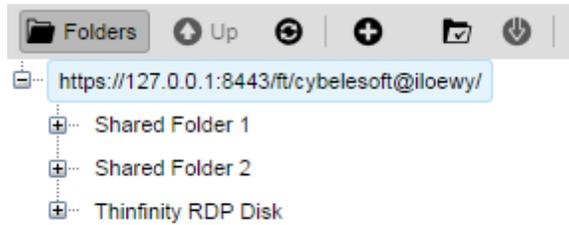
Follow these steps to configure a new Shared Folder:

1. On Thinfinity® Remote Desktop Server 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 screenshot shows a dialog box titled "Share This Folder" with a close button (X) in the top right corner. It contains two input fields: "Network path:" with a text box and a browse button (three dots), and "Share name:" with a text box. Below the "Share name:" field, it states "The following characters are considered invalid:" followed by the characters "<, >, \", /, \, |, :, =". At the bottom, there are "OK" and "Cancel" buttons.

5. Press OK.

6. From now on, users will find this directory as a mapped drive in every Thinfinity® Remote Desktop Server connection, and also as a Remote location on the File Transfer Manager.



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.

7.4 After Customization

If you have already customized Thinfinity® Remote Desktop Server, check out the following sections to see how your changes will reflect on Thinfinity® Remote Desktop Server application:

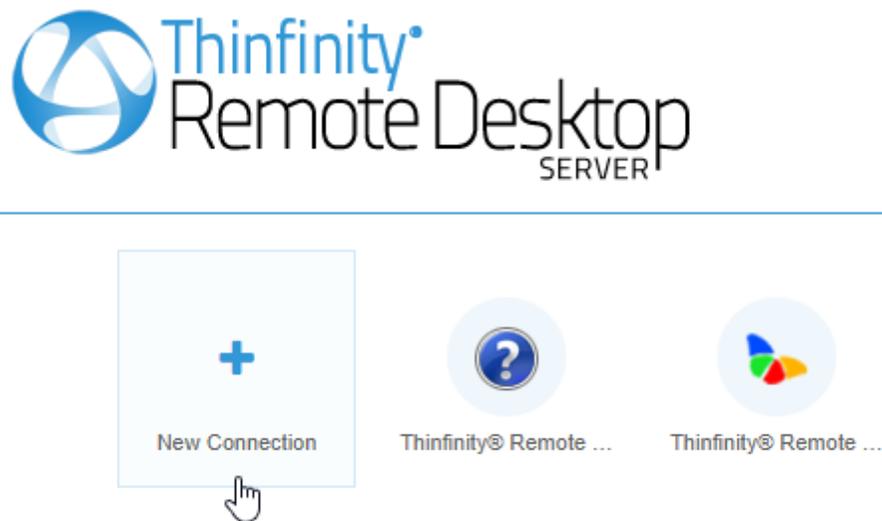
Read more:

- [Connecting to a desktop](#)
- [Connecting to an application](#)
- [Connecting from Mobile Devices](#)
- [Performing a file transfer](#)

7.4.1 Connecting to a Desktop

In order to connect to a remote desktop using Thinfinity® Remote Desktop Server, open a browser and type the Thinfinity® Remote Desktop Server url, which is composed by <https://Server IP:Port>.

1. You will be asked for the application login (user and password). This step may be skipped for some [access security level](#) configuration: if you have the authentication set to [none](#), or the [Allow anonymous access](#) option enabled in all the access profiles, the application will take you directly to the next step.
2. You will be presented with the following screen :



The "New Connection" option represents the Any Computer profile: it enables the user to type the remote computer's IP and credentials, and configure the connection.

General	Display	Resources	Program	Experience	Advanced	-
Computer:	<input type="text" value="192.168.0.52"/>					
Username:	<input type="text" value="MyAdminUser"/>					
Password:	<input type="password"/>					
<input type="button" value="CONNECT"/> <input type="button" value="BACK"/>						

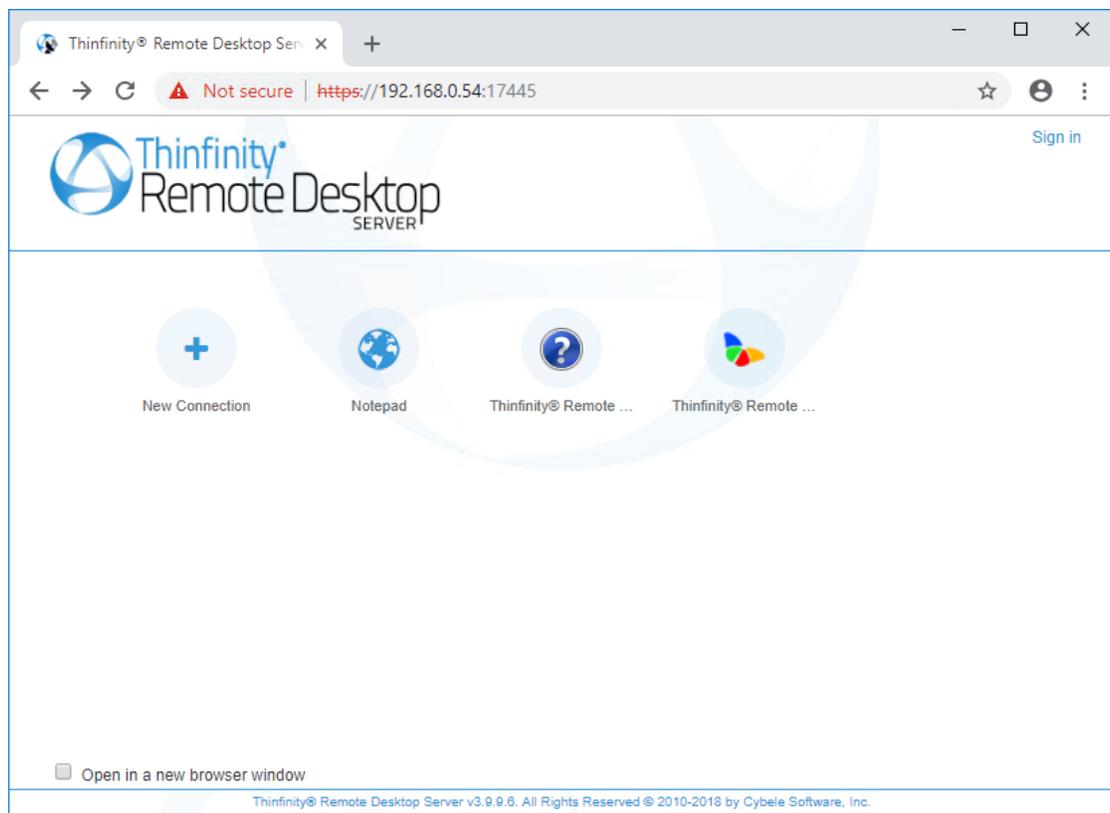
What you see depends on what is available for the authenticated user: When the Any Computer profile is the only one available, you will see that screen. If the Any Computer profile is not available, but you have access to other profiles, you will see the access profiles screen. If the authenticated user has access to both the Any Computer profile and other(s) profile(s), you will see an arrow to the right of the screen. Use it to switch between the Any Computer profile and the other(s).

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

4. Connecting to an Access Profile:

A) Click on the profile you want to connect to.

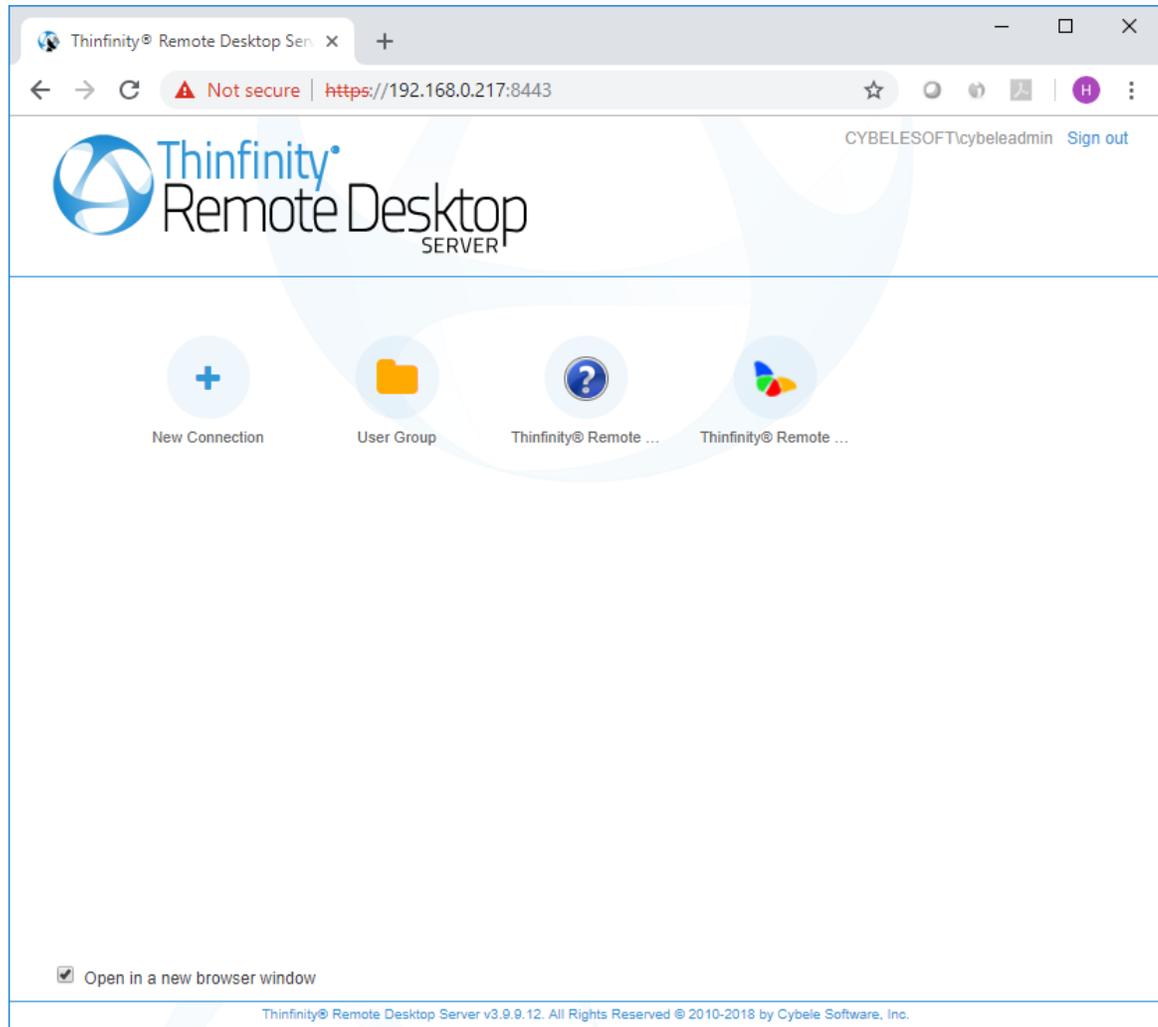
B) You won't be allowed to change the computer's IP or the RDP options at this moment, because these are already set for each profile.



5. Connecting to Any Computer:

- a) If you are in the access profiles page, click on the arrow to the left of the screen to go back to the Any Computer profile.
- 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.
- d) You can also change the RDP options by pressing the plus [+] sign in order to show the settings tabbed interface.
- e) Read more about each option on the [Web Interface Settings](#) section.

Useful information: you can create folders by dragging one profile over the other (only available when you sign in).



Read more:

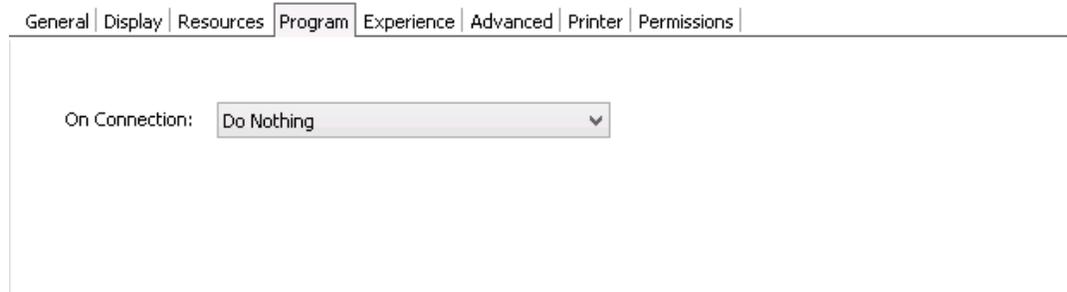
- [Connecting to an application](#)
- [Performing a file transfer](#)

7.4.2 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 access to an application and not to the desktop. This feature will be only available when you connect to remote desktops running on Windows server versions.

Configuring a profile to connect to an application

- a. Go to the [Profiles Editor](#) 'Program' tab.
- b. Set the 'On Connection' field to 'Start a Program' and then specify the path and the executable file to initialize the desired program. For more information regarding these options, read the ['Program' tab](#) topic .



Connecting to an application using the Any Computer profile

- a. Log in to Thinfinity® Remote Desktop Server.
- b. Press the 'Options' button to show the settings tabs.
- c. Go to the 'Program' tab.
- d. Set the 'On Connection' field to 'Start a Program' and then specify the path and the executable file to initialize the desired program. For more information regarding these options, read the ['Program' tab](#) topic.



General Display Resources **Program** Experience Advanced

On Connection:

Do Nothing

CONNECT

BACK

Open in a new browser window

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

Read more:

- [Performing a file transfer](#)

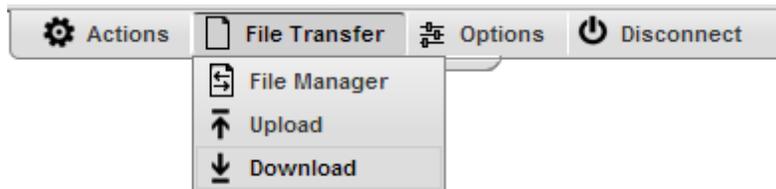
7.4.3 Performing a File Transfer

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.

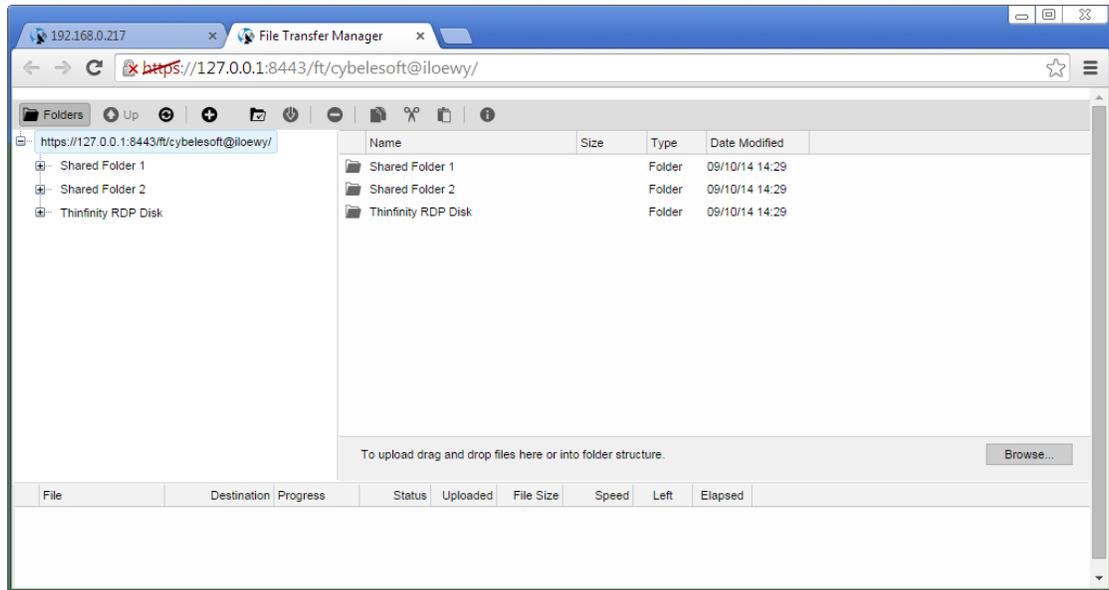


Upload	Click on this option to upload a file located on the local computer into the remote desktop. A window will be opened so that you can select the file to be uploaded.
Download	This option enables you to download any file located inside the Intermediate disk . Select the file on the presented list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



See also, the option to [Automatically download any newly-added file](#).

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



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.

Read more:

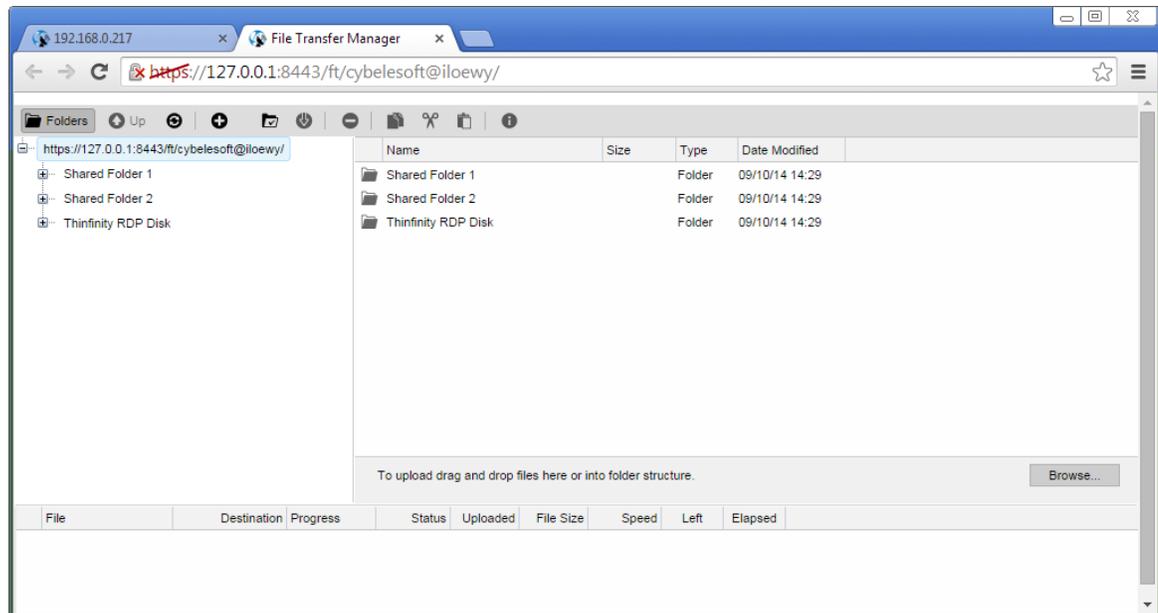
- [Navigating on the File Transfer Screen](#)
- [File Options](#)
- [Remote Folder Area Options](#)
- [Downloading and Uploading Files](#)

7.4.3.1 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.

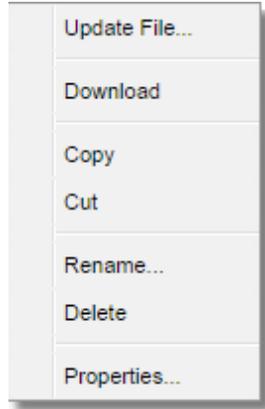


Read more:

- [File Options](#)
- [Remote Folder Area Options](#)
- [Downloading and Uploading Files](#)

7.4.3.2 File Options

Right click on a remote file to access these options:



Find the behaviour for each one of these options below:

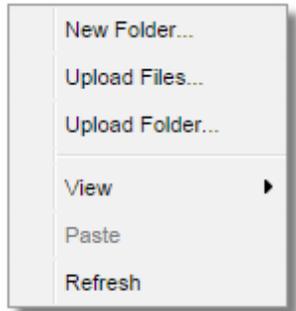
Update File	Choose this option to replace the selected remote file with a local file.
Open/Download	Choose this option to open or download the selected file.
Custom Properties	Choose this option to see the remote file's properties.
Copy	Choose this option to copy the file into the remote clipboard. You 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.

Read more:

- [Remote Folder Area Options](#)
- [Downloading and Uploading Files](#)

7.4.3.3 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.

Read more:

- [Downloading and Uploading Files](#)

7.4.3.4 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.

7.5 Supported RDP Shortcut Keys

The supported shortcut keys in Thinfinity® Remote Desktop Server 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).

8 Advanced Settings

Once you have [configured the basic access](#) for Thinfinity® Remote Desktop Server, you might want to learn a little more about other configuration options.

[Gateways](#)

[Security](#)

[Access Profiles](#)

[Folders](#)

[Permissions](#)

[SSO](#)

[Scaling and Load Balancing](#)

[Custom Settings](#)

[Customizing the toolbar](#)

[Remote FX](#)

[Save Session](#)

[Multi-touch Redirection](#)

[Enhanced Browser and DPI Support](#)

8.1 Thinfinity® Remote Desktop Server Manager

The Thinfinity® Remote Desktop Server Manager is a tool for administrators to set up general settings. You can manage users, profiles, RDP preferences and settings related to the Thinfinity® Remote Desktop Server service.

To access the Thinfinity® Remote Desktop Server manager go over the Start Menu options and look for the "Thinfinty RDP Manager" item.

The Thinfinity® Remote Desktop Server Manager interface is composed by the following tabs:

[Gateways](#)

[Security](#)

[Access Profiles](#)

[Folders](#)

[Permissions](#)

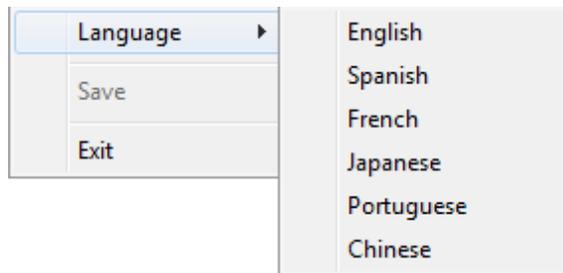
[Gateways](#)

[SSO](#)

[Scaling and Load Balancing](#)

The Thinfinity® Remote Desktop Server Manager main menu consists of two sub-menus:

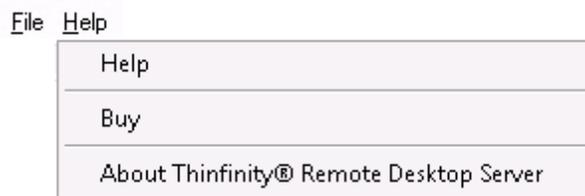
The File Menu:



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 Thinfinity® Remote Desktop Server Manager.

The Help Menu:



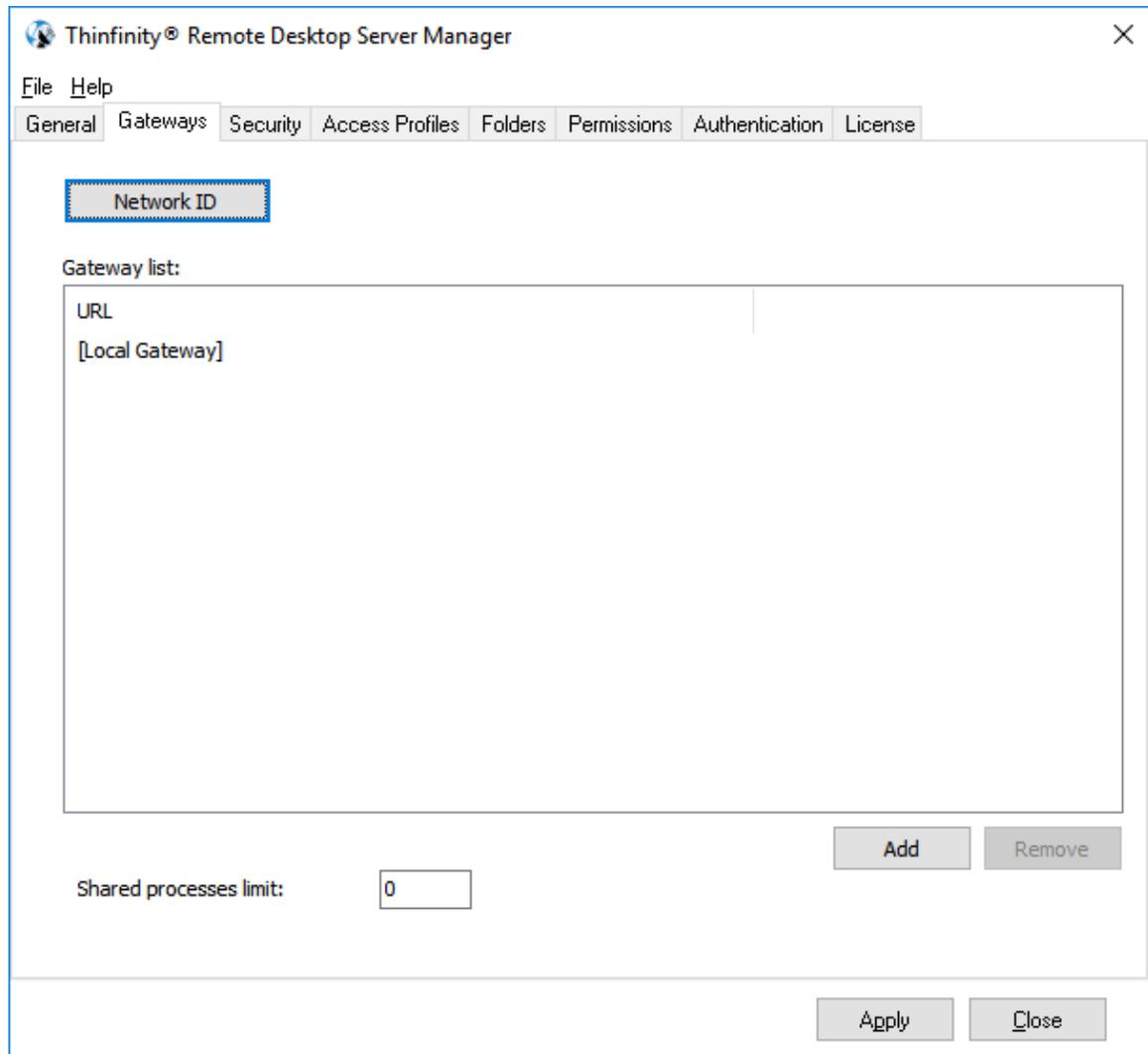
The Help Menu is composed by the following options:

Help	Takes you to the online application Guide.
Buy	Takes you to the Cybele Software Buy page.
About Thinfinity® Remote Desktop Server	Click here to see the application version and build number.

Read more:

- [The 'Security' Tab](#)
- [The 'Access Profiles' Tab](#)
- [The 'Folders' Tab](#)
- [The 'Permissions' Tab](#)
- [The 'Gateways' Tab](#)
- [The 'SSO' Tab](#)
- [Scaling and Load Balancing](#)

8.1.1 Gateways



In the Thinfinity® Remote Desktop Server manager 'Gateways' tab you will find the following options:

<p>Network ID</p>	<p>The network ID identifies this installation. Thinfinity Remote Desktop Servers that want to share their resources through one or more Gateways must match their Network ID.</p> <p>Press this button to see and/or change the Network ID. The default value is a random string but you can change it to something more descriptive.</p>
<p>Gateway List</p>	<p>A list of the gateways that a user can connect to in order to access this server's resources.</p> <p>For a typical installation, with no load balancing architecture,</p>

	leave it blank.
Add	Add a new gateway to the Gateway List. Only if you will use Scaling and Load Balancing .
Remove	Remove a selected gateway from the Gateway List.
Shared Processes Limit	The number of processes that Thinfinity Remote Desktop Server will share for all the user.

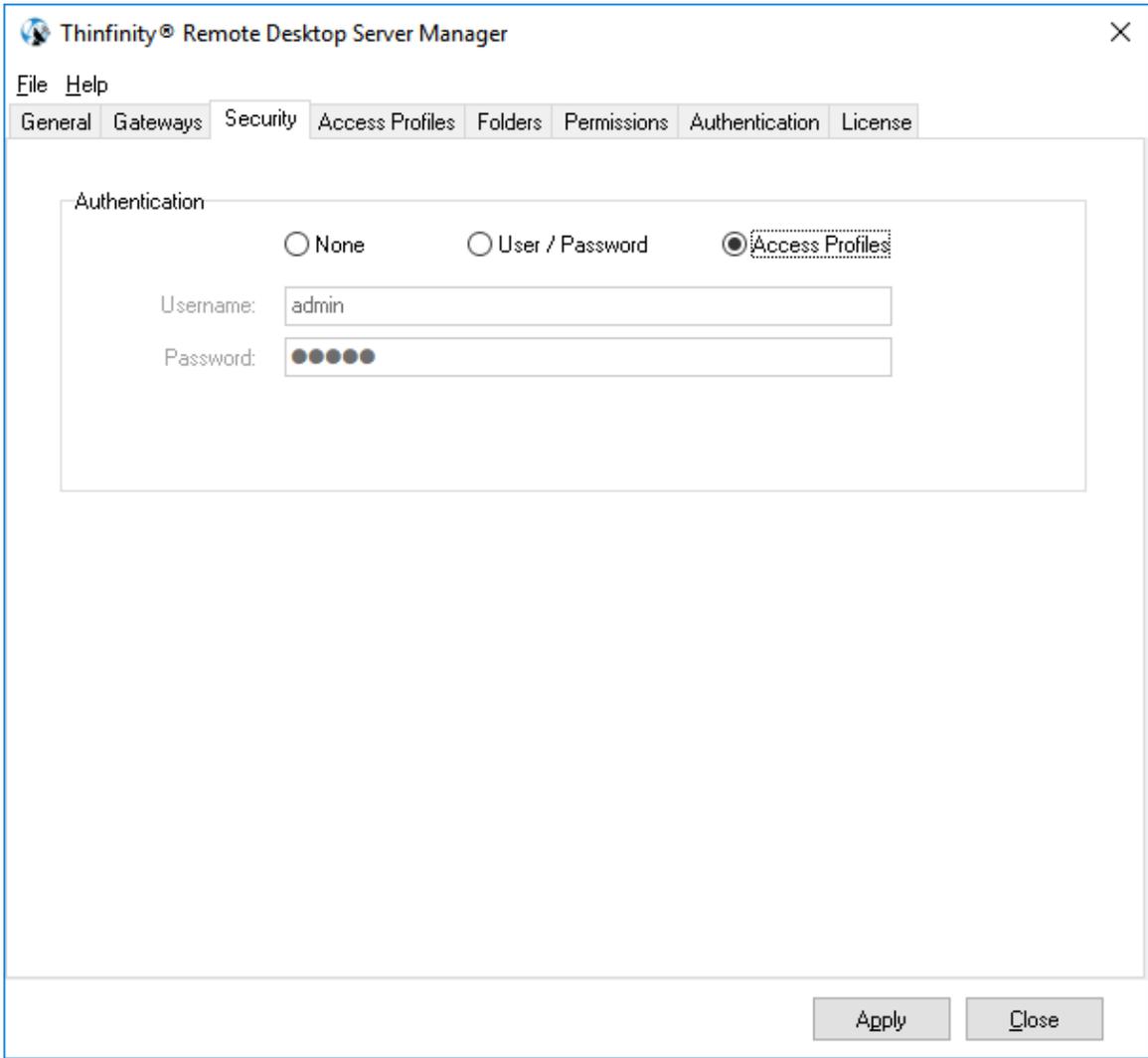
Always remember to press 'Apply' in order to save the changes.

Read more:

- [SSO](#)

8.1.2 Security

In the Thinfinity® Remote Desktop Server manager 'Security' tab you will find the following options:



Authentication	Choose the level of authentication for the users access to Thinfinity® Remote Desktop Server. Users will still need to authenticate afterwards against the computer they connect to.	
	None	No authentication for Thinfinity® Remote Desktop Server access. This is only recommended for exclusive local access.

	<table border="1"> <tr> <td>User / Password</td> <td>Set your own credentials for Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server users.</td> </tr> </table>	User / Password	Set your own credentials for Thinfinity® Remote Desktop Server access authentication.	Access Profiles	Manage the authentication with Active Directory users by creating a profile. Also select this option to enable profiles and set predetermined preferences for the Thinfinity® Remote Desktop Server users.
User / Password	Set your own credentials for Thinfinity® Remote Desktop Server access authentication.				
Access Profiles	Manage the authentication with Active Directory users by creating a profile. Also select this option to enable profiles and set predetermined preferences for the Thinfinity® Remote Desktop Server users.				
Use Standard browser authentication dialog	Check this option to use the standard browser authentication dialog instead of the Thinfinity Remote Desktop Server web login. This option is only available when "Authentication" is set to "Access Profiles". Check it to use the standard browser authentication dialog.				
Only use external authentication	This option is available when "Authentication" is set to "Access Profiles" and you are using SSO . If you leave it unchecked, you will see an option in the Thinfinity® Remote Desktop Server Login Screen to choose the login method. If you check it, the credentials you enter there will be authenticated against your SSO provider.				

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

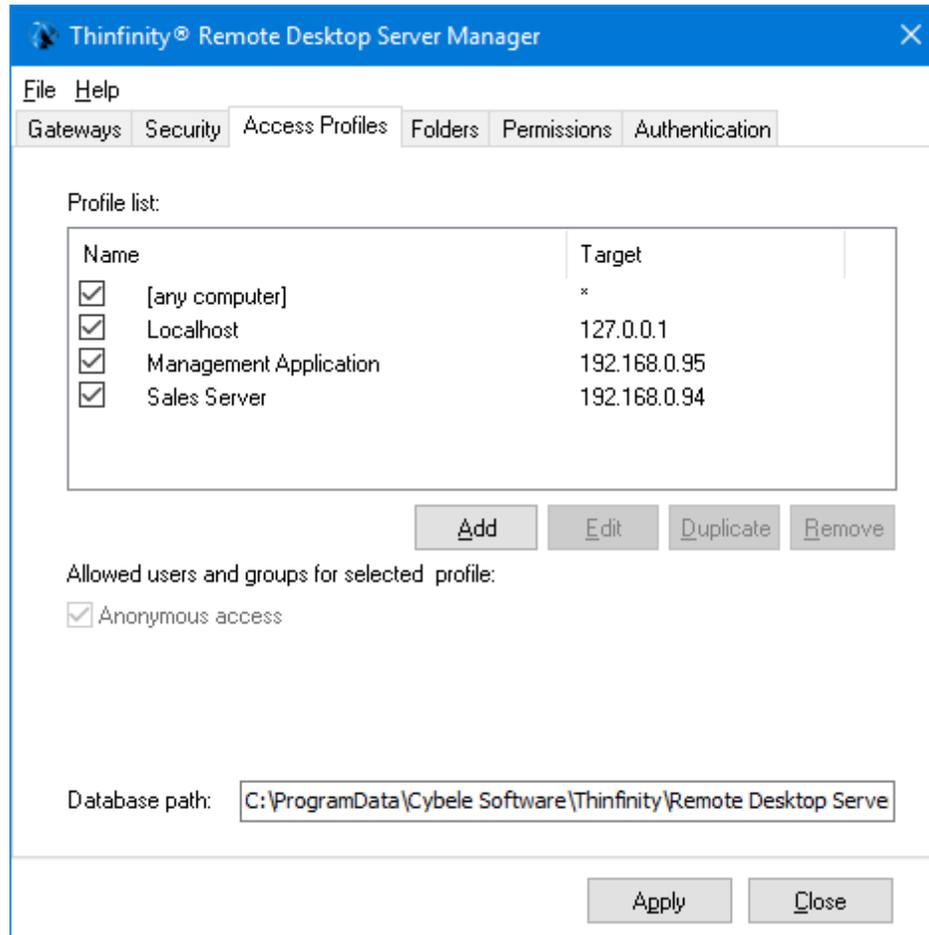
Note: Only when the "Only use external authentication" option in [the "Security" tab](#) is checked and OAuth 2 is the only [SSO](#) method enabled in [the 'SSO' tab](#), a connection to the Thinfinity Remote Desktop landing page or [virtual path](#) will be redirected to the OAuth 2 authentication and then return to the landing page or virtual path.

Read more:

- [The 'Access Profiles' Tab](#)
- [The 'Folders' Tab](#)
- [The 'Permissions' Tab](#)
- [The 'Gateways' Tab](#)
- [The 'SSO' Tab](#)

8.1.3 Access Profiles

The "Access Profiles" tab is only enabled when you choose "Access Profiles" as the authentication option on the [Security tab](#).



In the Thinfinity® Remote Desktop Server manager "Access Profile" tab you will find the following options:

<p>Profile List</p>	<p>This list shows the available profiles. You can enable or disable them by checking the box to the left of the name.</p> <table border="1" data-bbox="613 1566 1192 1797"> <tbody> <tr> <td data-bbox="613 1566 802 1640">Name</td> <td data-bbox="802 1566 1192 1640">Name of the profile.</td> </tr> <tr> <td data-bbox="613 1640 802 1797">Target</td> <td data-bbox="802 1640 1192 1797">The remote desktop IP or host name for RDP profiles and the web address in case of the Web Link profiles.</td> </tr> </tbody> </table>	Name	Name of the profile.	Target	The remote desktop IP or host name for RDP profiles and the web address in case of the Web Link profiles.
Name	Name of the profile.				
Target	The remote desktop IP or host name for RDP profiles and the web address in case of the Web Link profiles.				
<p>Add</p>	<p>Press this button to add a new profile. You can add an RDP Profile, or a Weblink Profile.</p>				

Edit	Select a profile and press this button to edit it. Depending on the profile, you will be directed to the RDP Profile editor , or the Weblink Profile editor .
Remove	Select a profile and press this button to remove it.
Allowed users and groups for selected profile	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.
Database path	When the application is set to work with Load Balancing, you can set a common database path to all Thinfinity® Remote Desktop Server Brokers by informing it on this field.

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

Read More:

- [RDP Profile Editor](#)
- [Web Link Profile Editor](#)
- [RD Web Access Editor](#)
- [The 'Folders' Tab](#)
- [The 'Permissions' Tab](#)
- [The 'Gateways' Tab](#)
- [The 'SSO' Tab](#)

8.1.3.1 RDP Profile Editor

The Profile Editor is the tool to create, configure and edit Thinfinity® Remote Desktop Server Access Profiles.

The first thing you have to consider is if you want to create an RDP Profile, a Web Link profile or an RD Web Access Profile.

These options are represented by the 'RDP Profile'/'Web Link'/'RD Web Access' radio button.

- **An RDP Profile:** is a Thinfinity® Remote Desktop Server connection to a machine or an application.
- **A Web Link profile:** is a link to an external website of your choice, which will be presented along with the profiles to the user. [Read More](#).
- **An RD Web Access:** is an administrator profile to populate Microsoft RD Web Access remote apps and desktops links in the user view. [Read More](#).

This sections explains the RDP Profile Editor, so if you are here and you want to create a Weblink profile, check the 'Web Link' radio button and read about the [Web Link Profile Editor](#) and if you want to create an RD Web Access profile, check the 'RD Web Access' option and read about the [RD Web Access Editor](#).

This is the RDP Profile Editor General tab view:

The screenshot shows the 'Thinfinity® Remote Desktop Server - Profiles Editor' window. The title bar includes the application name and standard window controls. The main area is divided into several sections:

- Name:** A text box containing 'New RDP Profile'.
- Virtual Path:** A text box containing 'New_RDP_Profile'.
- Access Key:** A text box containing 'LTSFAENHVqVSiuwsunLgttPbHrAuJwkIW@bZx4-0eRJzEwV' and a 'New Key' button.
- Icon:** A dropdown menu set to 'None'.
- Profile Type:** Three radio buttons: 'RDP Profile' (selected), 'Web Link', and 'RD Web Access'.

Below these fields is a tabbed interface with the following tabs: 'General', 'Display', 'Resources', 'Program', 'Experience', 'Advanced', 'Printer', and 'Permissions'. The 'General' tab is active, showing:

- Computer:** A text box containing '127.0.0.1'.
- Two checkboxes: 'Connect to a Hyper-V Virtual Machine' and 'Connect to a Virtual Desktop on an RDS Collection', both of which are unchecked.
- Credentials:** A section with three radio buttons: 'Use the authenticated credentials' (selected), 'Ask for new credentials', and 'Use these credentials:'. Below these are two text boxes for 'User name:' and 'Password:'.

At the bottom right of the window are 'Ok' and 'Cancel' buttons.

These are the profile properties you can edit:

Name	Use this field to change the profile name. The profile name is shown to users to identify the connection.
Virtual Path	The Virtual Path will create a unique URL address for this connection. The complete path will consist of: <code>http(s)://ThinfinityRDPDomain:port/VirtualPath/</code> . The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Desktop Server web interface.
Access Key	Used in combination with Thinfinity® Remote Desktop Server 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 icon image for the profile. This image will be shown with the profile name to the authenticated user in the web interface.
Web link / RDP Profile/ RD Web Access	Select the 'RDP Profile' option to have a regular profile that connects to a remote machine or application through RDP. Select the 'Web Link' option to make this profile a link to an external web site (read about the Weblink Profile Editor). Select the 'RD Web Access' option to pull the RD Web Access Windows connections into the web interface (read about the RD Web Access Editor).

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

Read More:

- [General](#)
- [Display](#)
- [Resources](#)
- [Program](#)
- [Experience](#)
- [Advanced](#)
- [Printer](#)
- [Permissions](#)
- [Web Link Profile Editor](#)
- [RD Web Access Editor](#)
- [Folders](#)

8.1.3.1.1 General

In the Thinfinity® Remote Desktop Server profiles editor "General" tab you will find these following options:

<p>Computer</p>	<p>Specify the computer that this profile will connect to. Enter the internal IP or computer name.</p>				
<p>Connect to a Hyper-V Virtual Machine</p>	<p>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.</p>				
<p>Connect to a Virtual Desktop on an RDS Collection</p>	<p>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.</p>				
<p>Credentials</p>	<p>Choose the credentials for logging into the specified computer:</p> <table border="1" data-bbox="651 1524 1469 1900"> <tr> <td data-bbox="651 1524 911 1801"> <p>Use the authenticated credentials</p> </td> <td data-bbox="911 1524 1469 1801"> <p>Use the same credentials entered in the browser for Thinfinity® Remote Desktop Server (specified 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 Thinfinity® Remote Desktop Server if this is the only profile for their credentials</p> </td> </tr> <tr> <td data-bbox="651 1801 911 1900"> <p>Ask for new credentials</p> </td> <td data-bbox="911 1801 1469 1900"> <p>Prompt the user for new credentials to access the computer.</p> </td> </tr> </table>	<p>Use the authenticated credentials</p>	<p>Use the same credentials entered in the browser for Thinfinity® Remote Desktop Server (specified 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 Thinfinity® Remote Desktop Server if this is the only profile for their credentials</p>	<p>Ask for new credentials</p>	<p>Prompt the user for new credentials to access the computer.</p>
<p>Use the authenticated credentials</p>	<p>Use the same credentials entered in the browser for Thinfinity® Remote Desktop Server (specified 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 Thinfinity® Remote Desktop Server if this is the only profile for their credentials</p>				
<p>Ask for new credentials</p>	<p>Prompt the user for new credentials to access the computer.</p>				

	<p>Use these credentials</p>	<p>Complete the credentials used to access the computer.</p> <p>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 Thinfinity® Remote Desktop Server if this is the only profile for their credentials</p>
--	------------------------------	---



See also, the [credentials behavior when using the One-Time-URL](#).

Read More:

- [Setting up a Hyper-V Profile](#)
- [Setting up an RDS Collection Profile](#)
- [Display](#)
- [Resources](#)
- [Program](#)
- [Experience](#)
- [Advanced](#)
- [Printer](#)
- [Permissions](#)

8.1.3.1.1.1 Setting up a Hyper-V Profile

When you can't access your Hyper-V Virtual Machine through a direct IP address or computer name, or you want to protect this virtual machine location, 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.

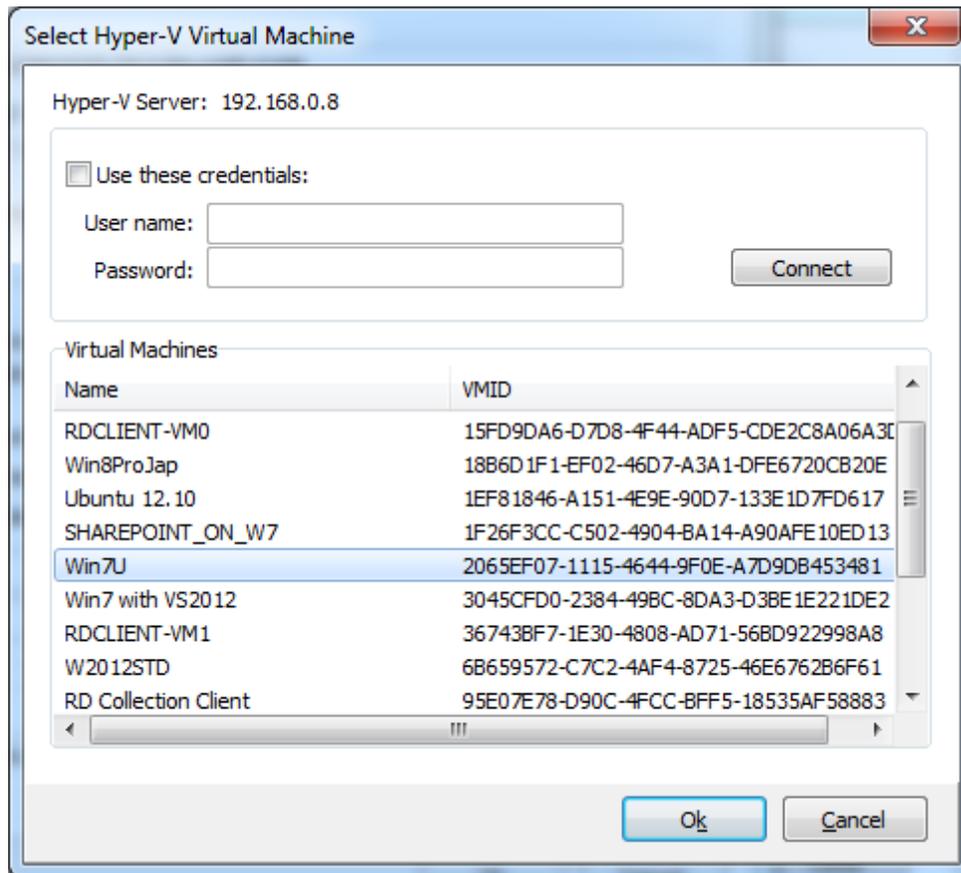
The screenshot shows the 'Profiles Editor' window with the following fields and options:

- Name:** New RDP Profile
- Virtual Path:** New_RDP_Profile
- Access Key:** LrTseBG4Id5Y4mX1Yc@3r7aEL-QfkKuwV0k-fd5A5pKfCj-q (with a 'New Key' button)
- Icon:** A blue square icon.
- Profile Type:** RDP Profile, Web Link, RD Web Access
- General Tab:**
 - Computer:** 192.168.0.8
 - Connect to a Hyper-V Virtual Machine
 - Connect to a Virtual Desktop on an RDS Collection
 - Credentials:**
 - Use the authenticated credentials
 - Ask for new credentials
 - Use these credentials:
 - User name:** [Empty field]
 - Password:** [Empty field]
 - Virtual machine:** 123CFF37-752D-45C6-828C-43100FE0D90F (with a 'Browse...' button)

3. Check the option "Connect to a Hyper-V" Virtual Machine.
4. Complete the 'Credentials', necessary to authenticate against the Hyper-V Virtual Machine.
5. If you know the Virtual Machine ID (GUID), you can inform it on the field "Virtual machine id" and skip 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.



6b. If the Hyper-V Server requires authentication you can enter the credentials on the "Use these credentials" box, and then 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 'OK' and then 'Apply'.

8.1.3.1.1.2 Setting up an RDS Collection Profile

When you need to connect to an 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.

Thinfinity Remote Desktop Server - Profiles Editor

Name: My RDS Collection VM Profile

Virtual Path: My_RDS_Collection_VM_Profile

Access Key: xU3VePa3ykrZ8rnXURdLq1rLELoPI9ZPPjK0WMA4k7g8Rrys New Key

Icon: RDP Profile Web Link RD Web Access

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 an RDS Collection

Credentials:

Use the authenticated credentials

Ask for new credentials

Use these credentials:

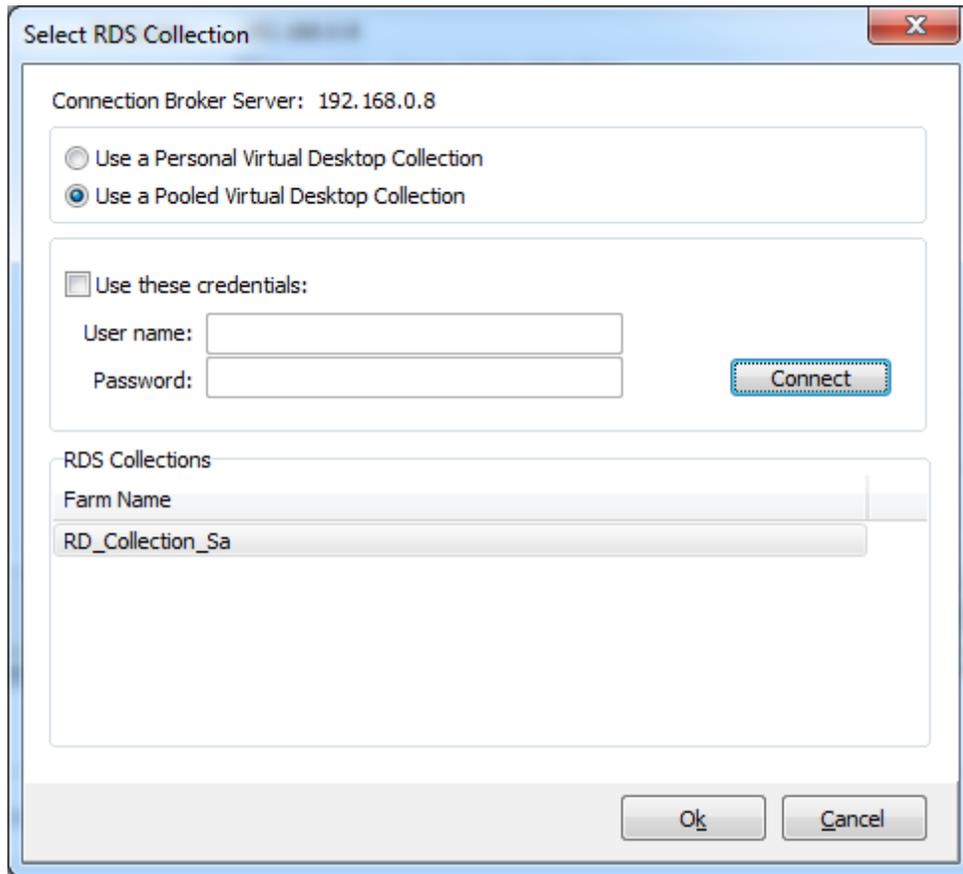
User name:

Password:

RDS Collection: TSV://VMResource.1.RD_Collection-Sa Browse...

Ok Cancel

3. Check the option "Connect to a Virtual Desktop on an RDS Collection".
4. Complete the 'Credentials' fields to authenticate against the virtual machine.
5. If you know the URL to the Terminal Service VM Host Agent (the URL follows this format `tsv://VMResource.1.RD_Collection_Sa`), you can inform it on the 'TSV URL' field and skip the next step.
6. If you don't know the TSV URL, click on the 'Browse' button and the following search dialog will be presented:



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

6b. Click on the Connect button. If necessary, inform the credentials to 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.

8.1.3.1.2 Display

General | **Display** | Resources | Program | Experience | Advanced | Printer | Permissions

Color Depth: True color (16bit) ▼

Resolution: Fit to browser window ▼

Image Quality: Optimum ▼

In the Thinfinity® Remote Desktop Server profiles editor "Display" tab you will find the following options:

Color Depth	Choose the color depth for the remote computer view. If Remote FX is enabled, the color depth will be set to 32bit regardless of what is stated in this field. Read more about the conditions under which Remote FX will be enabled.
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	<p>The connection image quality is very related with the application performance (higher quality=lower performance).</p> <p>The default Image quality is Optimum, because it presents the best cost benefit relationship between quality and performance. If you need to have more quality or better performance, take a look at the other options below:</p> <p>Highest - Uses PNG images only (0% compression)</p> <p>Optimum - Combines PNG and JPEG images (20% compression).</p> <p>Good - Uses JPEG images only (40% compression)</p> <p>Fastest - Uses JPEG images only (50% compression).</p>

Read More:

- [Resources](#)

- [Program](#)
- [Experience](#)
- [Advanced](#)
- [Printer](#)
- [Permissions](#)

8.1.3.1.3 Resources

General | Display | **Resources** | Program | Experience | Advanced | Printer | Permissions

Enable Clipboard

Enable Intermediate Disk

Disk name:

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

Automatically download any newly-added file

Enable Sound

Sound quality:

In the Thinfinity® Remote Desktop Server profiles editor "Resources" tab you will find the following options:

Enable Clipboard	Check 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, Thinfinity® Remote Desktop Server will automatically download any file saved or copied in the Intermediate disk direction. Files with the format *.tmp y ~\$*. * are excluded by default. Exclude different files from this download by configuring the ini file (see below).
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 the quality that Thinfinity® Remote Desktop Server will use to reproduce the remote sound. The highest the quality, the most resources will be required.

The Thinfinity.RemoteDesktop.Server.ini configuration file location depends on the Windows version Thinfinity® Remote Desktop Server is running at:

```
C:\ProgramData\Cybele Software\Thinfinity\Remote Desktop Server
\Thinfinity.RemoteDesktop.Server.ini
or
C:\Documents and Settings\All Users\Application Data\Cybele Software\Thinfinity\Remote
Desktop Server\Thinfinity.RemoteDesktop.Server.ini (older Windows versions)
```

Inside the ini file, create an [AutoDownload] section and use the 'Exclusion' key with the values that you want to exclude using Glob Expression Syntax (standard DOS mode), separated by the "|" char. You can also use the regular expression notation to indicate which files to exclude, except for the single pipe character, which is reserved for Thinfinity® Remote Desktop Server to notice separation between exclusion rules. Use the double pipe character, instead, within the regex for the "or" operator.

Take a look at the following example. Notice the use of ":" at the beginning of the jpg exclusion rule and the double pipe to note that files starting with the letter a or the letter b will be excluded.

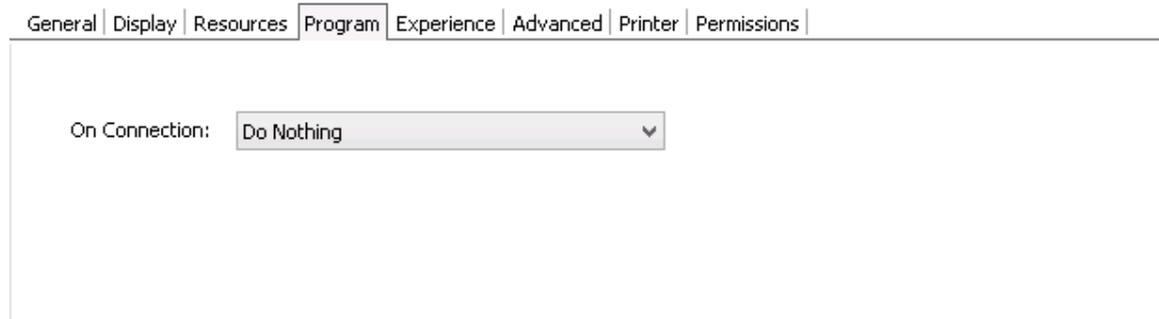
```
[AutoDownload]
Exclusion=*.tmp|~$*.*|^.*\.*.jpg$|^[a|b].*$
```

Read More:

- [Program](#)
- [Experience](#)
- [Advanced](#)
- [Printer](#)
- [Permissions](#)

8.1.3.1.4 Program

In this tab you can configure the connection to open a specific application. The "Do nothing" option is selected by default. This option will show the whole remote desktop.



General | Display | Resources | **Program** | Experience | Advanced | Printer | Permissions

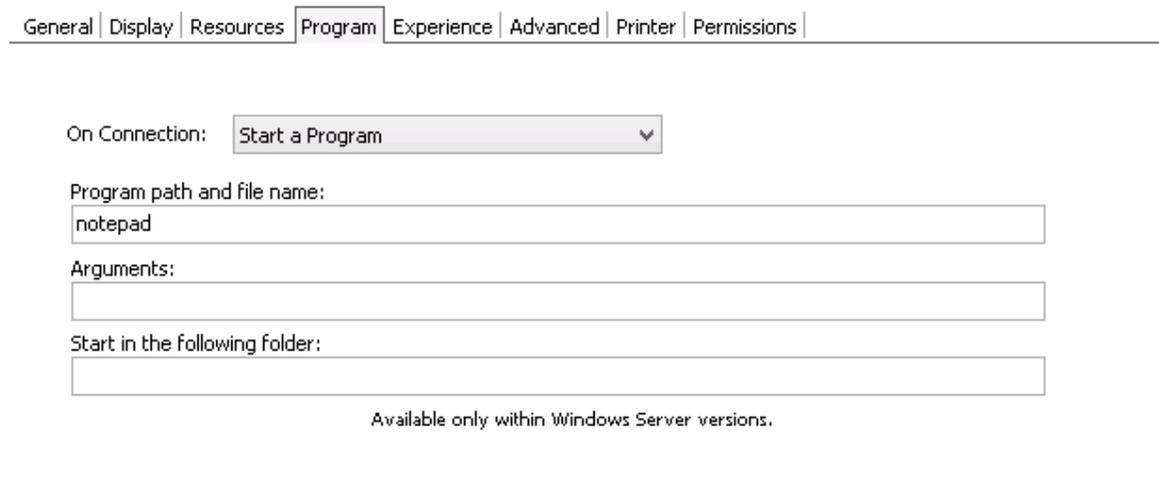
On Connection: Do Nothing

Start a Program option:

If you want to set a specific application to start with the connection, select the "Start a Program" option.

Once you close the program, the remote session will get disconnected.

This feature is only available within Windows Server versions.



General | Display | Resources | **Program** | Experience | Advanced | Printer | Permissions

On Connection: Start a Program

Program path and file name:
notepad

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:

<p>Program path and file name</p>	<p>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.</p>
---	--

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 Thinfinity® Remote Desktop Server, by selecting the "Launch RemoteApp" on the Program tab. This feature is only available within Windows Server versions.

General | Display | Resources | **Program** | Experience | Advanced | Printer | Permissions

On Connection: Execute as RemoteApp ▼

Program path and file name:

Arguments:

Start in the following folder:

Available only within Windows Server versions.

Show Windows Login and Logout Screen

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"
Show Windows Login and Logout Screen	Toggles the visibility of the Windows login and logout screens, which are shown during connection to a desktop or a remote application and show, for example, the username that's being logging in or out.

Read More:

- [Experience](#)
- [Advanced](#)
- [Printer](#)
- [Permissions](#)

8.1.3.1.5 Experience

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

Browser:

Smart sizing

Input:

Multitouch redirection

Graphics:

RemoteFX

Desktop background

Visual styles

Menu and window animation

Font smoothing

Show window contents while dragging

Desktop Composition

In the Thinfinity® Remote Desktop Server profiles editor 'Program' tab you will find the following options:

Smart Sizing	Check this option to scale the connection image. The maximum size of the connection will be the original desktop size.
RemoteFX	Check this option to enable RemoteFX. Read More about Remote FX . This option affects other settings.
Desktop Background	Check this option to show the desktop background.
Visual Styles	Check this option to show Windows Visual Styles: the appearance of common controls, colors, borders, 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.

Read More:

- [Advanced](#)
- [Printer](#)
- [Permissions](#)

8.1.3.1.6 Advanced

General | Display | Resources | Program | Experience | **Advanced** | Printer | Permissions

Unicode keyboard

Keyboard layout: Spanish

Connect to console session

Disable NLA login

Websocket compression

Record remote desktop session

Touch Behavior:

Drag to relative mouse movements

Touch to hold delay: milliseconds

Minimum drag distance: pixels

In the Thinfinity® Remote Desktop Server profiles editor "Advanced" tab will find the following options:

Unicode Keyboard	Uncheck this option to connect to Unix computers through xRDP.
Keyboard Layout	Choose the keyboard layout for the remote computer.
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.
Disable NLA login	Check this to skip NLA as the default login and have the authentication done by an alternative method.
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.
Record Remote Desktop Session	Enable to record the remote desktop session when connecting to this profile. Read more about the Save Session feature.
Drag to 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 when dragging.

	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.
Touch to hold delay	Specify time in milliseconds that you need to hold a touch until you can drag.
Minimum drag distance	Specify maximum distance in pixels that you can move the finger and have it be considered a touch instead of a drag movement.

Read More:

- [Printer](#)
- [Permissions](#)

8.1.3.1.7 Printer

General | Display | Resources | Program | Experience | Advanced | **Printer** | Permissions

Enable a Remote Printer

Printer name:

PostScript printer driver:

Set as default printer

On this tab you can configure the Thinfinity® Remote Desktop Server PDF Printer. These are the options you will find in the Thinfinity® Remote Desktop Server profiles editor "Printer" tab:

Enable a Remote Printer	Uncheck this option to disable Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server in order to print the remote documents. The " <i>HP Color Laser Jet 2800 Series PS</i> " driver is compatible with 2008 Windows versions. The " <i>HP Color LaserJet 8500 PS</i> " driver is compatible with 2003 Windows versions. The " <i>Microsoft XPS Document Writer V4</i> " 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 Thinfinity® Remote Desktop Server printer the remote machine default printer.

Read More:

- [Permissions](#)

8.1.3.1.8 Permissions

General | Display | Resources | Program | Experience | Advanced | Printer | **Permissions**

Allow anonymous access

Group or user names:

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 in the Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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.

Read more:

- [Web Link Profile Editor](#)

8.1.3.2 Web Link Profile Editor

The Web Link Profile Editor is the tool to create, configure and edit Thinfinity® Remote Desktop Server Web Links.

The first thing you have to consider is if you want to create an RDP Profile, a Web Link profile or an RD Web Access Profile.

These options are represented by the 'RDP Profile'/'Web Link'/'RD Web Access' radio button.

- **An RDP Profile:** is a Thinfinity® Remote Desktop Server connection to a machine or an application. [Read More.](#)

- **A Web Link profile:** is a link to an external website of your choice, which will be presented along with the profiles to the user.

- **An RD Web Access:** is an administrator profile to populate Microsoft RD Web Access remote apps and desktops links in the user view. [Read More.](#)

This sections explains the Web Link Profile Editor, so if you are here and you want to create an RDP Profile, check the 'RDP Profile' radio button and read about the [RDP Profile Editor](#) and if you want to create an RD Web Access profile, check the 'RD Web Access' option and read about the [RD Web Access Editor](#).

Thinfinity® Remote Desktop Server - Profiles Editor

Name:

Virtual Path:

Access Key:

Icon:  RDP Profile Web Link RD Web Access

Web Link | Permissions

Web URL:

These are the profile properties you can edit:

Name	Use this field to change the profile name.
Virtual Path	This field is not applicable for Web Link profiles.
Access Key	Used in combination with Thinfinity® Remote Desktop Server 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/ RD Web Access	Select the 'RDP Profile' option to have a regular profile that connects to a remote machine or application through RDP (read about the RDP Profile Editor). Select the 'Web Link' option to make this profile a link to an external web site. Select the 'RD Web Access' option to pull the RD Web Access Windows connections into the web interface (read about the RD Web Access Editor).

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

- [Web Link section](#)
- [Weblink permissions section](#).

8.1.3.2.1 Web Link



The screenshot shows a web interface with two tabs: "Web Link" and "Permissions". The "Web Link" tab is active. Below the tabs, there is a "Web URL" label followed by a text input field containing the URL "http://www.cybelesoft.com". To the right of the input field is a button labeled "Get Icon".

In the Thinfinity® Remote Desktop Server Web Link Profile Editor "Web Link" tab you will find the following options:

Web URL	Enter here the URL of the web page you want this profile to link to.
Get Icon	Press this button to get the web page icon directly from the URL entered in the 'Web URL' field. This icon will replace the Icon set in the 'Icon' option above. To change it back, press on the icon. Read more.

8.1.3.2.2 Permissions

Select the users that will be allowed to access this profile. If you don't select any users, this profile will not be accessed.

General | Display | Resources | Program | Experience | Advanced | Printer | **Permissions**

Allow anonymous access

Group or user names:

These are the options you will find on the Thinfinity® Remote Desktop Server's 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 Thinfinity® Remote Desktop Server 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 from the available profiles.

8.1.3.3 RD Web Access Editor

The RD Web Access Editor is the tool to create, configure and edit Thinfinity® Remote Desktop Server RD Web Access.

The first thing you have to consider is if you want to create an RDP Profile, a Web Link profile or an RD Web Access Profile.

These options are represented by the 'RDP Profile'/'Web Link'/'RD Web Access' radio button.

- **An RDP Profile:** is a Thinfinity® Remote Desktop Server connection to a machine or an application. [Read More.](#)

- **A Web Link profile:** is a link to an external website of your choice, which will be presented along with the profiles to the user. [Read More.](#)

- **An RD Web Access:** is an administrator profile to populate Microsoft RD Web Access remote apps and desktops links in the user view.

This sections explains the RD Web Access Editor, so if you are here and you want to create an RDP Profile, check the 'RDP Profile' radio button and read about the [RDP Profile Editor](#) and if you want to create a Weblink profile, check the 'Web Link' radio button and read about the [Web Link Profile Editor](#).

Thinfinity® Remote Desktop Server - Profiles Editor

Name: RDWebAccessServer

Virtual Path: RDWebAccessServer

Access Key: COa4VNx8KIKNGAeRy\$ISK9nhKw-yt8BbNkRlQjHuwqJw9g@K New Key

Icon:

RDP Profile Web Link RD Web Access

General | Permissions

RD Web URL:

Credentials:

Use the authenticated credentials

Use these credentials:

User name:

Password:

Ok Cancel

These are the profile properties you can edit:

Name	Use this field to change the profile name.
Virtual Path	The Virtual Path will create a unique URL address for this connection. The complete path will consist of: http(s)://ThinfinityRDPDomain:port/VirtualPath/. The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Desktop Server web interface.
Access Key	Used in combination with Thinfinity® Remote Desktop Server 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/ RD Web Access	Select the 'RDP Profile' option to have a regular profile that connects to a remote machine or application through RDP (read about the RDP Profile Editor). Select the 'Web Link' option to make this profile a link to an external web site (read about the Weblink Profile Editor). Select the 'RD Web Access' option to pull the RD Web Access Windows connections into the web interface.

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

- [The 'General' Tab](#)
- [The 'Permissions' Tab](#)

8.1.3.3.1 General

In the Thinfinity® Remote Desktop Server RD Web Access Editor 'General' tab you will find the following options:

General | Permissions

RD Web URL:

Credentials:

Use the authenticated credentials

Use these credentials:

User name:

Password:

RD Web URL	Enter here the Microsoft RD Web Access URL. Typically, it follows this format: https://ServerIp/rdweb	
Credentials	Specify the RD Web Access credentials.	
	Use the authenticated credentials	Use the same credentials entered in the browser for Thinfinity® Remote Desktop Server (specify the "Permissions" tab).
	Use these credentials	Complete the credentials for RD Web Access.

8.1.3.3.2 Permissions

Select the users that will access the connections in this computer's RD Web Access. If you don't select any users, those connections will not be accessed.

General | Display | Resources | Program | Experience | Advanced | Printer | **Permissions**

Allow anonymous access

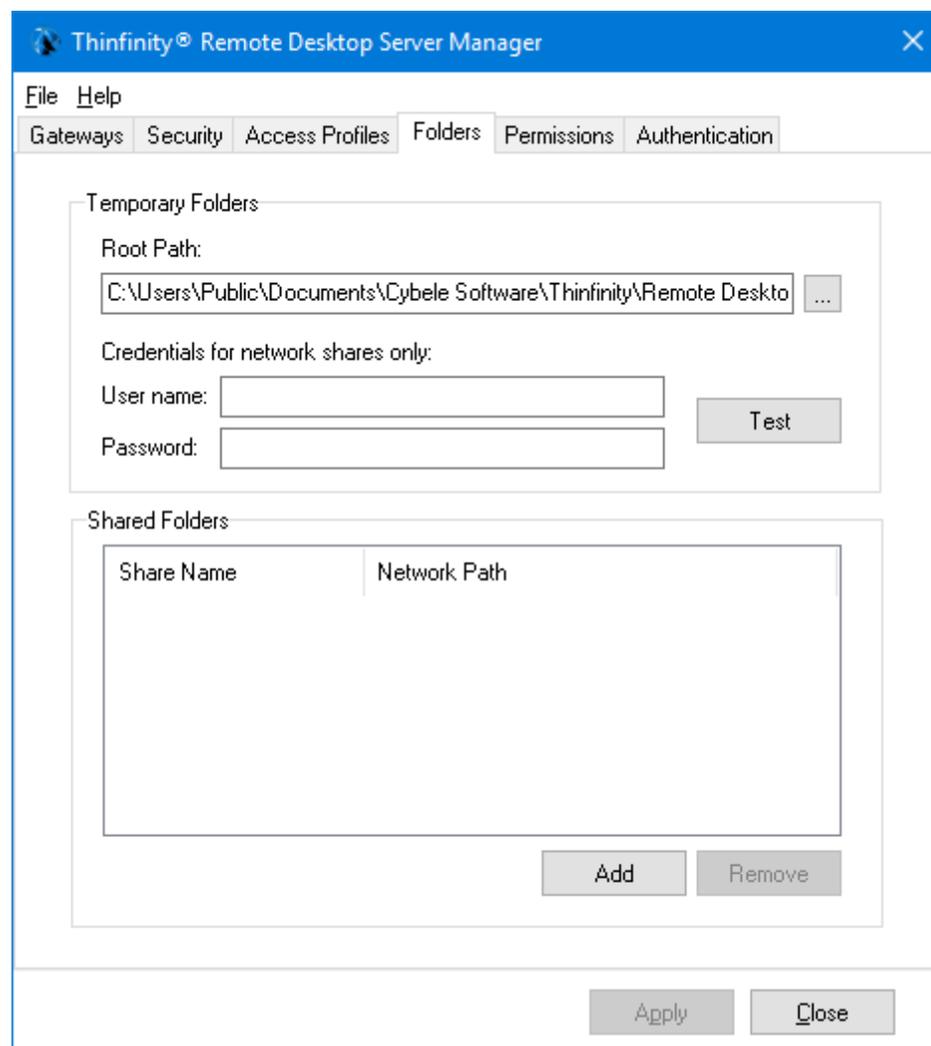
Group or user names:

These are the options you will find in the Thinfinity® Remote Desktop Server RD Web Access editor 'Permissions' tab:

Allow anonymous access	Check this option to make the RD Web Access connections available without any authentication. Use this option if you want the RD Web Access connections to be available for everyone. This means that everybody accessing Thinfinity® Remote
------------------------	--

	Desktop Server will see those connections. 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.

8.1.4 Folders

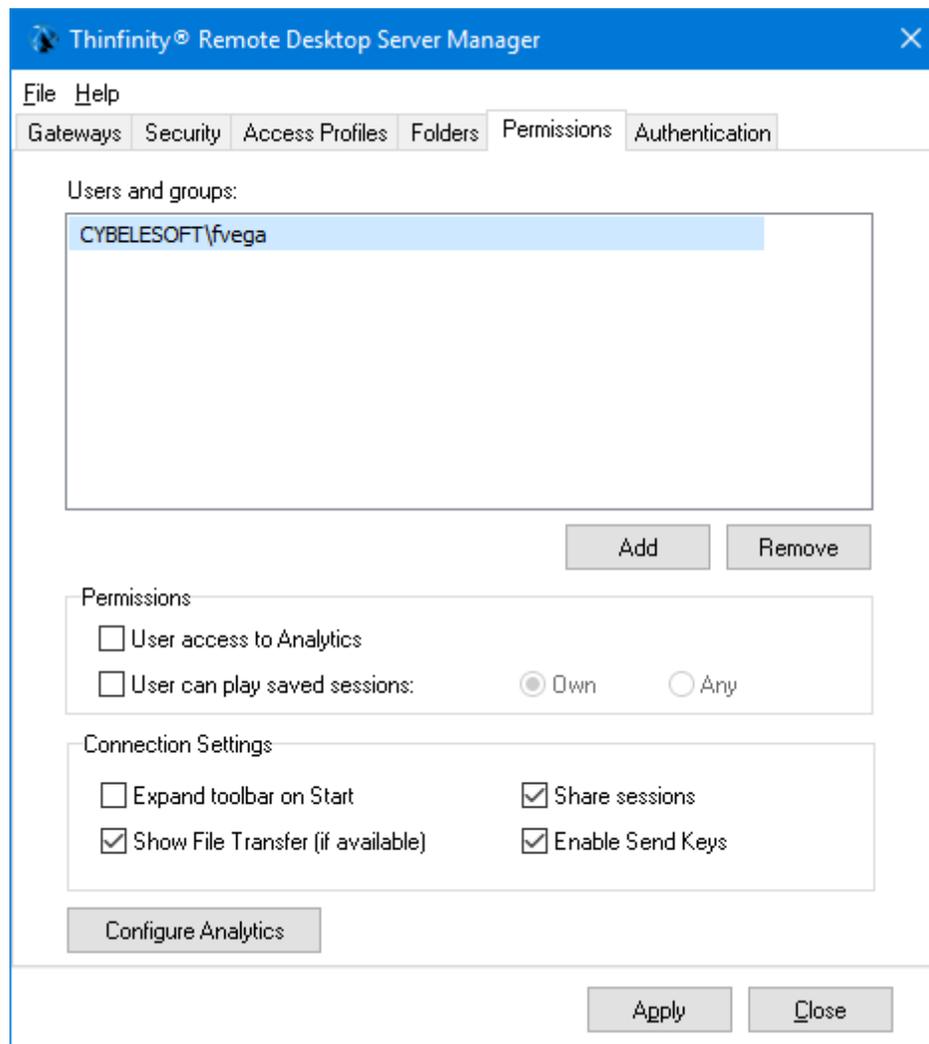


In the Thinfinitiy Remote Desktop Server manager 'Folders' tab you will find the following options:

<p>Temporary Folders (root path)</p>	<p>The temporary folders are used to keep temporary files such as:</p> <ul style="list-style-type: none">- Printed documents- Files uploaded from the remote machine- Files copied into the mapped intermediate disks <p>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.</p>
<p>Credentials for network shares only</p>	<p>The Windows credentials you want to use when authenticating to the network temporary folder.</p> <p>You can check those credentials with the "Test" button.</p>
<p>Shared Folders</p>	<p>A Shared Folder is a directory that will be set as one mapped disk inside the remote desktop connection. They are accessible by all Thinfinity® Remote Desktop Server users/profiles as a disk in the remote connection and also as a File Transfer location.</p> <p>Add: Click on the 'Add' button and inform the directory to be shared, in order to create a new shared folder.</p> <p>Remove: Select an existing folder and click on the 'Remove' button.</p>

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

8.1.5 Permissions

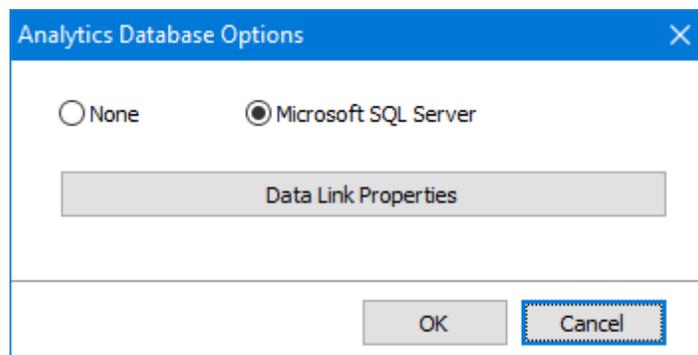


In the Thinfinity® Remote Desktop Server manager 'Permissions' tab you will find the following options:

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.

User can play saved sessions	Check this option to enable users to see remote sessions that have been recorded. Read more about Saved Sessions .
Own / Any	If the 'User can play saved sessions' option is checked, choose to allow the use to see any recorded sessions or only those recorded by themselves. Read more about Saved Sessions .
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 available)	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.
Enable Send Keys	Uncheck to remove the Send Keys options from the Thinfinity® Remote Desktop Server toolbar.
Configure Analytics	Press this button to access the Analytics Database Options.

Access this options dialog by pressing the 'Configure Analytics' button.



None / Microsoft SQL Server	Set this option to 'None' to use Thinfinity Remote Desktop Server's database format as backend for Analytics . Set this option to 'Microsoft SQL Server' to use MS SQL Server as backend for Analytics .
Data Link Properties	This button is only enabled when 'Microsoft SQL Server' is selected. Press this button to access the Microsoft SQL Server Data Link Properties.

	Learn how to configure MS SQL Server as backend .
--	---

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

8.1.6 Authentication

In 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.

Choose between OAuth/2, RADIUS, DUO or SAML using the buttons on the Authentication tab.

Read more:

- [More information about Single Sign On](#)
- [OAuth/2](#)
- [RADIUS](#)
- [DUO](#)
- [SAML](#)

8.1.6.1 OAuth/2

Thinfinity® Remote Desktop Server authentication can be integrated with Google OAuth 2.0 or a custom OAuth 2.0 server. Version 4.0 has added support for OpenID Protocol as well. Enable OAuth/2 and complete your client ID and secret in [The 'Methods' tab](#). Click on 'Add', choose the authentication method you desire to configure any other kind of authentication server. Finally, map the external users to Windows users in [The 'Mapping' tab](#).

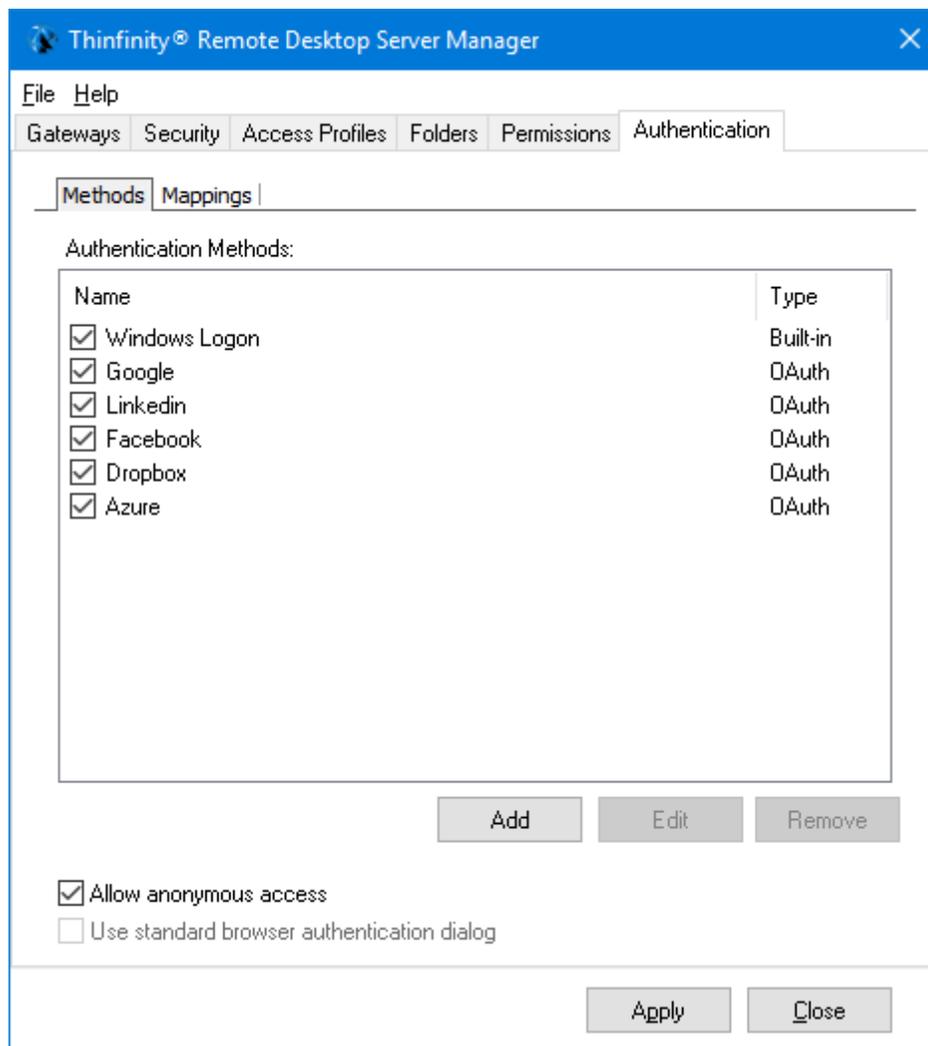
Note: Only when the "Only use external authentication" option in [the "Security" tab](#) is checked and OAuth 2 is the only [SSO](#) method enabled in [the 'SSO' tab](#), a connection to the Thinfinity Remote Desktop landing page or [virtual path](#) will be redirected to the OAuth 2 authentication and then return to the landing page or virtual path.

Read more:

- [More information on OAuth/2 authentication](#)
- [The 'Basic' tab](#)
- [The 'Server' tab](#)
- [The 'Mappings' tab](#)

8.1.6.1.1 Methods

In the 'OAuth/2' - 'Methods' section of the Thinfinity® Remote Desktop Server manager , you will find the following options:



Add	Add an OAuth 2.0 server, a Radius server, or chose a specific .dll , as an authentication method .
Edit	Edit an OAuth 2.0 , Radius , or .dll authentication method
Remove	Remove the specified authentication method
Allow anonymous access	Allows bypassing the login page without the need to authenticate with a valid user

--	--

Built-in configurations for OAuth 2.0 :

- Google
- Facebook
- LinkedIn
- Azure
- Dropbox
- Forgerock

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

Read more:

- [The 'Settings' tab](#)
- [The 'Mapping' tab](#)

8.1.6.1.2 Settings

In the 'OAuth/2' - 'Settings' section of the Thinfinity® Remote Desktop Server manager 'SSO' tab, you will find the following options:

Authentication Method Settings

Name: OAuth

Virtual Path: OAuth

General Server

Client ID:

Client Secret:

Ok Cancel

Authentication Method Settings
✕

Name:

Virtual Path:

General

Server

Authorization URL

Authorization parameters

Token Validation Server URL

Token Validation extra parameters

Profile information server URL Add default parameters

Login username value in returned JSON

General tab

Client ID	<p>This client ID identifies Thinfinity VirtualUI in the OAuth Server.</p> <p>If you are using Google OAuth, it's the Google Client ID generated while configuring the google account integration.</p>
Client Secret	<p>This client secret identifies Thinfinity Remote Desktop Server in the OAuth Server.</p> <p>If you are using Google OAuth, it's the Google Client Secret generated while configuring google the account integration.</p>
Force approval prompt (Google connection only)	<p>If this option is marked, the user will be always prompted to approve the account integrations, when logging into the</p>

	application. This option applies only to Google SSO Integration.
--	--

Server tab

Server Kind	Choose which kind of OAuth/2 Server you will be configuring. Select 'GOOGLE' to use Google OAuth 2.0 authentication, or CUSTOM to enter the parameters of another OAuth 2.0 server.
Authorization URL	This is the OAuth 2.0 server address where Thinfinity Remote Desktop Server validates the corresponding OAuth 2.0 user. This address is used in combination with the values specified in the 'Other Keys...' field.
Parameters (key1=value1&key2=value2&...)	Complete other keys and their values following the query format specified. They will be sent to the authorization URL. Most of the times, the OAuth 2.0 servers require a scope that tells what user information Thinfinity Remote Desktop Server needs access to in order to perform the user validation. The information specified here will be returned in the profile consultation.
Token Validation Server URL	This is the server where the validation code is exchanged for the token that provides access to the user information. The client ID and client secret specified in the 'Basic' tab are sent here.
Profile information server URL	The token received in the Token Validation Server URL is passed onto the Information Server, where the user information is requested. The answer to this request is a JSON object with the user information. This user information is then parsed using the key specified in the 'Login username value at JSON profile' field.
Login username value in returned JSON	Specify here the name of the value returned by the Profile Information Server in the JSON object that represents the user's login username. This value will be used for mapping in the 'Mapping' tab .

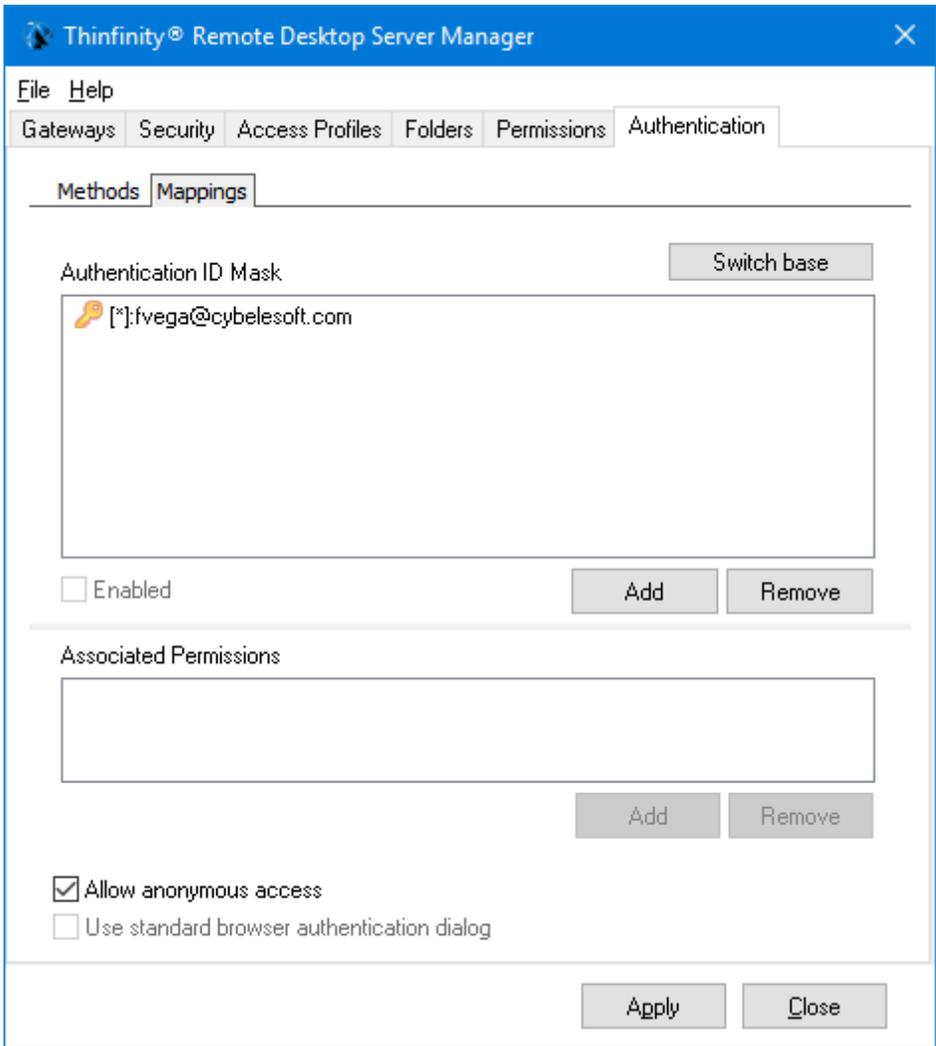
Read more:

- [The 'Methods' tab](#)
- [The 'Mapping' tab](#)

8.1.6.1.3 Mappings

In the 'OAuth/2' - 'Mappings' section of the Thinfinity® Remote Desktop Server manager 'Authentication' tab, you will link your OAuth/2 users to Active Directory users or groups. In this way, you tell Thinfinity Remote Desktop Server that users that authenticate with certain OAuth/2 user are to be shown certain profiles, the profiles that are available for the Active Directory user(s)/group(s) you selected to link them with. That is, to complete this process you have to link the Active Directory user(s)/group in this tab to the Active Directory user(s)/group of the profile you want to enable for a certain OAuth/2 user.

The 'Mappings' tab can be organized in two different ways. By pressing the 'Switch base' button, you select whether you prefer to see a list of Remote Usernames above, that you will map with the Associated User(s)/Group(s) Access below, or a list of Associated User(s)/Group(s) Access that you will map with the Remote Username list below. This doesn't change the way it works, only the way it is shown. You might want to think that a certain remote username has several Active Directory groups it's associated with and thus choose to see the remote users above, or you might prefer to see, for example, a list of Active Directory users and link each of them with several remote users. You can try, and even go back and forth as you add users and decide which way works best for you. Switching the base doesn't change the users and their mapping.



<p>Switch Base</p>	<p>Press to change the order in which the 'Authentication ID Mask and the 'Associated Permissions' boxes will be shown. This doesn't affect the configuration, only the view.</p>
--------------------	---

<p>Authentication ID Mask</p>	<p>List of the remote users.</p> <p>Add: Add a new remote user (SSO). If the 'Authentication ID Mask' box is above the the Associated Permissions box, you will then need to select it and add an Associated Permission to it. Otherwise, if the 'Authentication ID Mask' box is below the 'Associated Permissions' box, the remote user added will be mapped with the Active Directory User selected in the box above.</p> <p>Remove: Select a user and click on the 'Remove' button to take out this remote user from the SSO authentication control, when the 'Authentication ID Mask' box is above the Associated User/ Group Access box. This will also remove the mappings. If the 'Authentication ID Mask' box is below the 'Associated Permissions' box, you will instead remove the user from the mapping with the Active Directory user/group selected above.</p> <p>Enabled: Select an user on the list and uncheck the 'Enabled' field if you want to disable the access of this specific remote user.</p>
<p>Associated Permissions</p>	<p>List of Active Directory Users and Groups.</p> <p>Add: If the 'Associated Permissions' box is above, adds a user to later on select and associate with a remote user. If the Associated Permissions box is below the 'Authentication ID Mask' box, maps this user to the selected remote user above.</p> <p>Remove: If the 'Associated Permissions' box is above, it deletes this user and their mappings from the mapping tab. If the 'Associated Permissions' box is below the 'Authentication ID Mask' box, it disassociates this Active Directory user from the remote user selected above.</p>

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

Read more:

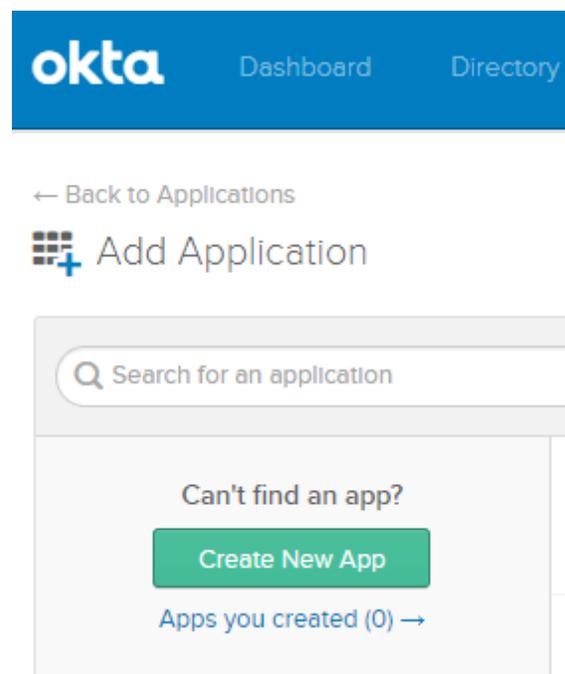
- [The 'Methods' tab](#)
- [The 'Settings' tab](#)

8.1.6.1.4 Configure OAuth with Okta

How to set up multifactor authentication to your environment or virtualized application.

In this quick tutorial, we will show how to properly configure Okta OAuth 2.0 for Thinfinity Remote Desktop Server and Thinfinity VirtualUI.

1) Navigate to your Okta space, go to the Applications tab, and create a new application using the “Create New App” button :



2) Select OpenID Connect as the Authentication Method :

Create a New Application Integration ✕

Platform

Sign on method

Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.

SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

3) Give the application a name, and type in the URL you use to reach Thinfinity. Then press "Save".

Create OpenID Connect Integration

GENERAL SETTINGS

Application name

Application logo (Optional) 

CONFIGURE OPENID CONNECT

Login redirect URIs 

Logout redirect URIs 

4) You should be redirected to the Application Settings. In here, press the “General” button, and edit the “Login information”.

Configure the “Initiate login URI” field, by adding the Thinfinity’s website address and “/Okta” at the end of the URL.

LOGIN

Login redirect URIs 

Logout redirect URIs 

Login initiated by

Initiate login URI

5) Copy and past both Client ID and Client Secret for future references :

Client Credentials Edit

Client ID 

Public Identifier for the client that is required for all OAuth flows.

Client secret  

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

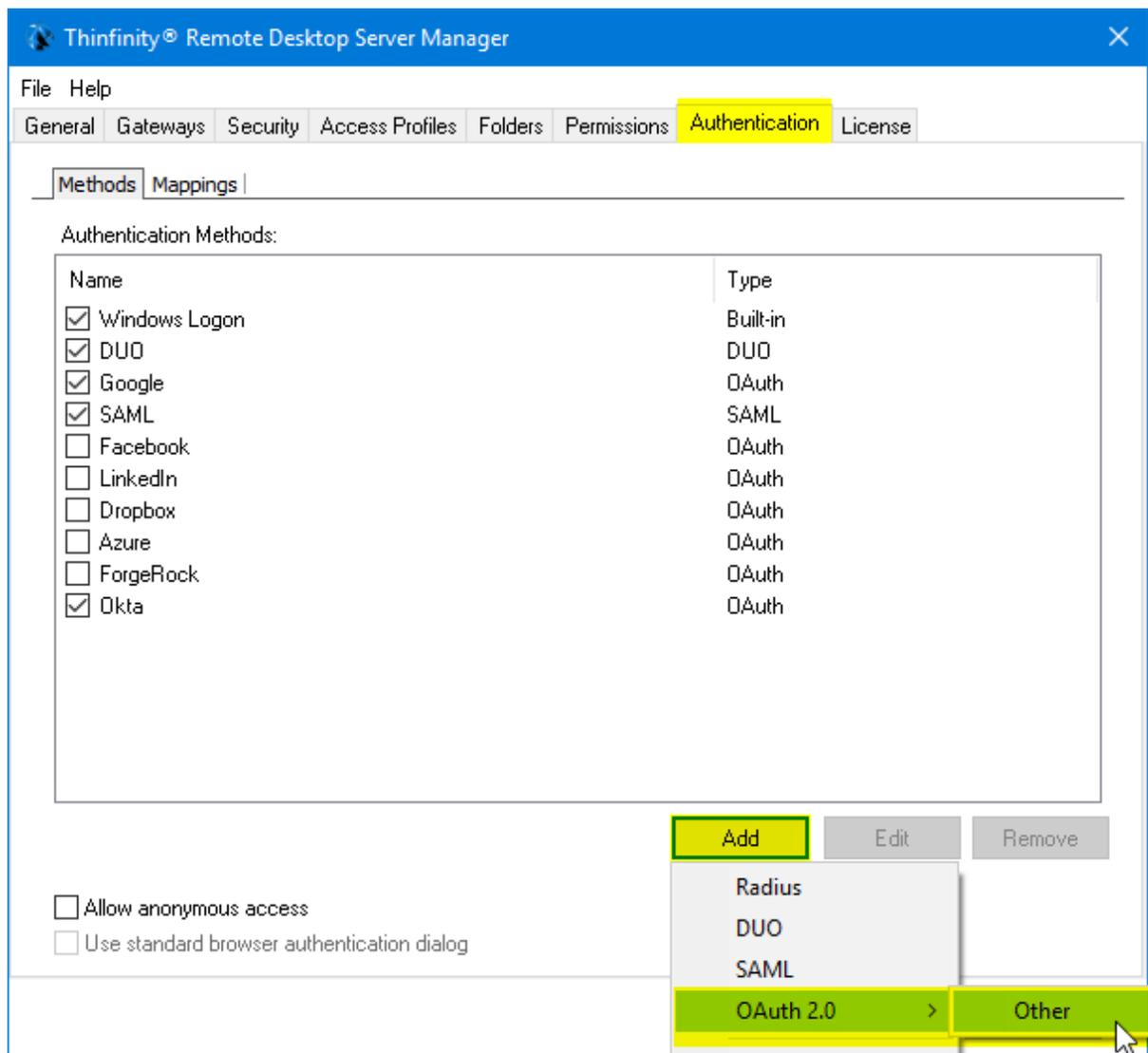
6) Click on the “Assignments” tab and add your users to the Application :

General Sign On **Assignments**

Assign Groups

FILTERS	Priority	Assignment
People		
Groups		
		01101110 01101111 01101100 01101000 01101001 01101110 01100111
		No groups found

7) Now , open either the Thinfinity Remote Desktop Server Manager or the Thinfinity VirtualUI Manager and navigate to the “Authentication” tab. Click on OAuth 2.0 and choose “Other”.



8) Enter your Client ID and Client Secret :

Authentication Method Settings

Name:

Virtual Path:

General **Server**

Client ID:

Client Secret:

Ok Cancel

9) Click on the “Server” tab and add the following parameters :

Authorization URL: [https://\[MyOktaSpace\].okta.com/oauth2/v1/authorize](https://[MyOktaSpace].okta.com/oauth2/v1/authorize)

Parameters: `scope=openid+profile&state=okta`

Token Validation Server URL: [https://\[MyOktaSpace\].okta.com/oauth2/v1/token](https://[MyOktaSpace].okta.com/oauth2/v1/token)

Profile Information Server URL: [https://\[MyOktaSpace\].okta.com/oauth2/v1/userinfo](https://[MyOktaSpace].okta.com/oauth2/v1/userinfo)

Login username value in returned Json: `preferred_username`

You'll also need to change the name of the Authentication Method to "Okta" (Or to the URL you configure in the Initiate Login URI)

The screenshot shows the "Authentication Method Settings" dialog box. The "Name" and "Virtual Path" fields are both set to "Okta" and are highlighted in yellow. The "Server" tab is selected, showing the following configuration:

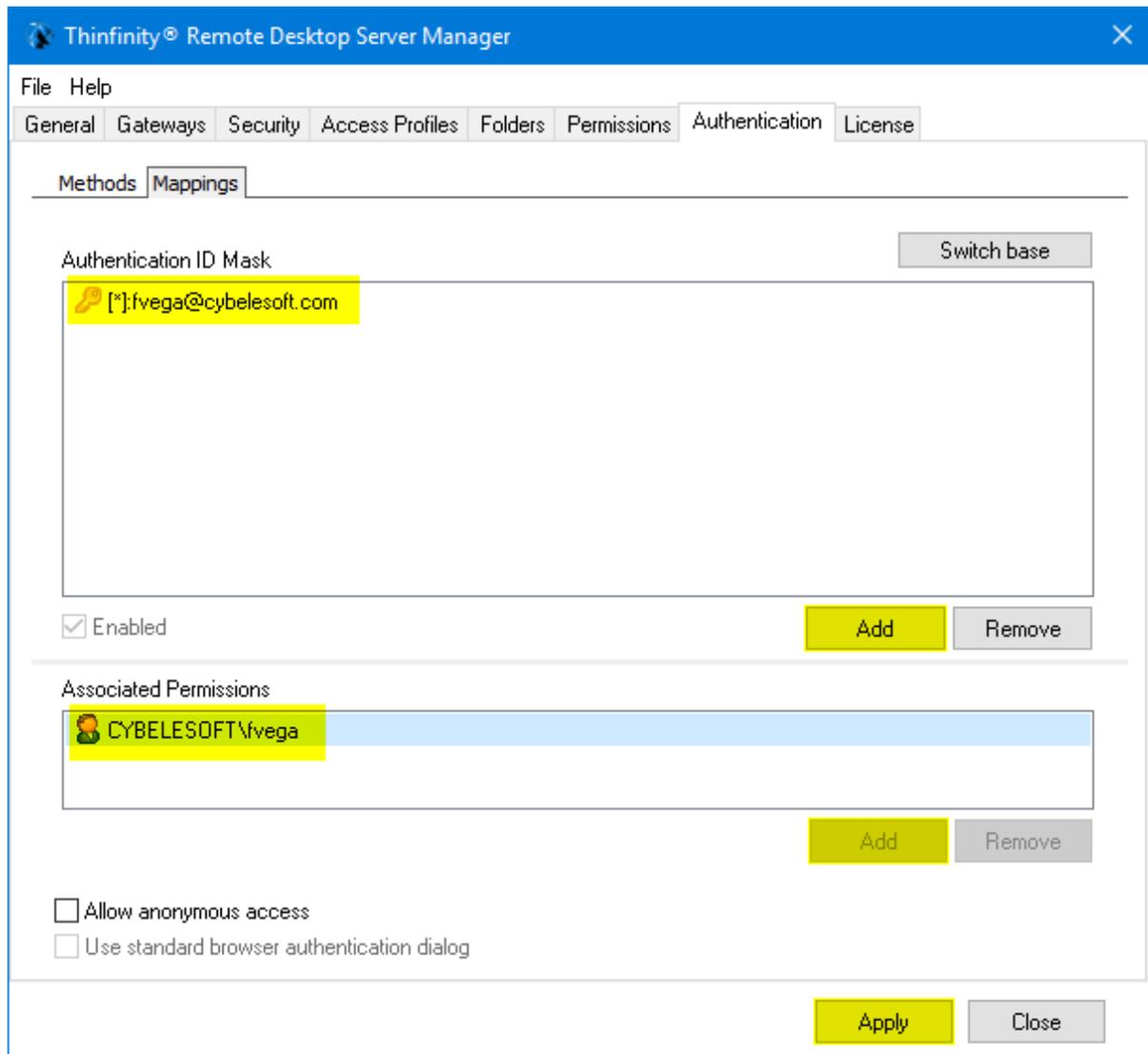
- Authorization URL: `https://[MyOktaSpace].okta.com/oauth2/v1/authorize`
- Authorization parameters: `scope=openid+profile&state=okta`
- Token Validation Server URL: `https://[MyOktaSpace].okta.com/oauth2/v1/token`
- Token Validation extra parameters: `https://[MyOktaSpace].okta.com/oauth2/v1/userinfo`
- User information:
 - Get from URL
 - Get from Token
 - Profile information server URL: (empty field)
 - Add default parameters
 - Add custom parameters: (empty field)
 - Send Basic Authentication header
 - Login username value in returned JSON: `preferred_username`

Buttons for "Ok" and "Cancel" are visible at the bottom right.

Press "OK" after you finish configuring the Authentication Method

10) Click on the "Mappings" tab and then press "Add" under the Authentication ID Mask. Add the email address of the Okta user you want to validate and press "Ok".

Then, under the “Associated Permissions” field, press on the “Add” button and search for the Active Directory User



After you add the appropriate mappings, click on the “Apply” button.

11) Navigate to the Thinfinity’s landing page, and you should see the “Login With Okta” option listed as an Authentication Method.

Sign in or select an option

The image shows a login interface. On the left, there is a blue button with a white square icon and the text "Login with Okta". To the right of this button is a vertical line, and below it is the word "or". To the right of "or" are two input fields: "Username" and "Password". Below these fields is a blue button with a white right-pointing arrow and the text "Sign in".

8.1.6.1.5 Configure OAuth with Auth0

This tutorial will show you how to enable 2FA using Auth0 with Thinfinity VirtualUI .

Auth0 Guardian mobile application is required for 2FA.

- 1) Create a new application on Auth0's administrator site, and chose "Single Page Web Application"

Create Application



Name

You can change the application name later in the application settings.

Choose an application type

 <p>Native</p> <p>Mobile or Desktop, apps that run natively in a device.</p> <p>eg: iOS SDK</p>	 <p>Single Page Web Applications</p> <p>A JavaScript front-end app that uses an API.</p> <p>eg: AngularJS + NodeJS</p>	 <p>Regular Web Applications</p> <p>Traditional web app (with refresh).</p> <p>eg: Java ASP.NET</p>	 <p>Machine to Machine Applications</p> <p>CLI, Daemons or Services running on your backend.</p> <p>eg: Shell Script</p>
---	--	--	--

[CREATE](#)

2) Copy your Client ID and Client Secret :

Name	<input type="text" value="MyThinfintyOAuth"/>	
Domain	<input type="text" value="cybelesoft.auth0.com"/>	
Client ID	<input type="text" value="lHxg45cuPs'"/>	
Client Secret	<input type="text" value="*****"/>	 

Reveal client secret.

The Client Secret is not base64 encoded.

3) In the “Allowed Callback URL” , you need to add the URL that you are going to use to authenticate, and the VirtualPath of the Authentication Method (OAuth by default)

Allowed Callback URLs

<https://MyThinfinityWebsite/oauth>

After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like QA or testing). Make sure to specify the protocol, `http://` or `https://` , otherwise the callback may fail in some cases.

4) To enable 2FA , click on the “Multifactor Auth” and enable “Push Notifications” :

Multifactor Auth With Guardian

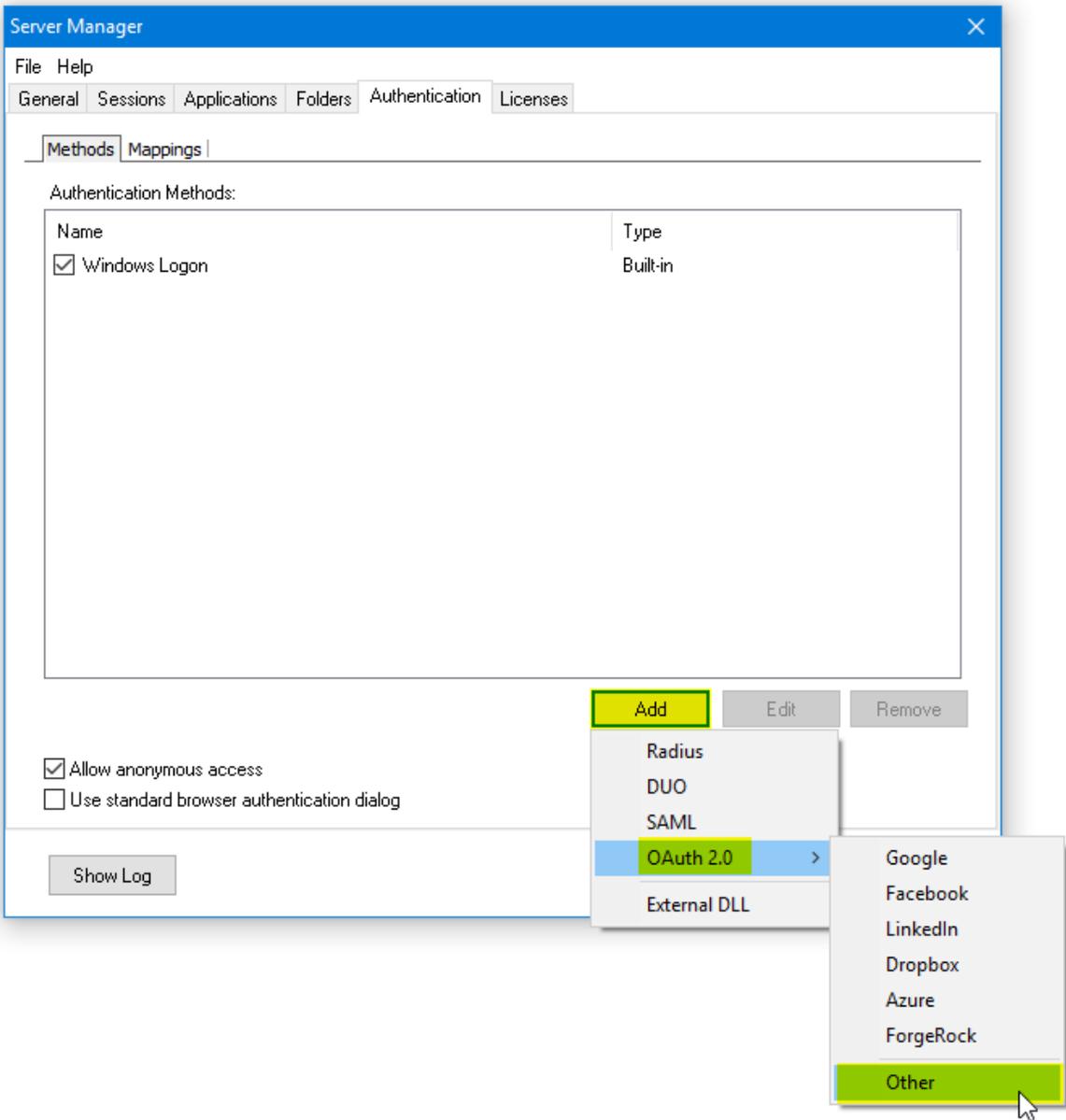
Use of this feature requires the purchase of an addon to your [Auth0 subscription](#). Please [contact us](#) with any questions.

Adds an additional factor to conventional logins to prevent unauthorized access. Use Push Notifications, SMS or both. [Learn more](#)

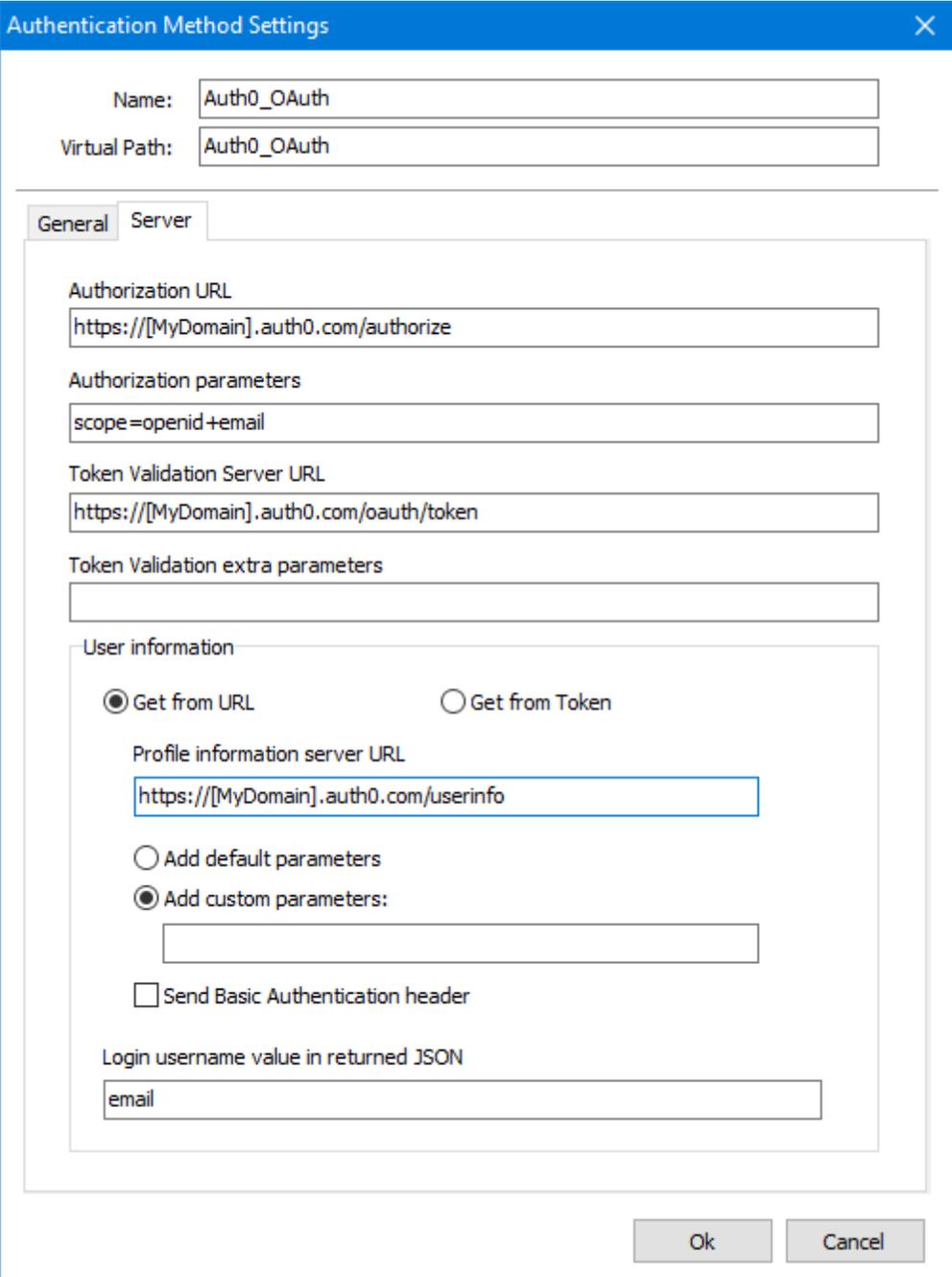
Push Notifications SMS

Auth0 also supports Google Authenticator and Duo. If you use any of these, click here [to configure them](#).

5) Open the Thinfinity VirtualUI Server manager , navigate to the authentication tab , press “Add” -> ”OAuth2.0” -> ”Other”.



6) Add the following information :



The screenshot shows the "Authentication Method Settings" dialog box with the "Server" tab selected. The "Name" and "Virtual Path" fields are both set to "Auth0_OAuth". The "Authorization URL" is "https://[MyDomain].auth0.com/authorize", "Authorization parameters" is "scope=openid+email", and "Token Validation Server URL" is "https://[MyDomain].auth0.com/oauth/token". The "Token Validation extra parameters" field is empty. Under "User information", the "Get from URL" radio button is selected, and the "Profile information server URL" is "https://[MyDomain].auth0.com/userinfo". The "Add custom parameters" radio button is also selected, with an empty text box below it. The "Send Basic Authentication header" checkbox is unchecked. The "Login username value in returned JSON" field contains the text "email". "Ok" and "Cancel" buttons are at the bottom right.

Authentication Method Settings

Name: Auth0_OAuth

Virtual Path: Auth0_OAuth

General Server

Authorization URL
https://[MyDomain].auth0.com/authorize

Authorization parameters
scope=openid+email

Token Validation Server URL
https://[MyDomain].auth0.com/oauth/token

Token Validation extra parameters

User information

Get from URL Get from Token

Profile information server URL
https://[MyDomain].auth0.com/userinfo

Add default parameters
 Add custom parameters:

Send Basic Authentication header

Login username value in returned JSON
email

Ok Cancel

This information can be verified in the “Endpoints” tab under Advanced Settings in the Application you created on Auth0’s interface.

Advanced Settings

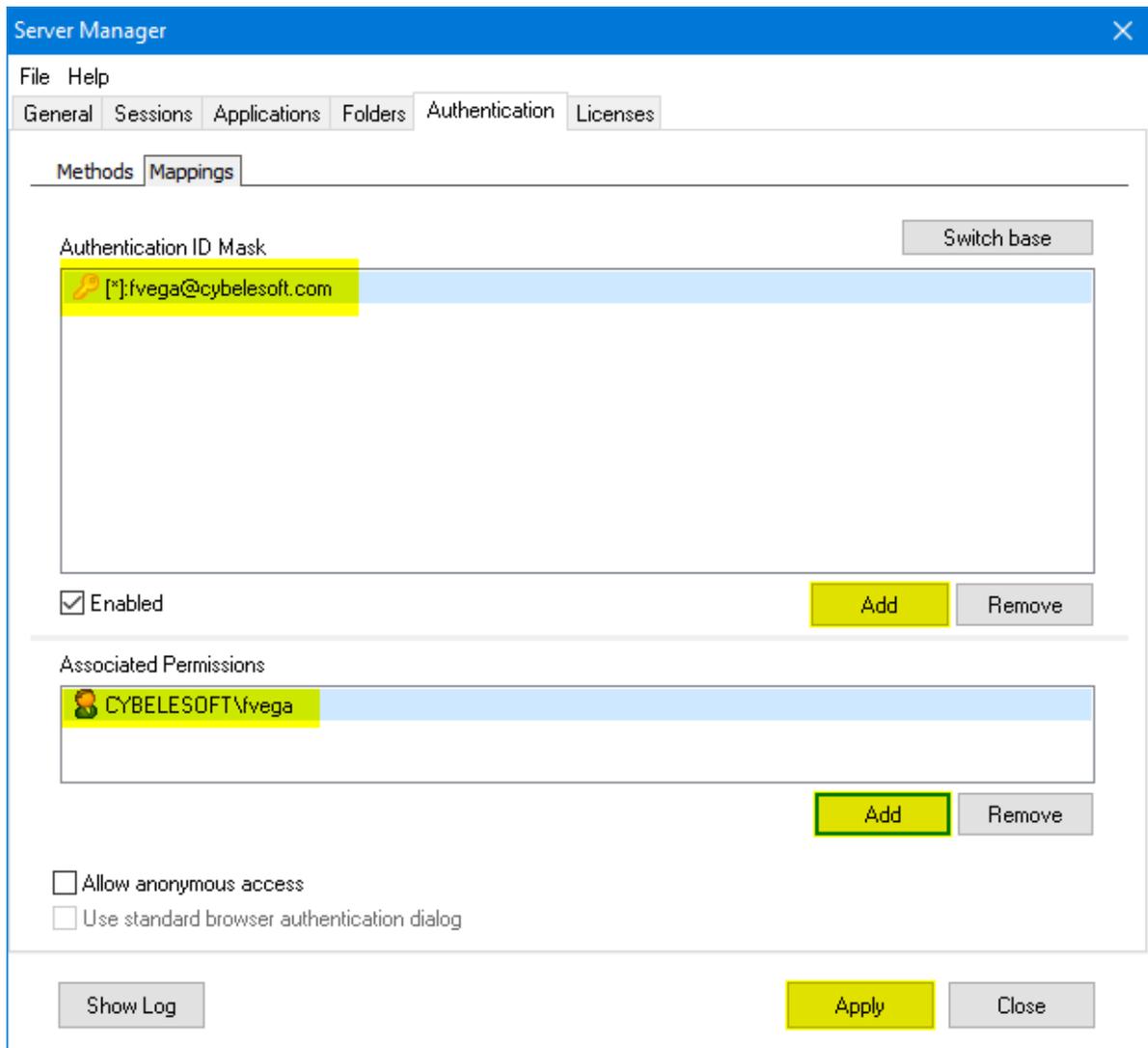
Application Metadata Mobile Settings OAuth Grant Types WS-Federation Certificates **Endpoints**

OAuth

OAuth Authorization URL	<input type="text" value="https://cybelesoft.auth0.com/authorize"/>	
OAuth Token URL	<input type="text" value="https://cybelesoft.auth0.com/oauth/token"/>	
OAuth User Info URL	<input type="text" value="https://cybelesoft.auth0.com/userinfo"/>	
OpenID Configuration	<input type="text" value="https://cybelesoft.auth0.com/.well-known/ox"/>	
JSON Web Key Set	<input type="text" value="https://cybelesoft.auth0.com/.well-known/jw"/>	

Click on “OK” after you entered the information.

7) Click on the “Mappings” tab and then press “Add” under the Authentication ID Mask.



Add the email address of the Auth0 user you want to validate and press “Ok”.

Then, under the “Associated Permissions” field, press on the “Add” button and search for the Active Directory User

After you add the appropriate mappings, click on the “Apply” button.

8) Navigate to the Thinfinity’s landing page, and you should see the “Login With OAuth” option listed as an Authentication Method.

Sign in or select an option

The image shows a login interface. On the left, there is a blue button with a white square icon and the text "Login with OAuth". To the right of this button is a vertical line, and to the right of the line is the word "or". Further to the right are two input fields: the top one is labeled "Username" and the bottom one is labeled "Password". Below these fields is a blue button with a white right-pointing arrow and the text "Sign in".

8.1.6.2 RADIUS

Thinfinity® Remote Desktop Server authentication can be integrated with a RADIUS account. On the links below you will find the information to set up Thinfinity® Remote Desktop Server to work with this.

Read more:

- [More information on RADIUS authentication.](#)
- [The 'Basic' tab](#)
- [The 'Mapping' tab](#)

8.1.6.2.1 Settings

In the 'RADIUS' - 'Basic' section of the Thinfinity® Remote Desktop Server manager 'SSO' tab, you will find the following options:

Authentication Method Settings

Name: Radius

Server

Server IP: 127.0.0.1 Port: 1812

Shared Secret:

Authentication Type: PAP

Test Configuration

Ok Cancel

Server IP	Enter the RADIUS Server IP
Port	Enter the RADIUS Port
Shared Secret	Enter the RADIUS Shared Secret
Authentication Type	Choose your authentication type. The 'EAP' option stands for all the EAP authentication methods.
Test Configuration	Press this button to communicate with RADIUS and test the information entered in the above fields to see if it is correct.

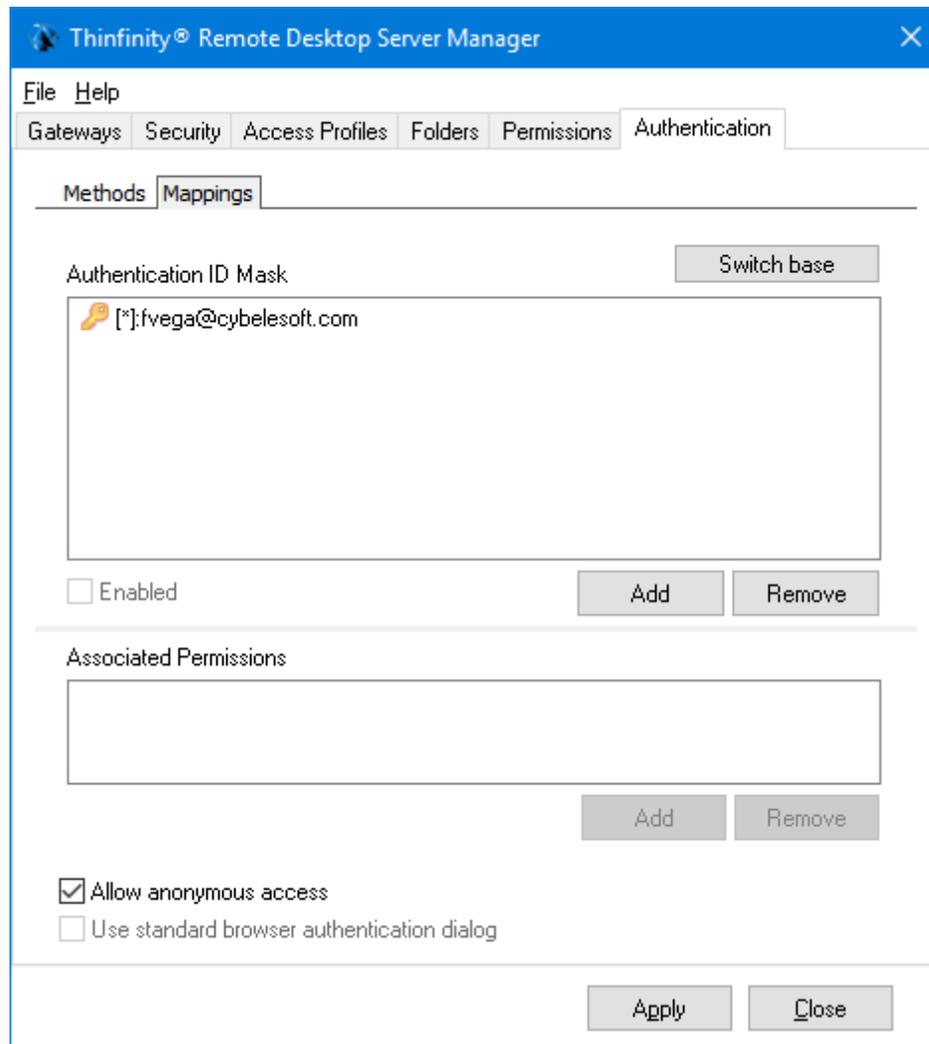
Read more:

- [The 'Mapping' tab](#)

8.1.6.2.2 Mappings

In the 'RADIUS' - 'Mapping' section of the Thinfinity® Remote Desktop Server manager 'SSO' tab, you will link your RADIUS users to Active Directory users or groups. In this way, you tell Thinfinity® Remote Desktop Server that users that authenticate with certain RADIUS users are to be shown certain profiles, the profiles that are available for the Active Directory user(s)/group(s) you selected to link them with. That is, to complete this process you have to link the Active Directory user(s)/group in this tab to the Active Directory user(s)/group of the profile you want to enable for a certain RADIUS user.

The 'Mapping' tab can be shown in two different ways to ease your mapping process. By pressing the 'Switch base' button, you select whether you prefer to see a list of Remote Usernames above, that you will map with the Associated User(s)/Group(s) Access below, or a list of Associated User(s)/Group(s) Access that you will map with the Remote Username list below. This doesn't change the way it works, only the way it is shown. You might want to think that a certain remote username has several Active Directory groups it's associated with and thus choose to see the remote users above, or you might prefer to see, for example, a list of Active Directory users and link each of them with several. You can try, and even go back and forth as you add users and decide which way works best for you. Switching the base doesn't change the users and their mapping.



Switch Base

Press to change the order in which the 'Remote Username' and the 'Associated User/ Group Access' boxes will be shown. This doesn't affect the configuration, only the view.

<p>Remote Username</p>	<p>List of the remote users.</p> <p>Add: Add a new remote user (SSO). If the 'Remote Username' box is above the the Associated User/Group Access box, you will then need to select it and add a Associated User/Group Access to it. Otherwise, if the Remote Username box is below the Associated User/Group Access box, the remote user added will be mapped with the Active Directory User selected in the box above.</p> <p>Remove: Select a user and click on the 'Remove' button to take out this remote user from the SSO authentication control, when the Remote Username box is above the Associated User/Group Access box. This will also remove the mappings. If the 'Remote Username' box is below the Associated User/Group box, you will instead remove the user from the mapping with the Active Directory user/group selected above.</p> <p>Enabled: Select an user on the list and uncheck the 'Enabled' field if you want to disable the access of this specific remote user.</p>
<p>Associated User/Group Access</p>	<p>List of Active Directory Users and Groups.</p> <p>Add: If the Active Directory User/Group Access box is above, adds a user to later on select and associate with a remote user. If the Active Directory User/Group box is below the Remote Username box, maps this user to the selected remote user above.</p> <p>Remove: If the Active Directory User/Group Access box is above, it deletes this user and their mappings from the mapping tab. If the Associated User/Group box is below the Remote Username box, it disassociates this Active Directory user from the remote user selected above.</p>

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

Read more:

- [The 'Settings' tab](#)

8.1.7 External DLL Authentication Method Settings

When you use your own customized external DLL as an authentication method, you only need to set the DLL.

Authentication Method Settings

Name:

External Authentication Provider: ...

Ok Cancel

Name	Choose a name to identify this authentication method.
------	---

External
Authentication
Provider

Select the DLL of your external authentication method.

8.1.8 Duo Authentication Method Settings

When you use Duo as an authentication method, you need to set some parameters.

Authentication Method Settings

Name:

General

Integration Key:

Secret Key:

API Hostname:

AKey:

Ok Cancel

Integration Key	Enter your authentication provider Integration Key, generated while configuring your account integration.
Secret Key	Your authentication provider's Secret Key generated while configuring your account integration.
API Hostname	Your authentication provider's API Hostname generated while

	configuring your account integration.
AKey	Automatically configured by VirtualUI

In the following topic we'll cover how to properly configure DUO as an authentication method using Thinfinity Remote Desktop Server :

- [How to configure DUO](#)

8.1.8.1 How to configure DUO

To configure DUO's Two-Factor authentication, please follow these steps :

On DUO's Web Interface :

1) Navigate to the Applications tab on Duo's administrator website :

The screenshot shows the Duo administrator interface. On the left, a dark sidebar contains a menu with items: Dashboard, Device Insight, Policies, Applications (highlighted in yellow with a '1' next to it), Users (2), Endpoints (3), 2FA Devices (2), Groups (0), Administrators (1), Reports, Phishing, Settings, and Billing. The main content area has a search bar at the top. Below it is a notification: "Your Trial of Duo Access Edition Ends Soon" with "7 days left". Underneath are three cards: "Endpoints List" (See a list of all endpoints accessing your Duo-protected applications.), "Mobile Device Insight" (View the security hygiene of mobile devices in your environment.), and "Self-Remediation" (Preview Duo's end-experience to encourage software updates.). Below these is a "Dashboard" section with three metrics: "3 Out of Date" (3 total endpoints), "0 Up to Date", and "0% Authentication Success" (0% denied authentications). To the right of these is a "2 Total Users" metric.

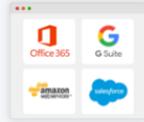
2) Click on "Protect an Application" :

[Dashboard](#) > [Applications](#)

Applications

[SSO Setup Guide](#)

[Protect an Application](#)



Did You Know Your Account Has Secure SSO?

Duo's secure single sign-on (SSO) allows users to access their cloud applications by logging in just once while providing you customized policies on a per-application basis, to secure them from risky users and devices.

3) Create a new "Web SDK" application and click on "Protect this Application" :

[Dashboard](#) > [Applications](#) > [Protect an Application](#)

Protect an Application

web sdk



Web SDK

[Protect this Application](#)

[Read the documentation](#)

4) Copy the Integration Key, Secret Key, and API Hostname :

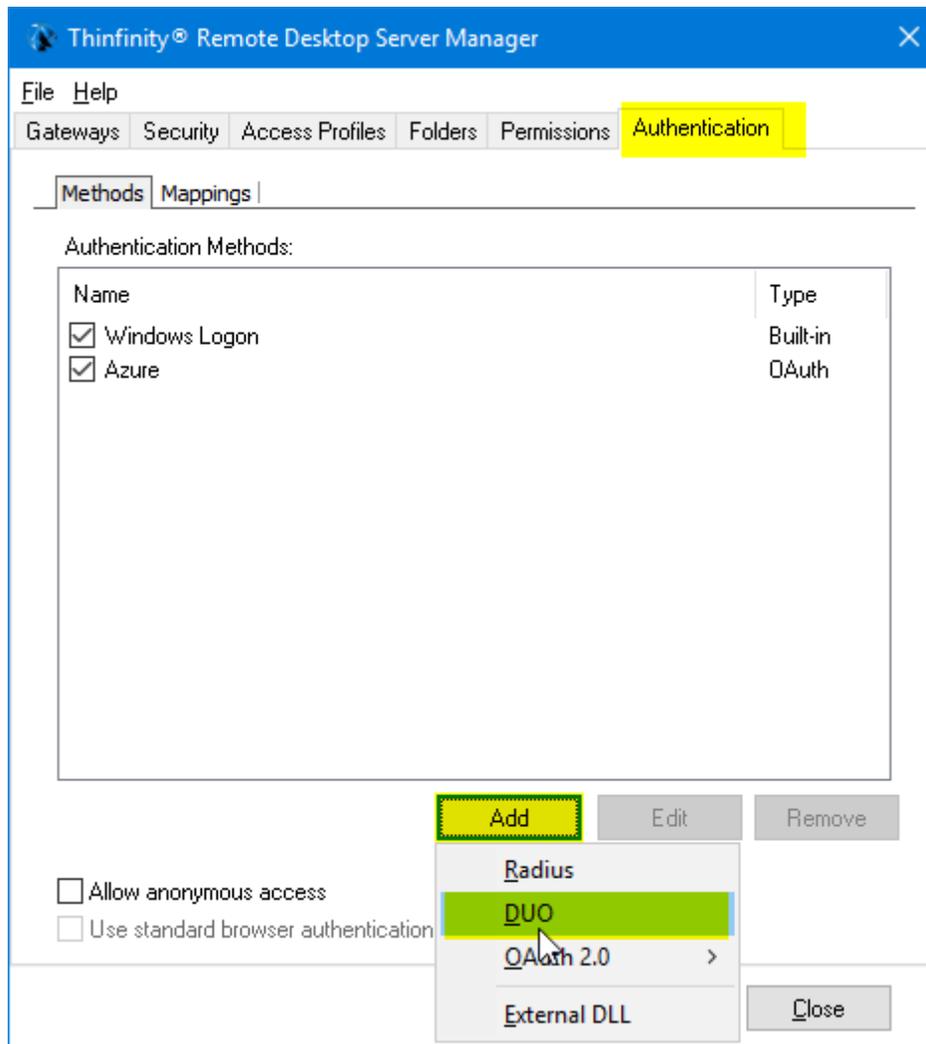
Web SDK 1

See the [Duo Web SDK Documentation](#) to integrate Duo into your custom web application.

Details

Integration key [REDACTED] WWHEZXD
Secret key [Click to view.](#)
Don't write down your secret key or share it with anyone.
API hostname [REDACTED].duosecurity.com

5) Now open the Thinfinity Remote Desktop Server Manager, navigate to the "Authentication" tab , click on "Add" and "DUO" :



6) Copy the Integration Key, Secret Key, and API Hostname provided by DUO , then click "OK" and "Apply" :

Authentication Method Settings

Name:

General

Integration Key:

Secret Key:

API Hostname:

Ok Cancel

7) Navigate to the Thinfinity login page , select "Use DUO" as a method of authentication, and enter valid credentials :

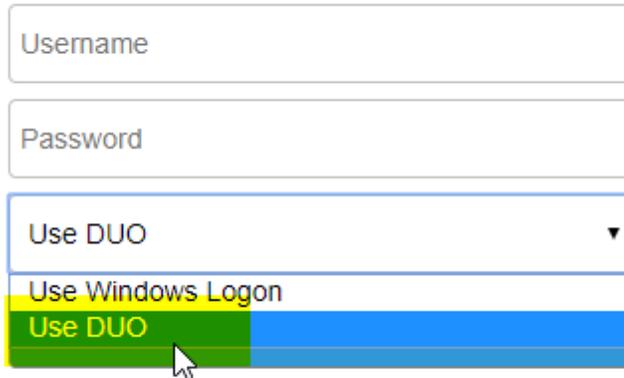
Username

Password

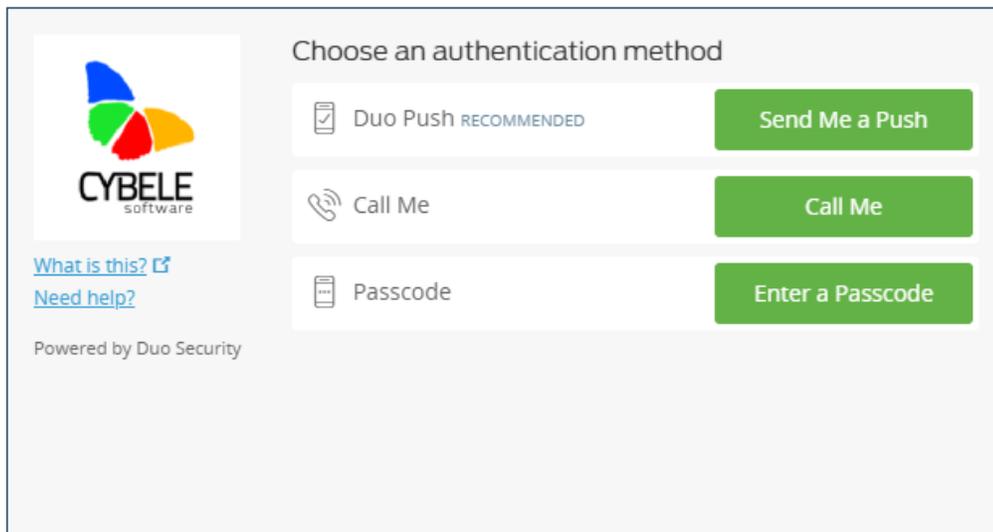
Use DUO ▼

Use Windows Logon

Use DUO



8) Now , you will be given the change to authenticate using a valid DUO authentication method :




CYBELE
software

[What is this?](#) [Need help?](#)

Powered by Duo Security

Choose an authentication method

DUO Push RECOMMENDED [Send Me a Push](#)

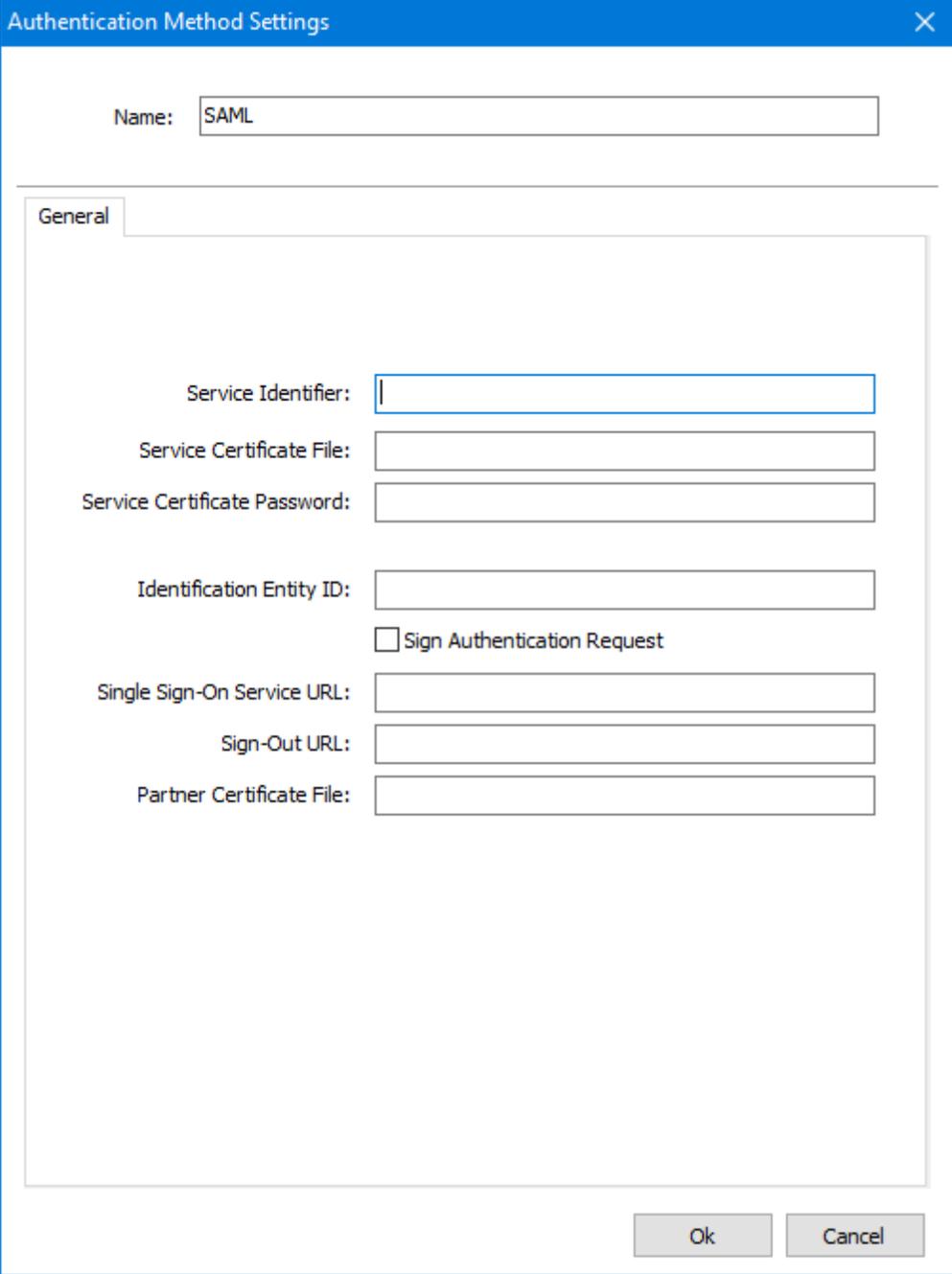
 Call Me [Call Me](#)

 Passcode [Enter a Passcode](#)

Once you validate your account , you will be redirected to the index page with the Duo user validated.

8.1.9 SAML Authentication Method Settings

When you use Duo as an authentication method, you need to set some parameters.



The screenshot shows a dialog box titled "Authentication Method Settings" with a close button (X) in the top right corner. The "Name" field is set to "SAML". Below this is a "General" tab. The "General" tab contains several input fields and a checkbox:

- Service Identifier: []
- Service Certificate File: []
- Service Certificate Password: []
- Identification Entity ID: []
- Sign Authentication Request
- Single Sign-On Service URL: []
- Sign-Out URL: []
- Partner Certificate File: []

At the bottom right of the dialog box are "Ok" and "Cancel" buttons.

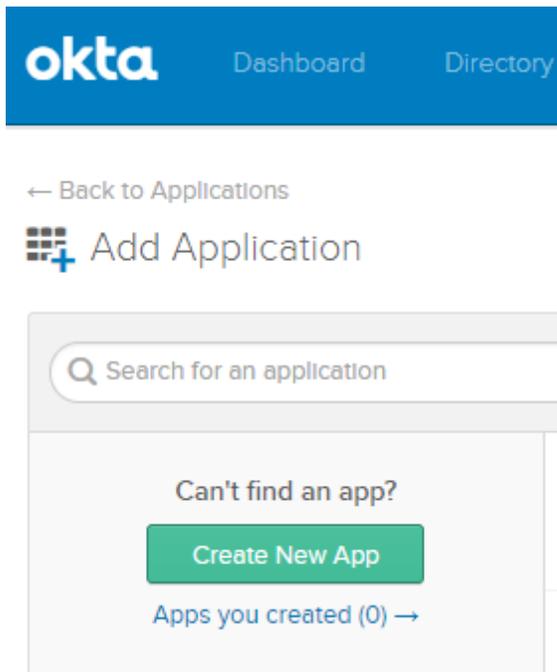
In the following topic we'll cover how to properly configure SAML with Okta as an authentication method using Thinfinity Remote Desktop Server :

- [Configure SAML with Okta](#)

8.1.9.1 Configure SAML with Okta

In this quick tutorial, we will show how to properly configure Okta SAML for Thinfinity Remote Desktop Server.

1) Navigate to your Okta space, go to the Applications tab, and create a new application using the “Create New App” button :



2) Chose “SAML 2.0” as the Authentication Method.

Create a New Application Integration [X]

Platform: Web

Sign on method:

- Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.
- SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
- OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

[Create] [Cancel]

3) Assign a name to the application.

1 General Settings

App name: Thinfinity SAML

App logo (optional) [gear icon] [Browse...]

Upload Logo

App visibility:

- Do not display application icon to users
- Do not display application icon in the Okta Mobile app

[Cancel] [Next]

4) Configure the “Single sign-on URL” and “Audience URI” .

A SAML Settings

GENERAL

Single sign on URL ?
 Use this for Recipient URL and Destination URL
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?
If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

[Show Advanced Settings](#)

The “Single Sign-on URL” address should be the following : [https://\[MyThinfinityWebSite\]/SAMLAssertionConsumerService](https://[MyThinfinityWebSite]/SAMLAssertionConsumerService)

The Audience URI should be the URI used to connect to Thinfinity : [https://\[MyThinfinityWebSite\]/](https://[MyThinfinityWebSite]/)

5) Choose the Feedback options that applies to your application :

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an Internal app

I'm a software vendor. I'd like to Integrate my app with Okta

 The optional questions below assist Okta Support in understanding your app integration.

App type 

This is an internal app that we have created

[Previous](#) [Finish](#)

6) Now that the application is created, it should redirect you to the “Settings” window. Click on “View Setup Instructions” for further information :

Settings [Edit](#)

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

SAML 2.0

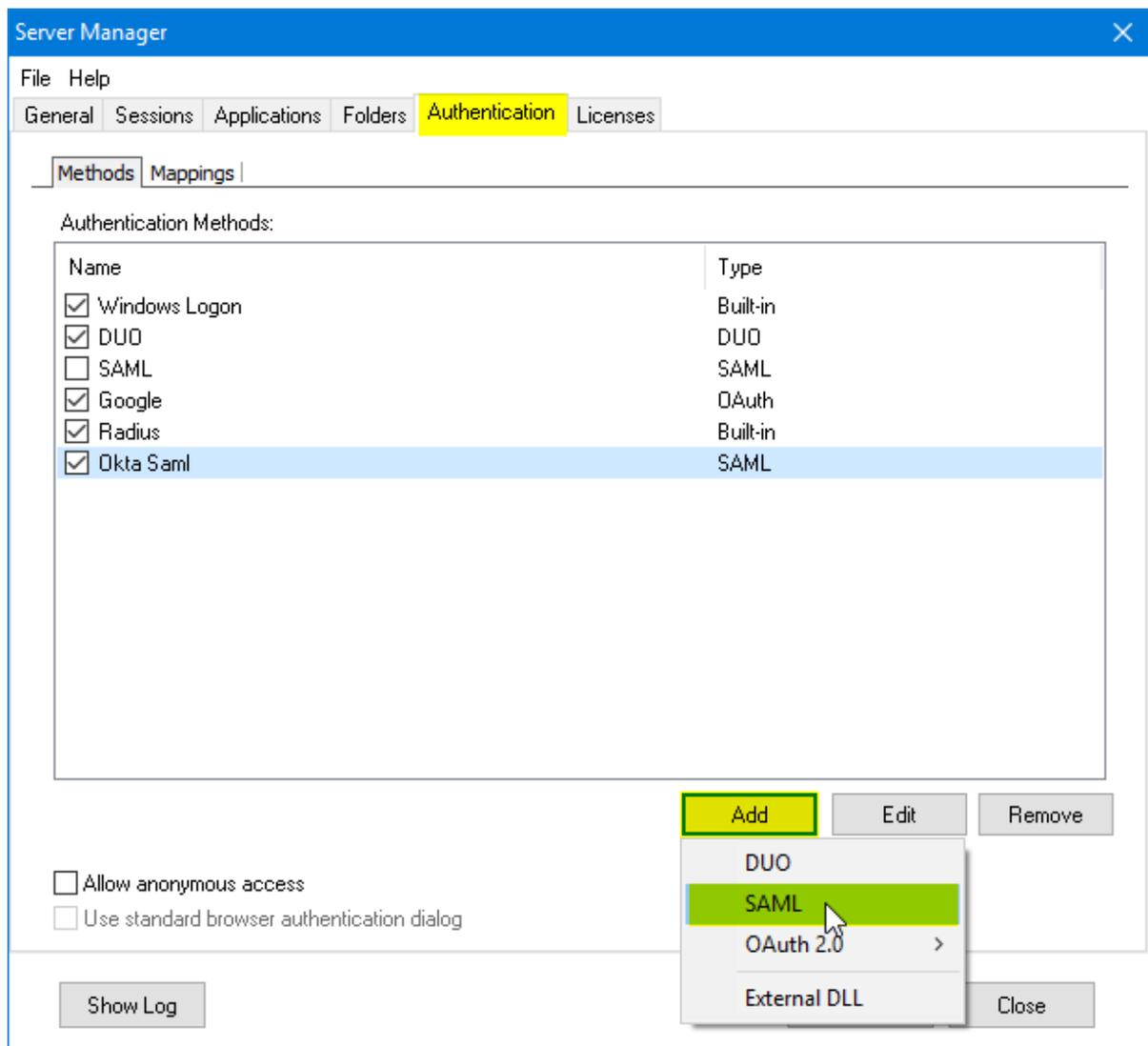
Default Relay State

 SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

In here you will get the “Identity Provider Single Sign-on URL”, the Identity Provider Issuer, and the Certificate provided by Okta.



8) In here, you will have to add the different values provided by Okta in order to enable SAML :

Service Identifier = Audience URI (SP Entity ID)

Service Certificate File = Your certificate's file.

Service Certificate Password = Your certificate's password.

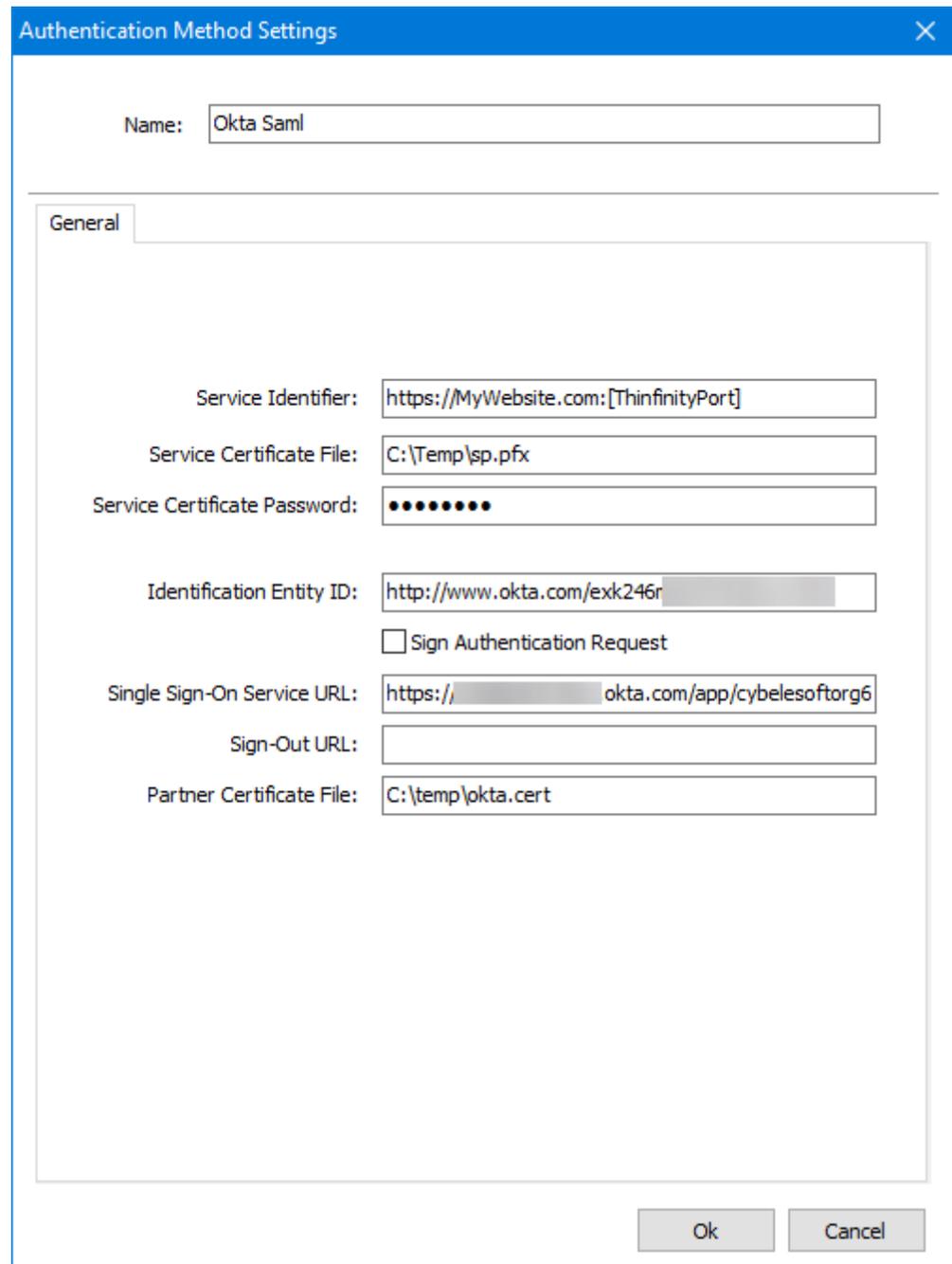
Identificacion Entity ID = Identity Provider Issuer

Single Sign-On Service URL = Identity Provider Single Sign-On URL

Sign-Out URL = This value is optional.

Partner Certificate File = X.509 Certificate provided by Okta.

Below you'll find an example on how it should look like :



The screenshot shows the "Authentication Method Settings" dialog box with the "General" tab selected. The "Name" field is set to "Okta Saml". The "Service Identifier" is "https://MyWebsite.com:[ThinfinityPort]". The "Service Certificate File" is "C:\Temp\sp.pfx". The "Service Certificate Password" is masked with dots. The "Identification Entity ID" is "http://www.okta.com/exk246r". There is an unchecked checkbox for "Sign Authentication Request". The "Single Sign-On Service URL" is "https://[redacted]okta.com/app/cybelesoftorg6". The "Sign-Out URL" is empty. The "Partner Certificate File" is "C:\temp\okta.cert". "Ok" and "Cancel" buttons are at the bottom right.

Authentication Method Settings

Name: Okta Saml

General

Service Identifier: https://MyWebsite.com:[ThinfinityPort]

Service Certificate File: C:\Temp\sp.pfx

Service Certificate Password: ●●●●●●●●

Identification Entity ID: http://www.okta.com/exk246r

Sign Authentication Request

Single Sign-On Service URL: https://[redacted]okta.com/app/cybelesoftorg6

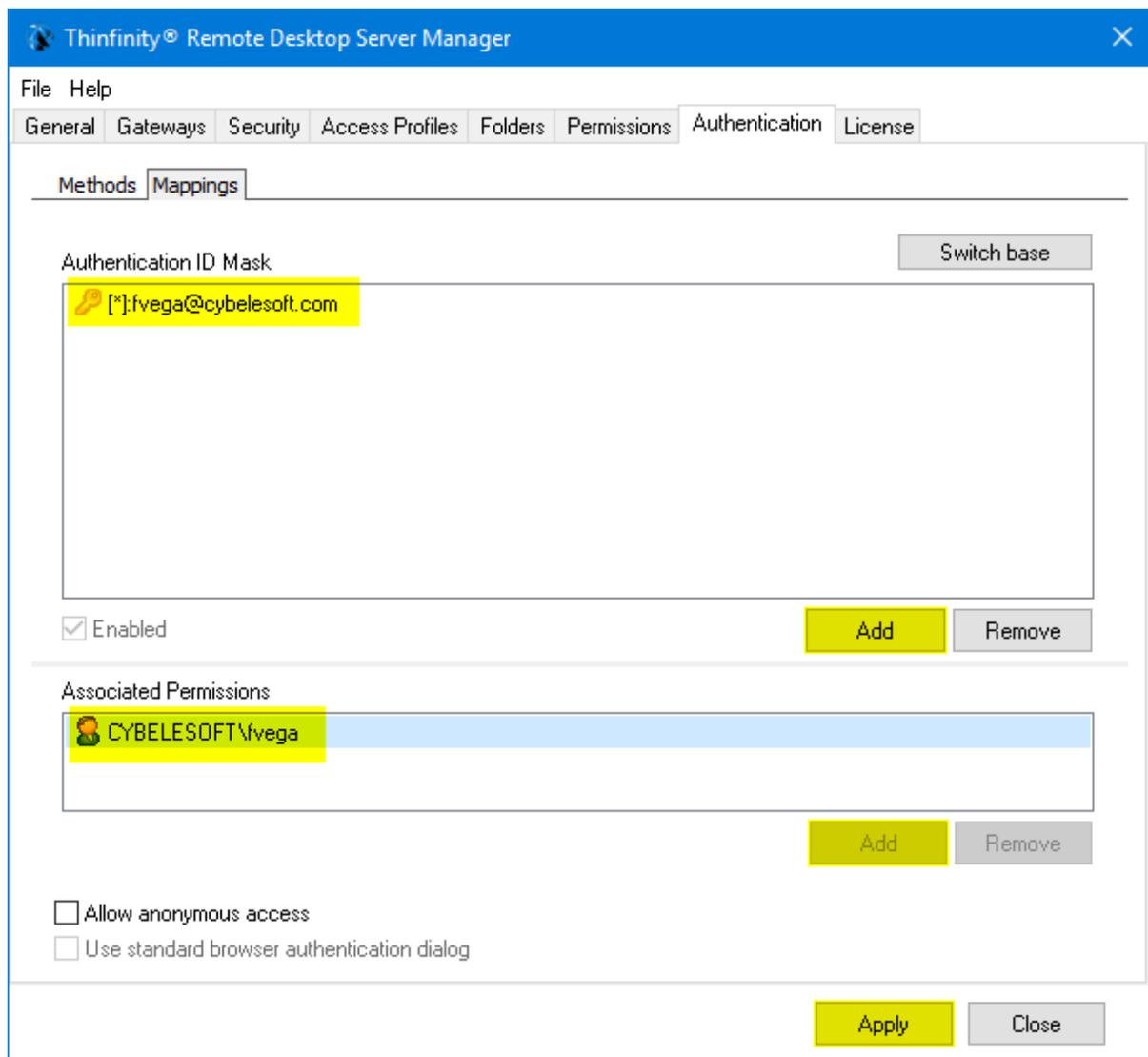
Sign-Out URL:

Partner Certificate File: C:\temp\okta.cert

Ok Cancel

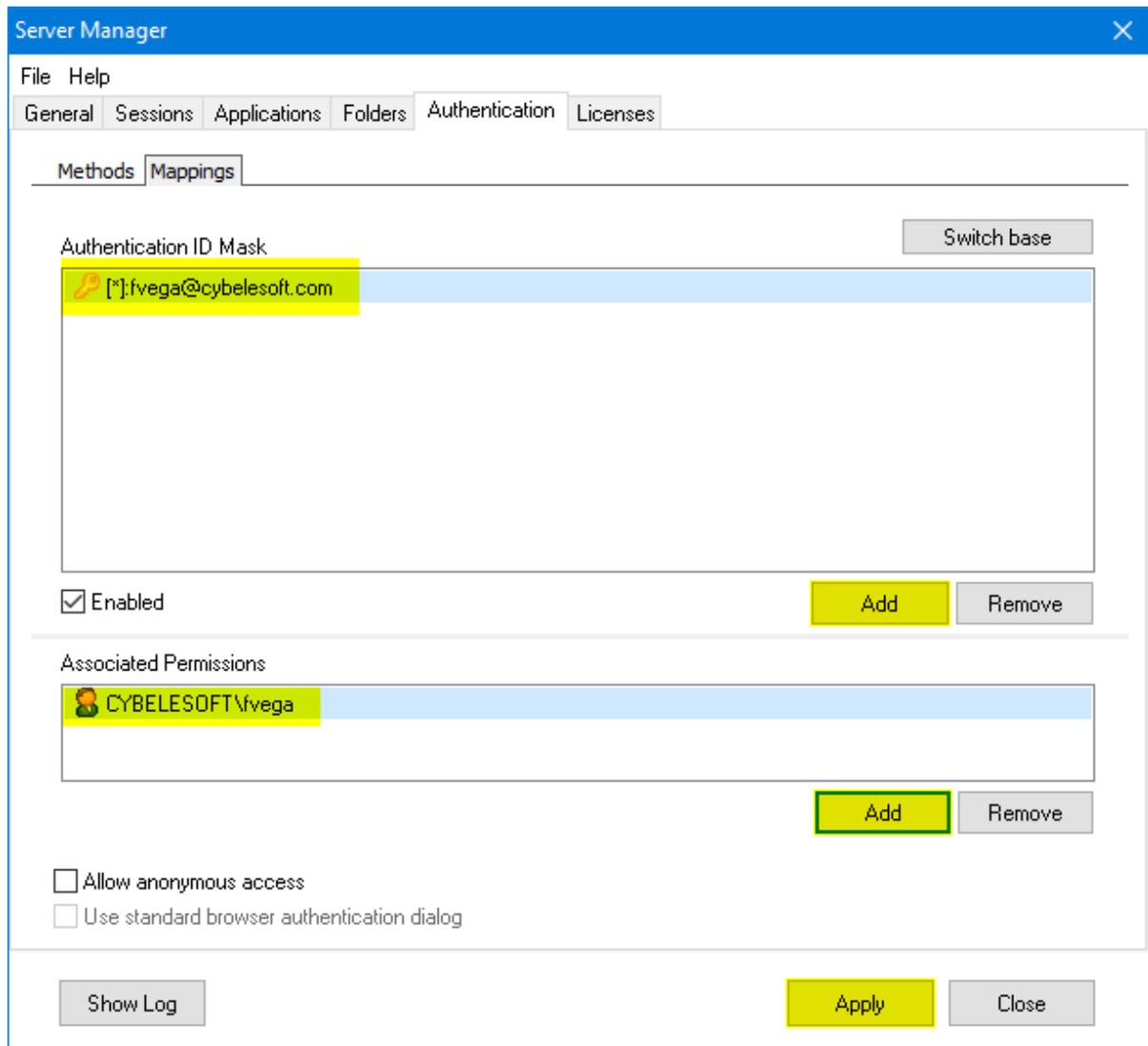
After you finish adding all those values, press "Ok".

10) Click on the "Mappings" tab and then press "Add" under the Authentication ID Mask.



Add the email address of the Okta user you want to validate and press “Ok”.

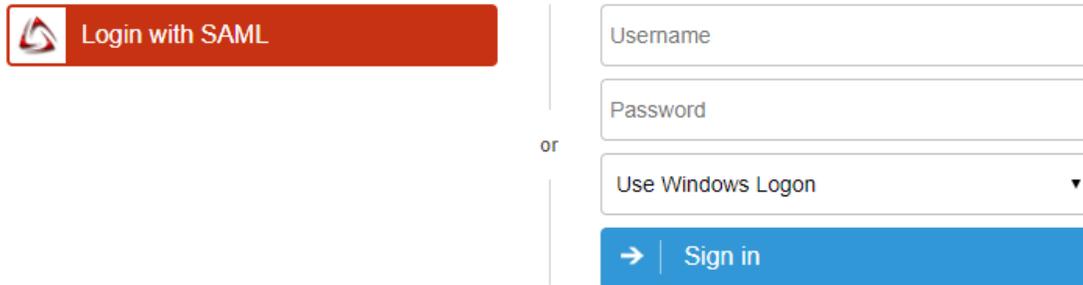
Then, under the “Associated Permissions” field, press on the “Add” button and search for the Active Directory User



After you add the appropriate mappings, click on the “Apply” button.

11) Navigate to the Thinfinity’s landing page, and you should see the “Login With SAML” option listed as an Authentication Method.

Sign in or select an option

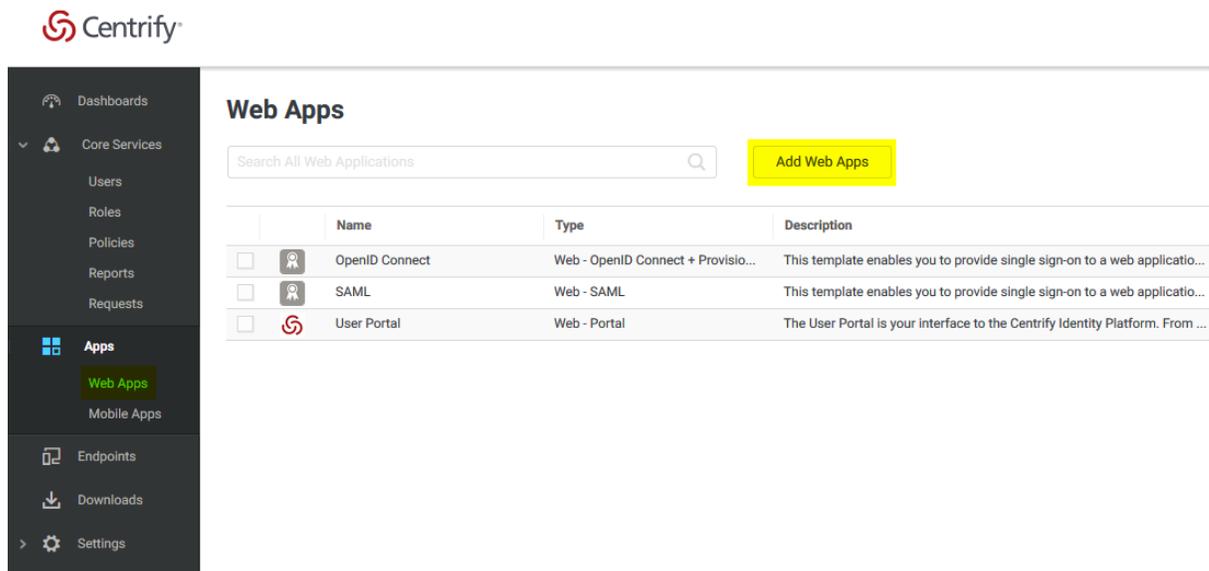


The login interface features a red button labeled "Login with SAML" on the left. To its right, the word "or" is centered. Further right is a form with three input fields: "Username", "Password", and "Use Windows Logon" (a dropdown menu). Below these fields is a blue "Sign in" button with a right-pointing arrow.

8.1.9.2 Configure SAML with Centrify

On the Centrify's Admin Portal.

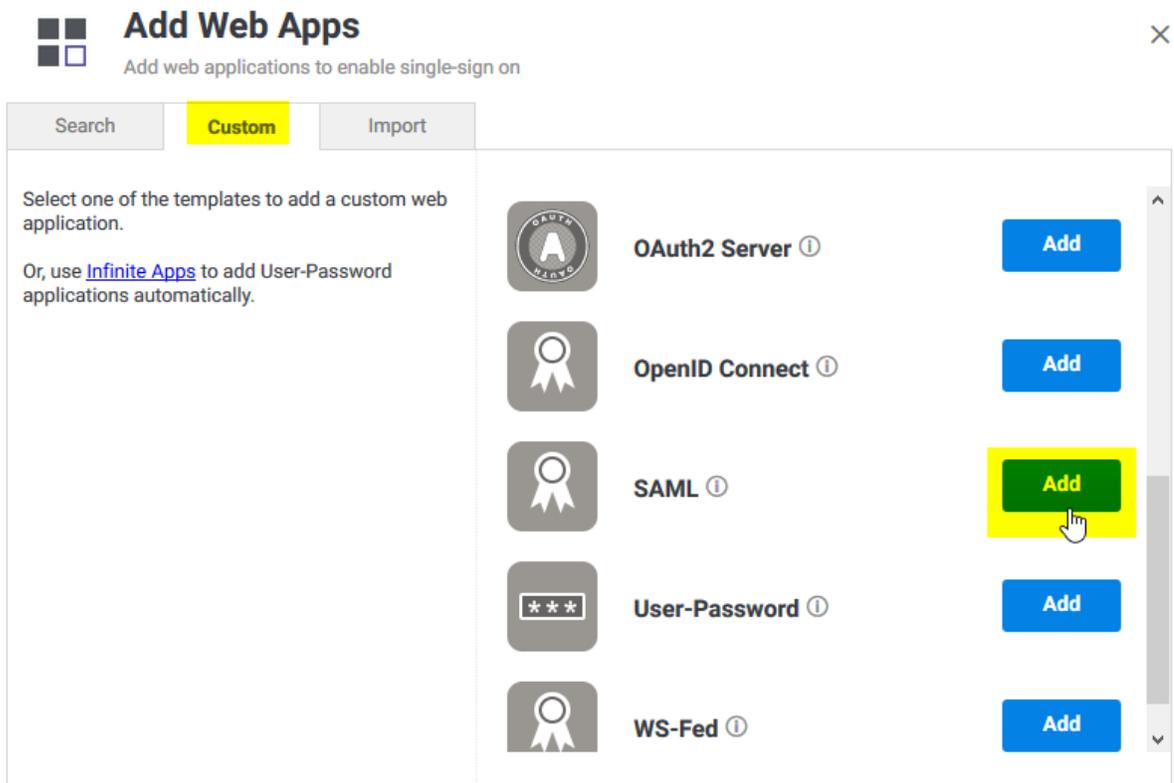
1) Click on "Apps" -> "Web Apps" :



The screenshot shows the Centrify Admin Portal interface. On the left is a dark sidebar with a menu including "Dashboards", "Core Services" (Users, Roles, Policies, Reports, Requests), "Apps" (Web Apps, Mobile Apps), "Endpoints", "Downloads", and "Settings". The "Web Apps" option is highlighted. The main content area is titled "Web Apps" and contains a search bar "Search All Web Applications" and a yellow "Add Web Apps" button. Below is a table with the following data:

	Name	Type	Description
<input type="checkbox"/>	OpenID Connect	Web - OpenID Connect + Provisio...	This template enables you to provide single sign-on to a web applicatio...
<input type="checkbox"/>	SAML	Web - SAML	This template enables you to provide single sign-on to a web applicatio...
<input type="checkbox"/>	User Portal	Web - Portal	The User Portal is your interface to the Centrify Identity Platform. From ...

2) Click on "Custom" and next to SAML, press "Add"



Add Web Apps ×

Add web applications to enable single-sign on

Search **Custom** Import

Select one of the templates to add a custom web application.

Or, use [Infinite Apps](#) to add User-Password applications automatically.

	OAuth2 Server ⓘ	Add
	OpenID Connect ⓘ	Add
	SAML ⓘ	Add
	User-Password ⓘ	Add
	WS-Fed ⓘ	Add

3) Give your application a name , and click on the “Trust” tab .

Trust

[Learn more](#)

Identity Provider Configuration

Configure your IdP Entity ID / Issuer and Signing Certificate, if needed. Your SAML Service Provider will require you to send IdP Configuration value

Metadata

Manual Configuration

Manual Configuration

If your SAML Service Provider provides a SAML SSO configuration screen, copy the applicable IdP Configuration. If SAML Service Provider requires you to send IdP Configuration values, copy them from below and send them to

IdP Entity ID / Issuer ⓘ

https://pod4.centrify.com, [redacted]

Copy

Signing Certificate ⓘ

Centrify SHA256 Tenant Signing Certificate (default)

Thumbprint: [redacted]
Subject: CN=Centrify Customer AAZ0594 Application Signing Certificate
Algorithm: sha256RSA
Expires: 12/31/2038 9:00:00 PM

Download

Click on “Manual Configuration”, and copy the IdP Entity ID, and download the certificate provided by Centrify.

4) Then copy the “Single Sign on URL”, and the “Single Logout URL”:

Single Sign On URL ⓘ

https://aaz0594.my.centrify.com/applogin/appKey/f08861d9-2de1-4c

Copy

Single Logout URL ⓘ

https://aaz0594.my.centrify.com/applogout/appkey/f08861d9-2de1-4c

Copy

Single Sign On Error URL ⓘ

https://aaz0594.my.centrify.com/uperror?title=Error%20Signing%20In

Copy

5) Now, on the “Service Provide Configuration”, click on “Manual Configuration” and configure the following:

Service Provider Configuration

Select the configuration method specified by Service Provider, and then follow the instructions.

Metadata

Manual Configuration

Manual Configuration

Fill out the form below with information given by your Service Provider. Be sure to save your work when done.

SP Entity ID / Issuer / Audience ⓘ

https://YourThinfinitySite:[Port]/

Assertion Consumer Service (ACS) URL ⓘ

https://YourThinfinitySite:[Port]/SAMLAssertionConsumerService

Recipient * ⓘ

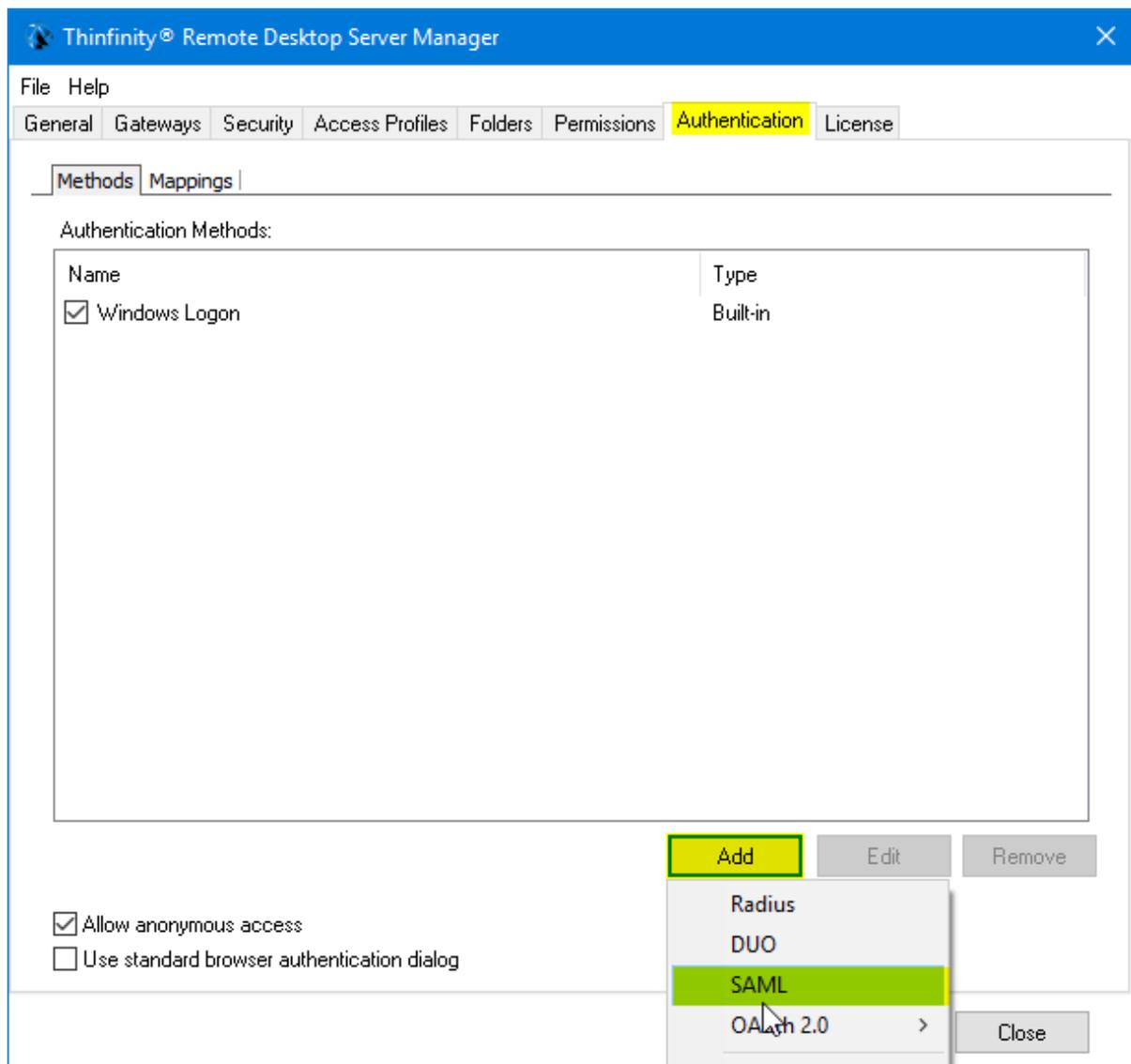
Same as ACS URL

Enter Recipient here

After doing these changes, click on the “Save” button.

6) Now we need to configure Thinfinity with all this information .

Open the Server Manager and navigate to the “Authentication” tab, press “Add” , and then SAML :



7) Now we must configure the connection itself :

The screenshot shows a dialog box titled "Authentication Method Settings" with a close button (X) in the top right corner. The "Name" field is set to "SAML". Below this is a "General" tab. The fields are as follows:

- Service Identifier: `https://YourThinfinitySite:[Port]`
- Service Certificate File: `c:\temp\sp.pfx`
- Service Certificate Password: `*****`
- Identification Entity ID: `https://pod4.centrifys.com/`
- Sign Authentication Request
- Single Sign-On Service URL: `https://[redacted].my.centrifys.com/applogin/appKey/f0`
- Sign-Out URL: `https://[redacted].my.centrifys.com/applogout/appkey/t`
- Partner Certificate File: `c:\temp\Centrifys SHA256 Tenant Signing Certificate (`

At the bottom right, there are "Ok" and "Cancel" buttons.

- Service identifier = `https://YourThinfinitySite:[Port]`
- Service Cert File = `[Path_To_Your_Certificate]`
- Service Cert Pass = `[Certificate_Password]`

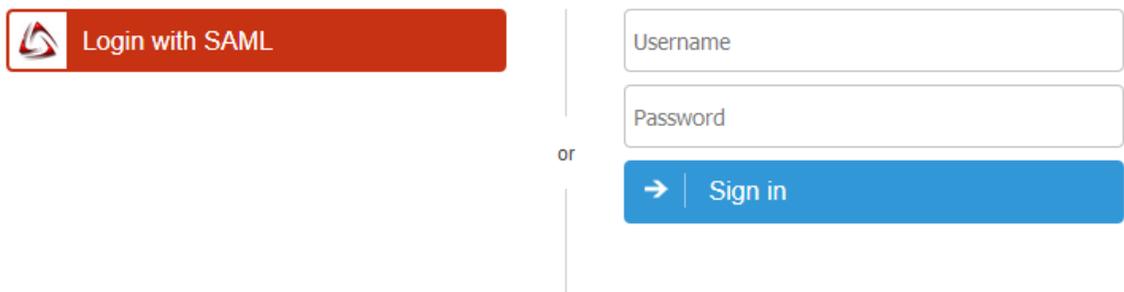
- Identification Entity = `[IdP Entity ID / Issuer]`

- Single Sign on Service URL = [Single Sign on URL]
- Sign-out URL = [Single Logout URL]
- Partnet Cert File = [Certificate Provided by Centrify]

Once you configured it properly , click “Ok” and then “Apply”

8) Now go the Thinfinity landing page and you should see the “Login with SAML” option now available to use.

Sign in or select an option

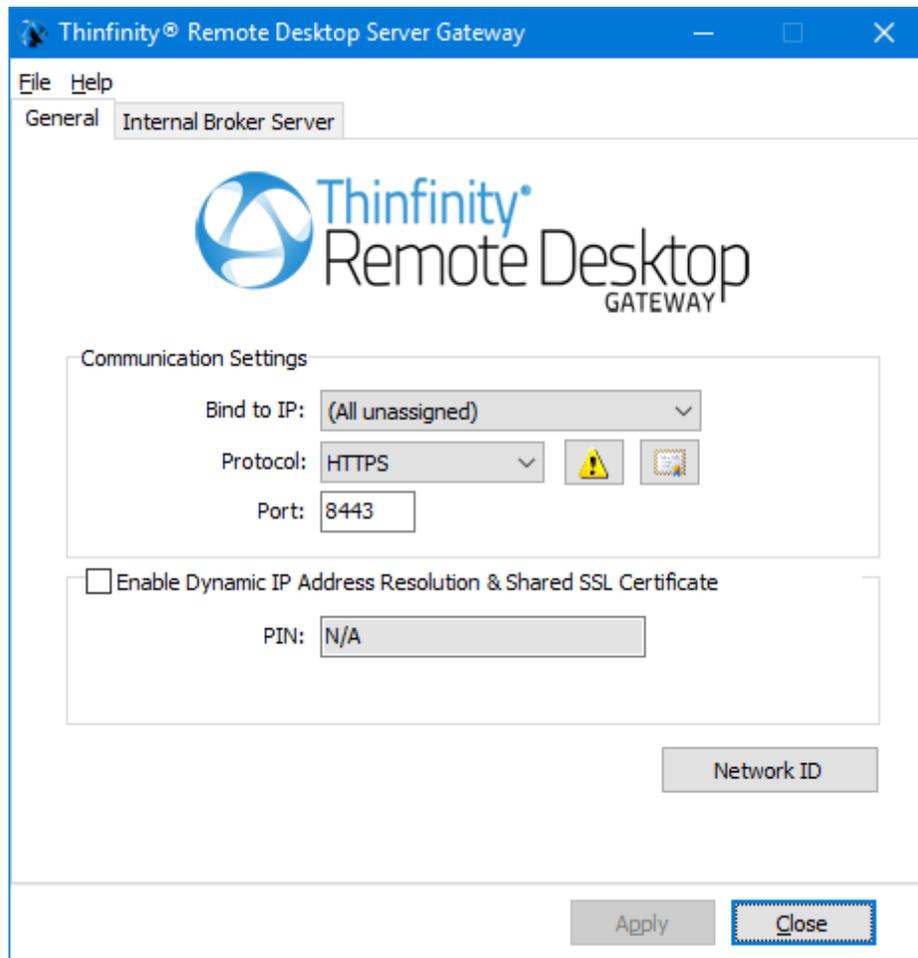


The screenshot shows a login interface. On the left, there is a red button with a white icon and the text "Login with SAML". To the right of this button is a vertical line with the word "or" centered between two shorter vertical lines. Further to the right is a form with three input fields: "Username", "Password", and a blue button with a white right-pointing arrow and the text "Sign in".

8.2 Gateway Manager

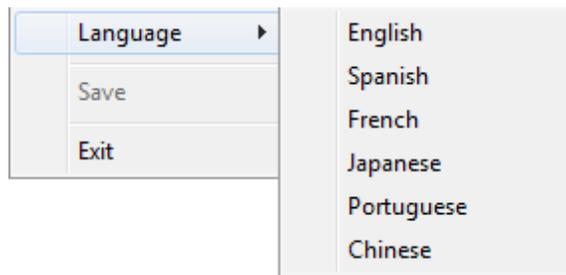
The Gateway Manager is a tool to configure gateway options in a [Load Balancing](#) scenario.

Install Thinfinity Remote Desktop Gateway Services and look for the 'Thinfinity Remote Gateway' shortcut in the Start Menu.



Its main menu has two sub-menus:

File Menu:

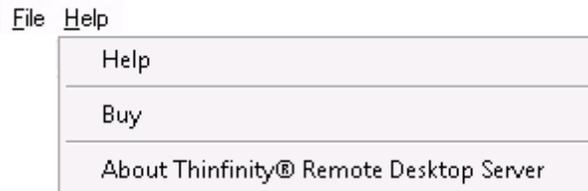


The File Menu is composed of the following options:

Save	Click to save any change done in the system Settings.
Exit	Click on this option to exit the Thinfinity® VirtualUI™ Server

Manager.

Help Menu:



The Help Menu is composed of the following options:

Help	Takes you to the application online guide.
Buy	Takes you to the Cybele Software Buy page.
About Thinfinity VirtualUI	Click on the 'About...' option to see the application version and build number.

The General tab presents the following options:

Bind to IP	Use this option to restrict access to the service to one specific IP address. The 'All unassigned' option allows access through all the available IP addresses.
Protocol	Choose between the http and https protocol.
	Press this button to configure HTTP error responses .
	This button is only visible when the protocol is set to HTTPS. Press this button to access the options for replacing the default Thinfinity VirtualUI installed certificate with your own. Read more about managing the SSL certificates .
Port	Choose which port will Thinfinity® VirtualUI™ Server be listening on. If the port is not available, you will see an error message on the status bar.
Network ID	<p>The network ID identifies this gateway services installation. Thinfinity VirtualUI Servers that want to share their resources through this this gateway must match this Network ID.</p> <p>Press this button to see and/or change the Network ID. The default value is a random string but you can change it to</p>

	something more descriptive.
Show Log	Press to open the file with the Thinfinity VirtualUI log.

8.2.1 Configure HTTP Error Responses

You can access configuration for the HTTP Error response pages by pressing this button in the [Gateway manager](#)



You will be presented with the following dialog:

Error Pages
✕

Configure HTTP error responses. The error responses can be custom error pages, or detailed error messages that contain troubleshooting information.

Status Code	Path	Type
401	401.html	Send File
402	402.html	Send File
403	403.html	Send File
404	404.html	Send File
409	409.html	Send File
500	500.html	Send File

Add

Edit

Remove

OK

Cancel

Status Code	<p>This numeric code indicates the status of the response when a browser tries to access content in Thinfinity Remote Desktop Server. The error responses may be displayed in the client browser.</p> <p>The HTTP status code may indicate whether a request is</p>
-----------------------------	---

	successful or unsuccessful, and may also reveal the exact reason that a request is unsuccessful.
Path	Shows the path to the error file that will show in case of a particular status code. The default path is the 'webrdp' directory in the Thinfinity Remote Desktop installation directory.
Type	Shows the Thinfinity Remote Desktop Server action in the event of an error status code: - Send file: Thinfinity Remote Desktop Server will show an error page located physically in the server's computer. - Redirect: Thinfinity Remote Desktop Server will redirect the page to any web page indicated in the configuration.
Add	Press this button to add a new Custom Error page. Read more about this below.
Edit	Press this button to edit an existing Custom Error Page. Read more about this below.
Remove	Press this button to remove a selected Custom Error Page.

If you choose to add or edit a Custom Error Page, you will be presented with the following dialog:

Status Code	Enter the Status Code that you want to configure.
-------------	---

Response Action	Choose whether Thinfinity Remote Desktop Server will show a page that is stored locally or will redirect the user to another web page.
Insert Content from file into the error response	Choose this option if you want Thinfinity Remote Desktop Server to show a static page locally stored in your Thinfinity Remote Desktop Server server. Complete the file path by selecting the file you want to show with the button.
Response with a 302 redirect	Choose this option if you want Thinfinity Remote Desktop Server to redirect users to a web page. Type the Absolute URL to this web page in the field below

Press OK to save the changes.

Read more:

- [Managing the SSL Certificate](#)

8.2.2 Managing the SSL Certificate

You can access configuration for the SSL certificate by pressing this button in the [Gateway manager](#), available when the protocol is set to HTTPS:



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 Thinfinity® Remote Desktop Server 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 ways 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 the Thinfinity® Remote Desktop Server manager "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 Thinfinity® Remote Desktop Server 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.

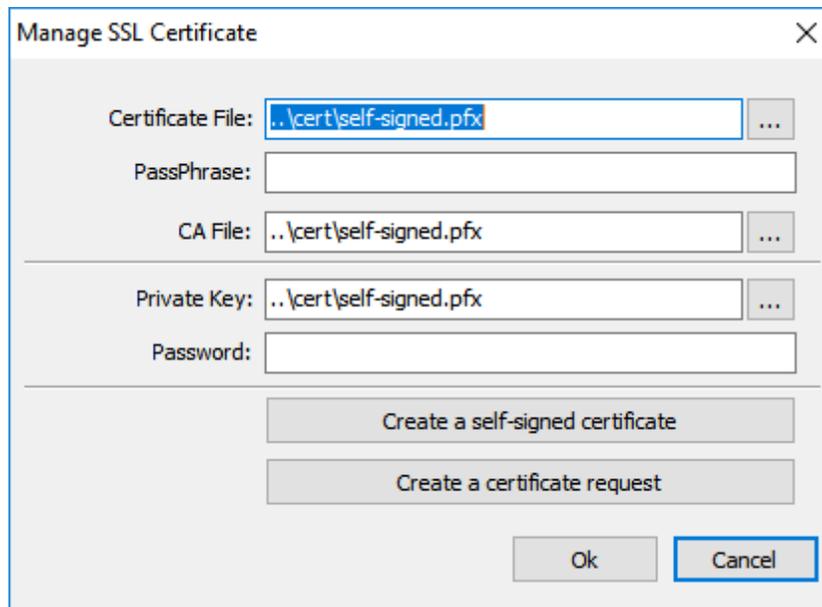
Read more:

- [The Default Embedded Certificate](#)
- [A Self-Signed Certificate](#)
- [A CA Certificate](#)
- Dynamic DNS and Certificate Sharing

8.2.2.1 The Default Embedded Certificate

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

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



Note: Because this certificate is not issued by a known Certificate Authority (CA), the web browsers will produce a warning about verifying its authority.

Read more:

- [A Self-Signed Certificate](#)
- [ACA Certificate](#)
- Dynamic DNS and Certificate Sharing

8.2.2.2 A Self-Signed Certificate

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

1. Go to the Thinfinity® Remote Desktop Server manager 'Security' tab.
2. Press the 'Create a self-signed certificate' button.
3. Fill in the form below with your organization data:

Country Code:

State:

Locality:

Organization:

Organizational Unit:

Common Name:

E-Mail address:

Bits: ≥ 512

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

Create Close

Country Code	The two letter country code of the International Organization for Standardization (ISO 3166)
State	Full unabbreviated name of the state or province your organization is located.
Locality	Full unabbreviated name of the city where your organization is located.
Organization	The name your company is legally registered under.
Organizational Unit	Use this field to differentiate between divisions within an organization.
Common Name	The domain name or URL you plan to use this certificate with.

E-Mail Address	Company e-mail address.
Bits	We recommend using a 2048 length key.

4. The "Common Name" field should be filled with the server+domain that will be used to access Thinfinity® Remote Desktop 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.

Read more:

- [ACA Certificate](#)
- Dynamic DNS and Certificate Sharing

8.2.2.3 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 Thinfinity® Remote Desktop Server manager 'Security' tab.
2. Click on the 'Create a certificate request' button.
3. Fill in the form below with your organization data:

Country Code	The two letter country code of the International Organization for Standardization (ISO 3166)
State	Full unabbreviated name of the state or province your organization is located.
Locality	Full unabbreviated name of the city where your organization is located.
Organization	The name your company is legally registered under.
Organizational Unit	Use this field to differentiate between divisions within an organization.

Common Name	The domain name or URL you plan to use this certificate with.
E-Mail Address	Company e-mail address.
Bits	We recommend using a 2048 length key.

4. The 'Common Name' field should be filled with the server+domain that will be used to access Thinfinity® Remote Desktop 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.

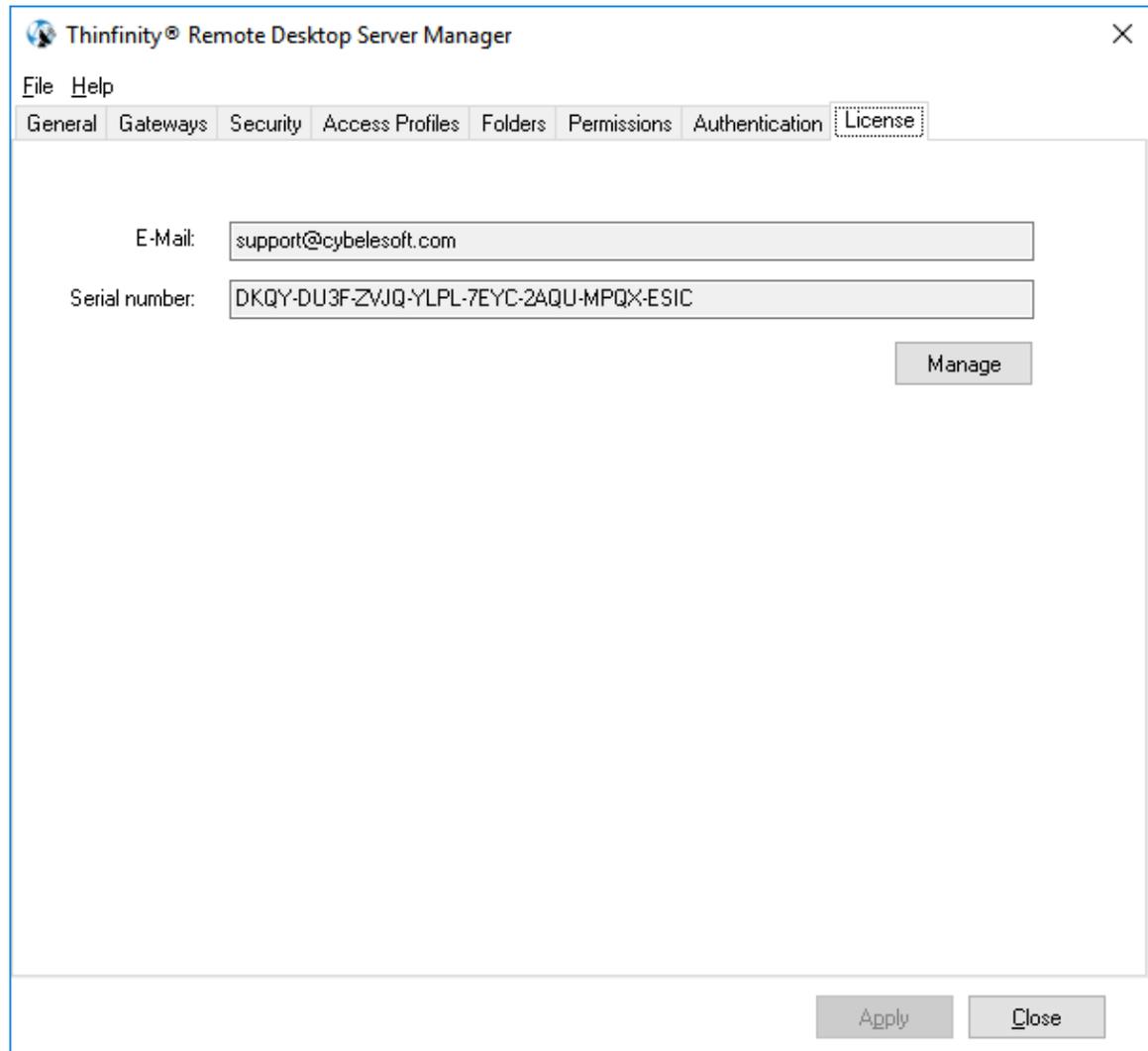
After the CA validation process, place the certificate they sent to you on Thinfinity® Remote Desktop Server cert directory and inform the path to the files on Thinfinity® Remote Desktop Server [Manage Certificate](#) option (Certificate file, CA file and Private Key).

Read more:

- Dynamic DNS and Certificate Sharing

8.3 License Manager

The license manager option is found in the License tab of Thinfinity Remote Desktop Server Manager. Use this manager to check your licensing status, activity, add or remove your licenses.

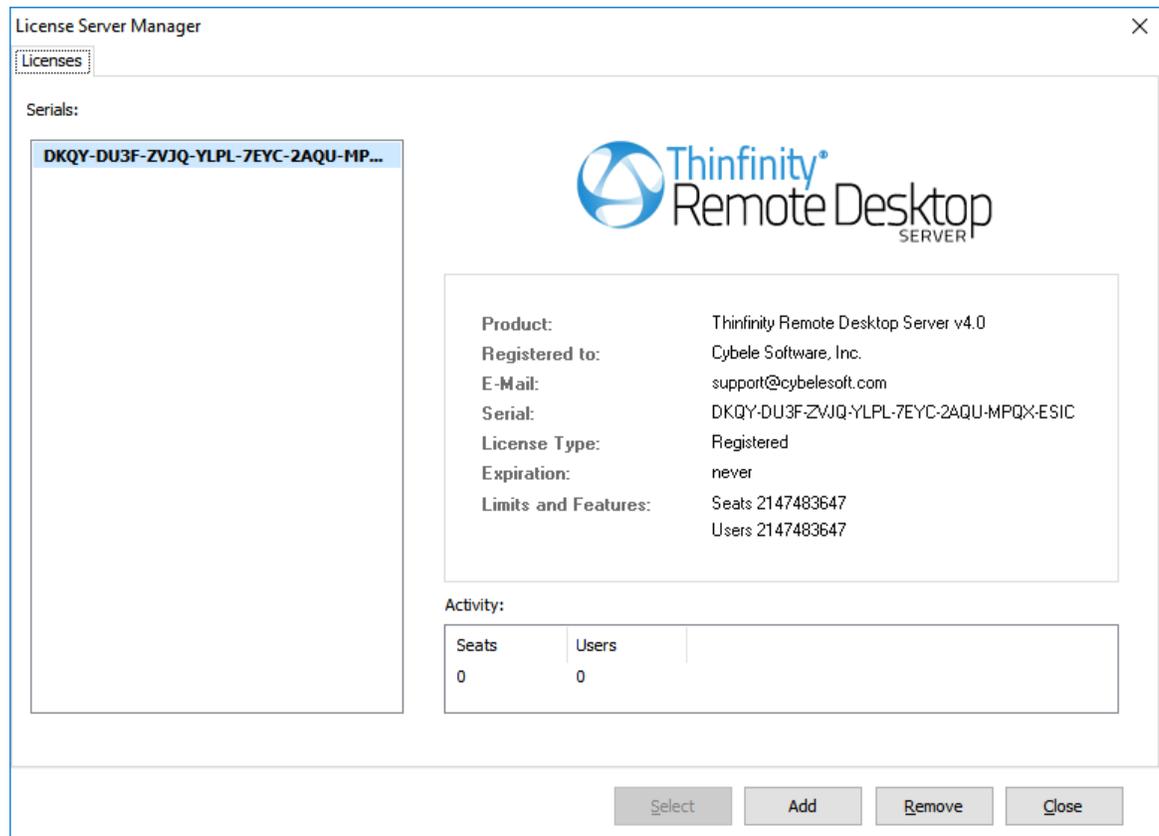


Read more:

- [License Activation](#)

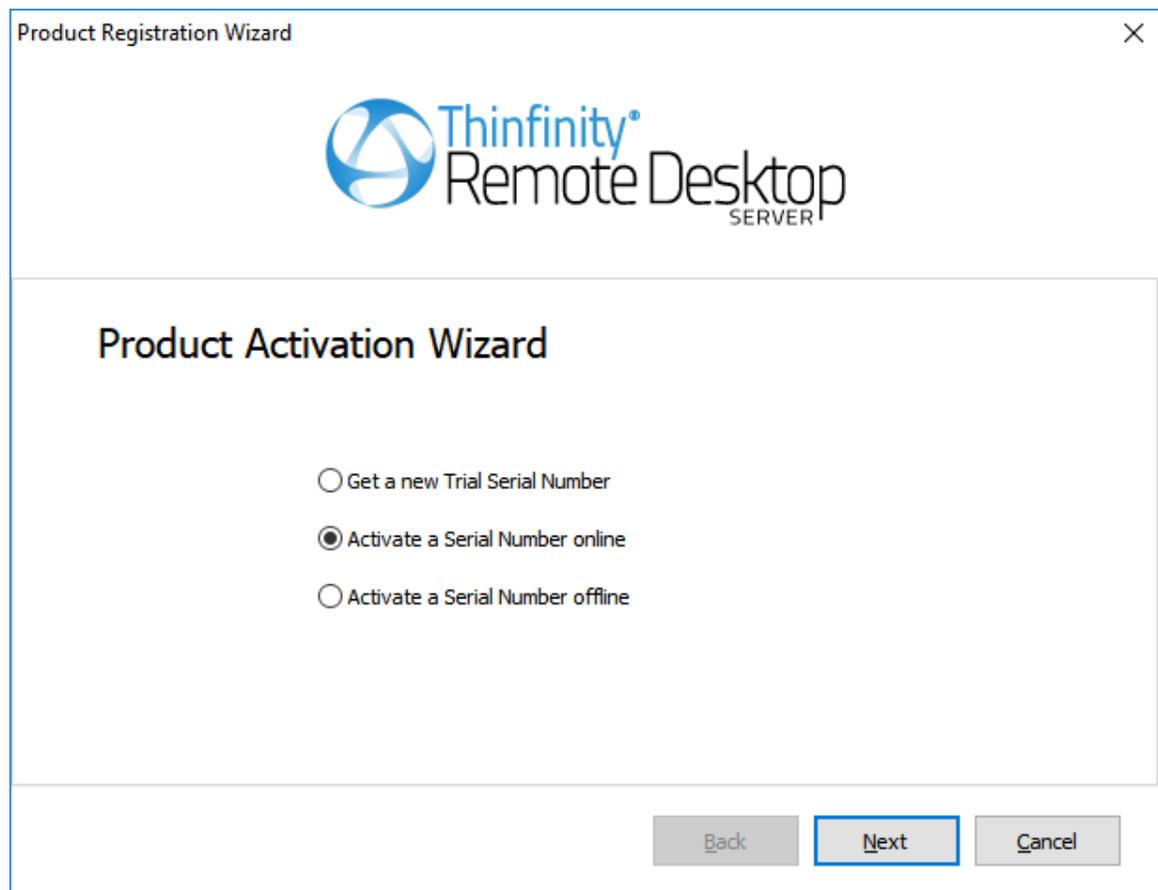
8.3.1 License Activation

This is how the License Manager should look once your license is registered:



Select	If you registered several serials on this server, press this button to select the key you wish to use.
Add	Press this button to enter your license information.
Remove	Press this button if you wish to deactivate the license on this machine. This will allow you to use the license somewhere else, or to re use the license after reinstalling Windows.
Close	Press this button to close the License Manager
Activity	Here you can verify in real time the amount of users consuming a license.

Pressing the 'Add' button will open the Product Registration Wizard:



Get a new Trial Serial Number	Select this option to receive a 30 day trial serial.
Activate a Serial Number Online	Select this option to register you Thinfinity® Remote Desktop Server serial.
Activate a Serial Number Offline	Select this option to register a license offline.

Read More:

- [Proxy Activation](#)
- [Get a new Trial Serial Number](#)
- [Activate a Serial Number Online](#)
- [Activate a Serial Number Offline](#)

8.3.1.1 Proxy Activation

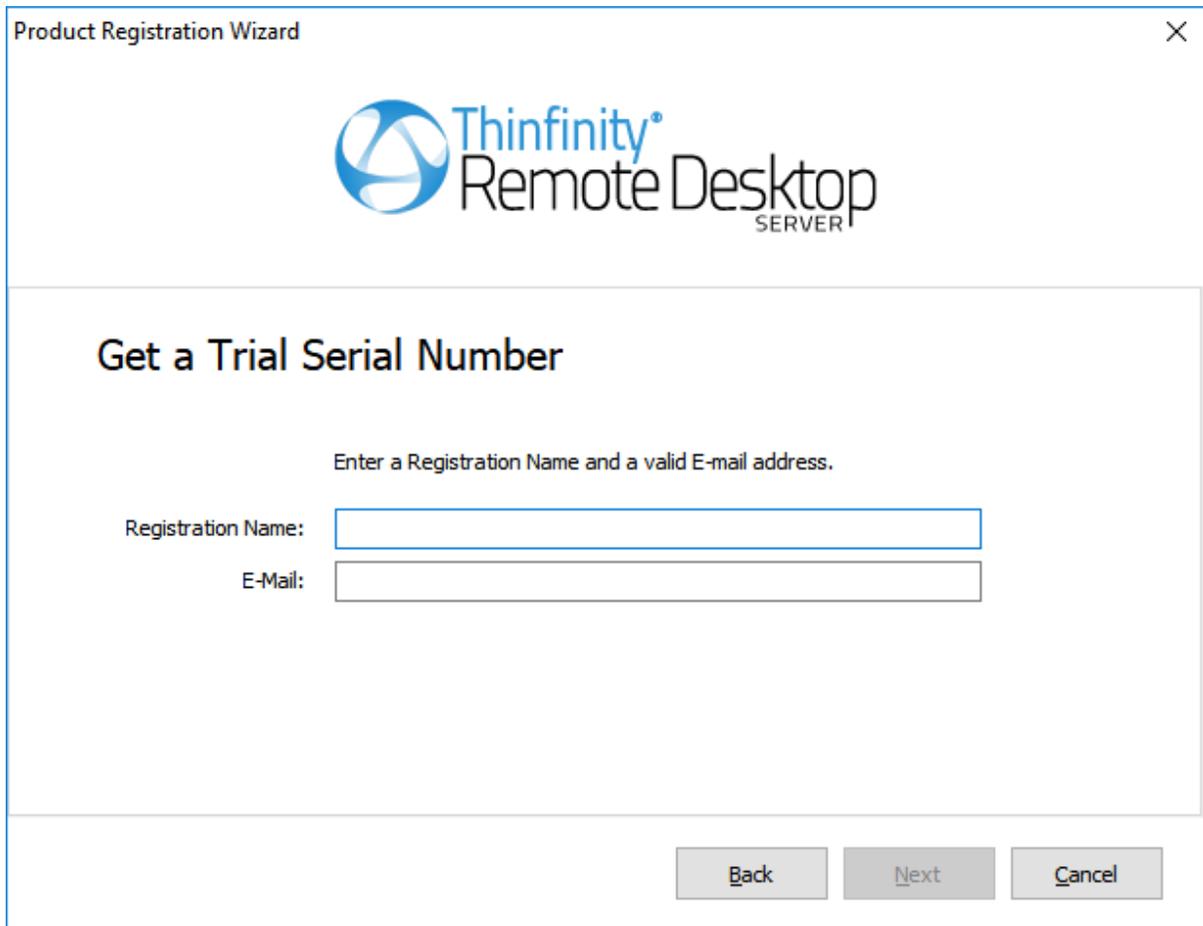
In order to register your license behind a proxy server you must register it using the License Server Administrator, for more information please contact support@cybelesoft.com.

Read More:

- [Get a new Trial Serial Number](#)
- [Activate a Serial Number Online](#)
- [Activate a Serial Number Offline](#)

8.3.1.2 Get a new Trial Serial Number

This option will allow you to request a 30 day trial license with unlimited access. You will be prompted to enter a valid name and e-mail address.



Product Registration Wizard

Thinfinity®
Remote Desktop
SERVER

Get a Trial Serial Number

Enter a Registration Name and a valid E-mail address.

Registration Name:

E-Mail:

Back Next Cancel

Once you filled this information hit 'Next' and check your in-box for the serial key.

Read More:

- [Proxy Activation](#)
- [Activate a Serial Number Online](#)
- [Activate a Serial Number Offline](#)

8.3.1.3 Activate a Serial Number Online

This is how the "Activate a Serial Number Online" windows looks:

Product Registration Wizard ×



Register Serial Number

Enter the e-mail address and serial number you received by e-mail.

E-Mail:

Serial:

Licensing Server URL:

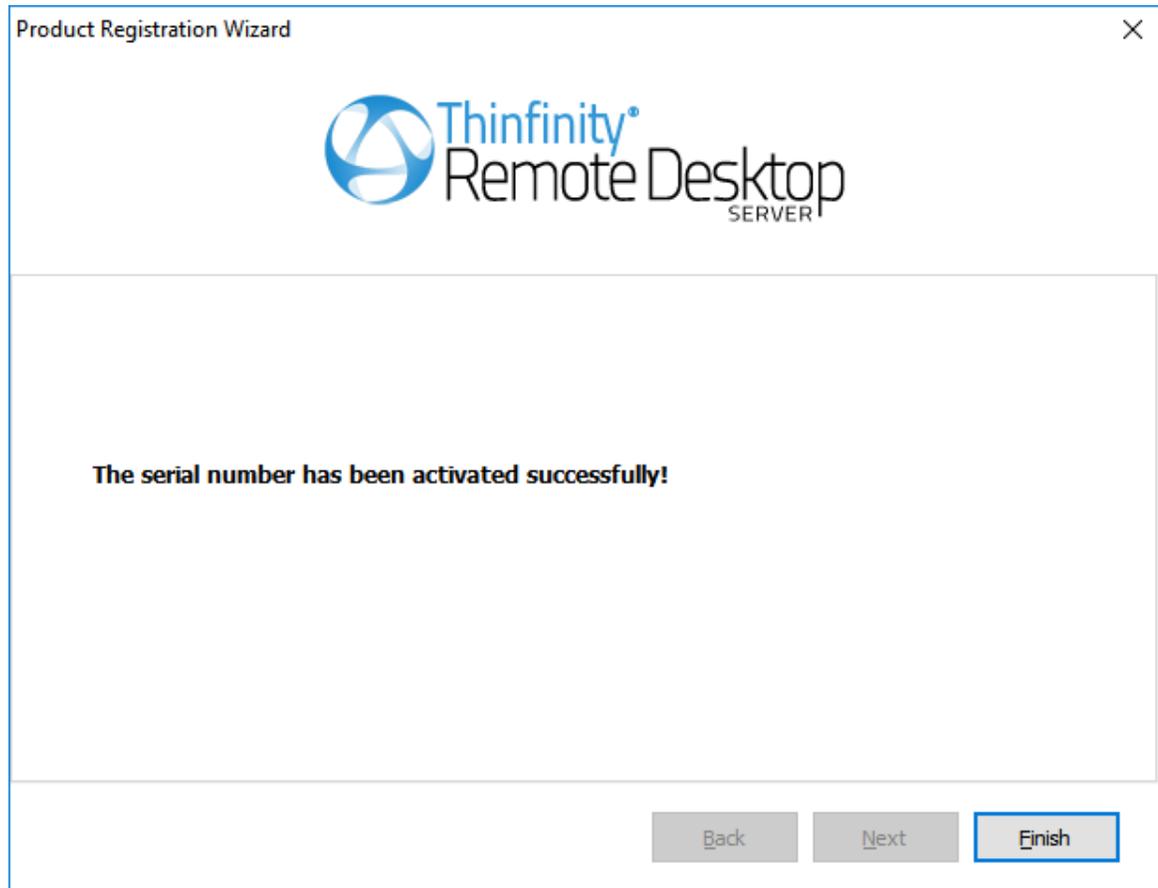
E-mail	Enter the e-mail address you've registered with.
Serial	Enter the serial information we provided you.
Licensing Server URL	If you installed the License Server administrator, enter the License Server URL. Otherwise leave this blank.*

If the license information is incorrect, you will see this warning: "The license information is invalid". In this case, please verify the following:

- That you are entering the exact email and Serial number sent to you. The best practice to do this correctly is to copy - paste it, being careful not to include any space after or before.
- That you have a working internet connection. If you intend to install it in a machine with no internet connection, you can try the [Manual Activation](#). If you have internet restrictions because of a proxy, try the [Proxy Activation](#).

If you need additional help, [contact us](#).

If the license information is correct, the License Manager will let you know that "The new license has been installed successfully" and its information will be show in the License Manager.



Read More:

- [Proxy Activation](#)
- [Get a new Trial Serial Number](#)
- [Activate a Serial Number Offline](#)

8.3.1.4 Activate a Serial Number Offline

Manual Activation is an activation option only for those cases when you want to activate Thinfinity® Remote Desktop Server in a machine that has no internet connection, or an internet connection restricted by heavy security policies that block a regular activation.

- If you haven't tried a regular activation, follow these instructions: [Activate a Serial Number Online](#).
- If your internet restrictions are caused by a proxy, follow these instructions: [Proxy Activation](#).

Before you continue with the steps to perform a manual activation, please [contact us](#).

Once you've selected Activate a Serial Number Offline. You will see the following pop up:

Product Registration Wizard



Register Serial Number

Enter the Serial Number to generate an offline activation key

Serial:

Activation Key:

Serial	Enter the license Serial number to generate the manual activation key
Generate Manual Key	After you have entered the serial number, press this button to generate the Manual Activation Key.
Manual Activation Key	After you press the 'Generate Manual Key' button, a Manual Activation Key will appear in this field. Send this Manual Activation Key to support .

Product Registration Wizard

Thinfinity®
Remote Desktop
SERVER

Activate license

Enter the validation key you've received by E-Mail

Back Next Cancel

Manual License	The support team will reply with the Manual License, a code that you will enter in the field above.
Next	Press this button once you have performed the previous steps to complete your license activation.

Read More:

- [Proxy Activation](#)
- [Get a new Trial Serial Number](#)
- [Activate a Serial Number Online](#)

8.3.1.5 Registering Your License With The License Server Manager

Registering the license against your license server manager is very similar to registering the license [Online](#).

Product Registration Wizard



Register Serial Number

Enter the e-mail address and serial number you received by e-mail.

E-Mail:

Serial:

Licensing Server URL:

Back Next Cancel

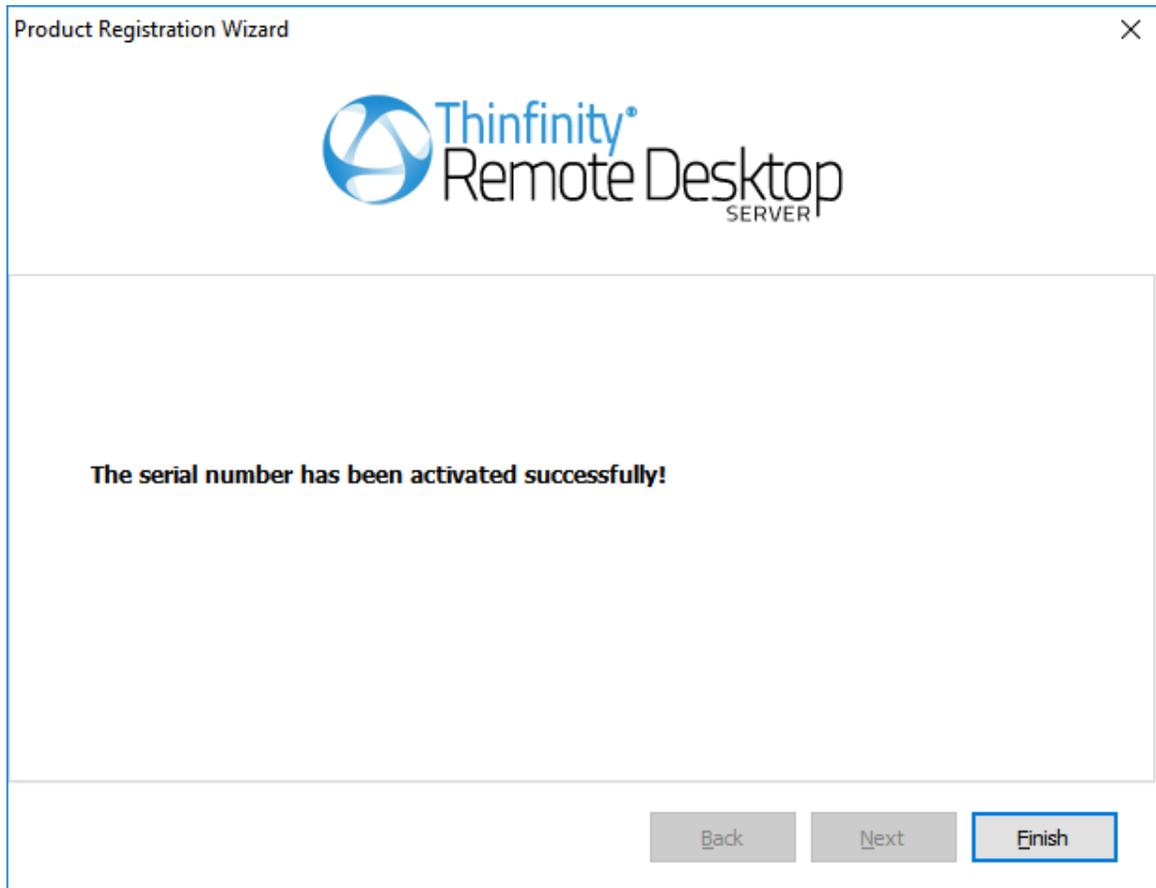
E-mail	Enter the e-mail address you've registered with.
Serial	Enter the serial information we provided you.
Licensing Server URL	Enter the License Server URL.

If the license information is incorrect, you will see this warning: "The license information is invalid". In this case, please verify the following:

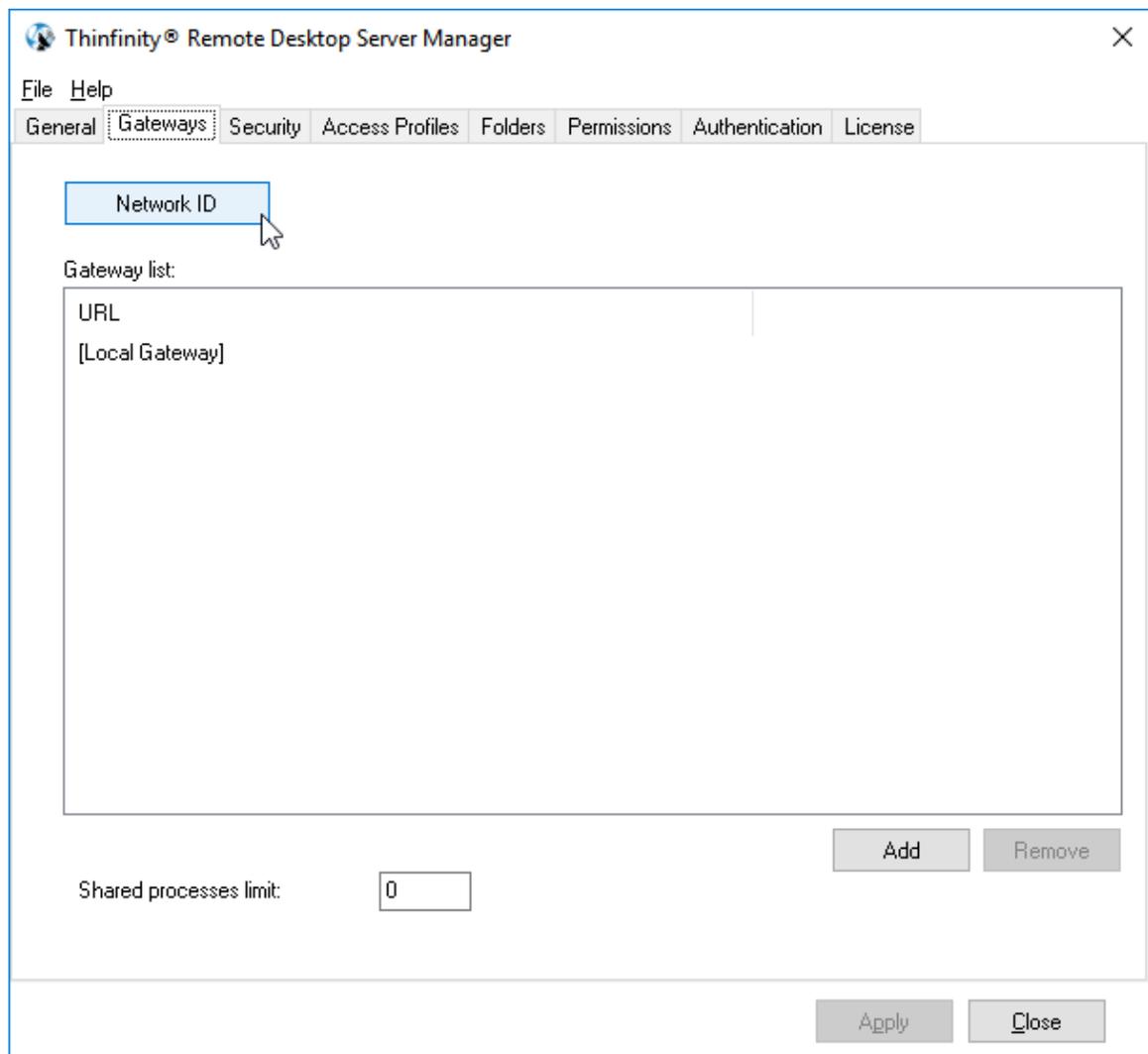
- That you are entering the exact email and Serial number sent to you. The best practice to do this correctly is to copy - paste it, being careful not to include any space after or before.
- That you have a working internet connection. If you intend to install it in a machine with no internet connection, you can try the [Manual Activation](#). If you have internet restrictions because of a proxy, try the [Proxy Activation](#).

If you need additional help, [contact us](#).

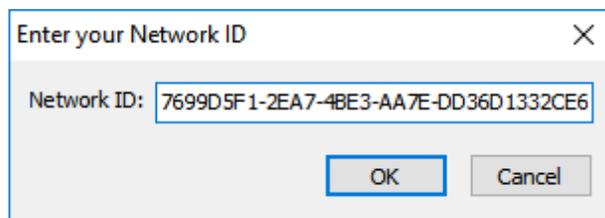
If the license information is correct, the License Manager will let you know that "The new license has been installed successfully" and its information will be show in the License Manager.



There is one additional step though, we have to modify the Network ID in the Gateway tab and make this match on all the servers you wish to share the license:



The Network ID doesn't necessarily have to follow the same format as the default value:



You can change this to any value, just ensure it matches all the servers.

Read More:

- [Proxy Activation](#)
- [Get a new Trial Serial Number](#)
- [Activate a Serial Number Offline](#)

8.4 Custom Settings

You can easily define some global parameters for all remote access connections, regardless of the selected profile by using `customSettings.js`. You can find this file in the installation directory, inside the 'webrdp' folder. It is an editable javascript file that contains a global variable called `customSettings`. The `customSettings` variable uses the *JSON* format to define a collection of attribute/value pairs with special parameters that are not available in the profile settings. You can open it with any text editor, like notepad.

These are the initial values:

Attribute	Default value	Description
createToolbar	true	Enables the Thinfinity Remote Desktop Toolbar creation.
toolbarVisible	false	Defines the initial toolbar visibility.
checkBeforeWindowClose	true	When false, bypasses the confirmation popup triggered in the <i>onBeforeUnload</i> event.
noSsnDialog	false	Disables the <i>share session</i> popup dialog display.

This collection can be extended with any other attribute of the `connect` JSON parameter, except for those that are relative to the connection —user, password and computer—. When extending the collection, the `overrideDefault` attribute must be set to `true`, as specified in the Thinfinity Remote Desktop [connect method](#) reference:

```
// GetThinRDP(serverURL, runRemote)
//   Creates a new ThinRDP instance
//   serverURL: substitute with the ThinRDP server URL (http[s]://[URL - IP]:port/)
//   runRemote: use to set ThinRDP mode
//       -- false-> Local (renders into this page)
//       -- true-> remote (posts connection data to postPage ("connection.html" as default)
mythinrdp = GetThinRDP("", true);
mythinrdp.connect({
  targetWindow: "rdpwindow",
  centered: true,
  overrideDefaults: true,
  ...
  ...
  ...
})
```

When starting a connection, Thinfinity Remote Desktop reads the values in `customSettings` and merges its parameter list with the profile settings, overriding the profile attributes with the `customSettings` variable values. Values set in the SDK [connect method](#) will also be overridden. This is a powerful tool that needs to be used carefully. Therefore, it is recommended to use

customSettings.js exclusively to set these special parameters, or when you need a centralized configuration to be shared among the totality of countless profiles. Remember: defining the configuration in each profile is always safer, as well as clearer.

In conclusion, the customSettings global variable offers a way to quickly apply general custom settings that will affect all the connections.

Read more:

- [The 'connect' Method](#)
- [Customizing the Toolbar](#)

8.4.1 Extend the Remote Desktop's Toolbar

The toolbar.shortcuts Structure

To extend the toolbar with new Send Key options, you have to use the toolbar JSON structure. It contains a javascript object array named shortcuts where each object represents a "Send Key..." menu option and has two fields:

- "text": It's the option caption text (String).
- "keys": It's an object array, where each element contains a keyboard action.

Why is "keys" an array? Because many times you need to press more than one key to create a "keyboard gesture". The best example of this are the [CTRL]+any key combinations, where the keyboard sequence is...

- Press [CTRL] (keydown)
- Stroke any other key (keydown, keypress, keyup)
- Release [CTRL] (keyup)

The same occurs with [SHIFT], [ALT], the [SHIFT]+[ALT], [CTRL]+[SHIFT] combinations, etc.

Other options can be added to supply and/or complement existing actions, or to add useful keystroke sequences to help your users.

To do this, each key action has two fields: a type (action field) and a value (key or text field, depending on the current value of action).

The following table explains each action in detail:

Action name	Meaning	Associated Field
down	It represents a keydown (just the key down, without the key release).	key
stroke	It represents the complete keystroke sequence action, from the keydown to the keyup (when you press and release a key).	key
up	It represents a keyup (the key release)	key
type	Send text	text

And these are the value types:

Value field	Meaning
key	Numeric code for the key.
text	A text to be remotely "typed".

The following example shows these actions and values in action:

```

"toolbar": {
  "shortcuts": [
    {
      "text": "Help (F1)",
      "keys": [
        { "action": "stroke", "key": 0x70 } // F1
      ]
    },
    {
      "text": "Find",
      "keys": [
        { "action": "down", "key": 0x11 }, // CTRL
        { "action": "stroke", "key": 0x46 }, //F
        { "action": "up", "key": 0x11 } // CTRL
      ]
    },
    {
      "text": "Type 'Hello'",
      "keys": [
        { "action": "type", "text": "Hello" }
      ]
    },
    {
      "text": "Find 'Hello'",
      "keys": [
        { "action": "down", "key": 0x11 }, // CTRL
        { "action": "stroke", "key": 0x46 }, //F
        { "action": "up", "key": 0x11 }, // CTRL
        { "action": "type", "text": "Hello" },
        { "action": "stroke", "key": 0x0D } //ENTER
      ]
    }
  ]
}

```

In this example, the first shortcut sends an F1, the second triggers a find/search (a [CTRL]+F), the third just types "Hello" and the fourth combines the second and third examples to process a find of "Hello".

There are two ways to add new toolbar options:

- Adding the new options to the customSettings global variable, whose settings will affect all users and

all connections in the Thinfinity Remote Desktop server installation.

- Adding the new options to the connection parameters, if you are an integrator who is using the sdk.html page or any other page with an embedded remote desktop.

Using customSettings to Extend the Remote Desktop's Toolbar

The customSettings global variable is a JSON object defined in the customSettings.js file, which you'll find in the Thinfinity Remote Desktop Server installation web folder. This variable, a Javascript object, has attributes to set or modify connection features, including some related to the toolbar. This structure doesn't have default attributes (they are disabled in the source code) and looks like this:

```
var customSettings = {
  /*
    "createToolbar": true,           // Creates ThinRDP toolbar
    "toolbarVisible": false,       // ThinRDP toolbar starts expanded (visible)
    "checkBeforeWindowClose": true, // when false, skips the user confirmation popup of
the onBeforeUnload event
    "noSsnDialog": false,          // avoids the share session popup dialog
    "noShowPopupsOnClose": false   // when true, skips the session closed message popup
  */
};
```

To add the toolbar.shortcuts structure to customSettings you'll just have to do this:

```
var customSettings = {
  ...
  "toolbar": {
    "shortcuts": [ ... ]
  }
}
```

Modifying Parameters in an SDK Custom Connection

If you are using the Thinfinity Remote Desktop SDK and you don't want to change the toolbar for all users, or if you want to modify it in a conditional way (e.g. depending on a user identification or profile), you can add the toolbar.shortcuts structure to the connection parameters. The difference with the previous example is that this addition is not for all users. This change will only affect SDK users, and optionally you can add this data conditionally.

Add the `toolbar.shortcuts` structure to the connection parameters for all SDK users:

```
var mythinrdp = null;

$(document).ready(function () {
    mythinrdp = GetThinRDP("", false);
    mythinrdp.connect({
        targetWindow: "myiframe",
        centered: true,
        ...
        // Custom shortcuts (Toolbar Actions/Send Keys...)
        "toolbar": {
            "shortcuts": [ ... ]
        }
    });
    ...
});
```

For a selective `toolbar.shortcuts` addition, you could do something like this:

```
var mythinrdp = null;

$(document).ready(function () {
    var params = {
        targetWindow: "myiframe",
        centered: true,
        ...
        ...
    };

    // hypothetical functions created by you
    if (userProfile(CurrentUser()).hasExtendsSendKeys) {
        params["toolbar"] = { "shortcuts": [ ... ] };
    }

    mythinrdp = GetThinRDP("", false);
    mythinrdp.connect(params);
    ...
});
```

8.5 Customizing the Toolbar

By default, the Thinfinity® Remote Desktop Server toolbar displays the wider range of options within reach for the end users. However, as an administrator or integrator, you might want to restrict the end user from accessing some of these options, or all of them. Thinfinity Remote Desktop has a method that allows you to tweak the toolbar according to your preferences. These settings will be applied before the connection occurs and will affect all users and all connections in the Thinfinity

Remote Desktop server installation.

General toolbar customization parameters

The `customSettings` global variable has two parameters that affect the complete toolbar: The **`createToolbar`** parameter enables the Thinfinity Remote Desktop Toolbar creation. Setting it to false will result in a Thinfinity® Remote Desktop Server connection with no toolbar at all. This might be useful if you want to restrict the user from all the options in the toolbar. The **`toolbarVisible`** parameter defines the initial toolbar visibility. When `toolbarVisible` is true, the toolbar will appear expanded upon establishing the connection; and when `toolbarVisible` is false, the toolbar will start collapsed.

Hiding toolbar components

When connecting to an application you might want to restrict the user to access the task manager by sending the [CTRL]+[SHIFT]+[ESC] keys. Or, perhaps, you might want to enable file transfer for downloading files without providing access to the file manager. For all of these cases, you have a way to programmatically define the exact toolbar options that will be excluded. The **`toolbarRestrictions`** `customSettings` property is an array that contains the full name of all the toolbar options you might want to restrict.

If you want a simple and straightforward configuration, you can add these parameters in the `customsettings.js` file. The options that you set through this method will affect all the Thinfinity® Remote Desktop Server connections, regardless of the session, and will also override SDK [connect method](#) settings. [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](#).

8.5.1 Using customsettings.js

The `customsettings.js` file is distributed with the installation of Thinfinity® Remote Desktop Server. You will find this file in the 'webrdp' folder in the Thinfinity® Remote Desktop Server installation directory.

`customsettings.js` is a javascript file that contains javascript code which is read by the client's browser when they access Thinfinity® Remote Desktop Server and then communicates with Thinfinity® Remote Desktop 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 Thinfinity® Remote Desktop Server toolbar
  "toolbarVisible": false   // Thinfinity® Remote Desktop Server 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 these examples, the comments are being used to describe the functions and to reference the name options have in the Thinfinity® Remote Desktop Server toolbar for users.

If you want to add the `toolbarRestrictions` parameter, add a comma after the last parameter (in this case `toolbarVisible`) and include in the `toolbarRestrictions` list only the buttons you want to be excluded from the toolbar. Follow the following format:

```
var customSettings = {
  "createToolbar": true,           // Create Thinfinity® Remote Desktop Server
  toolbar
  "toolbarVisible": false,       // Thinfinity® Remote Desktop Server toolbar
  starts expanded (visible)
  "toolbarRestrictions": [
    "actionsMenuBtn",           // "Actions"
    "actionsMenuBtn.refresh",   // "Refresh"
    "actionsMenuBtn.ssnShareBtn", // "Share session"
    "actionsMenuBtn.sendKeysBtn", // "Send Keys..."
    "actionsMenuBtn.sendKeysBtn.ctrlAltDelBtn", // "Ctrl + Alt + Del"
    "actionsMenuBtn.sendKeysBtn.ctrlEscBtn", // "Ctrl + Esc"
    "actionsMenuBtn.sendKeysBtn.shiftCtrlEscBtn", // "Shift + Ctrl + Esc"
    "actionsMenuBtn.sendKeysBtn.windowsExplorerBtn", // "Shell Explorer"
    "actionsMenuBtn.sendKeysBtn.runBtn", // "Run"
    "actionsMenuBtn.sendKeysBtn.altTabBtn", // "Alt + Tab"
    "actionsMenuBtn.sendKeysBtn.altShiftTabBtn", // "Alt + Shift + Tab"
    "actionsMenuBtn.sendKeysBtn.altEscBtn", // "Alt + Esc"
    "actionsMenuBtn.sendKeysBtn.leftWinBtn", // "Left Win Key"
    "actionsMenuBtn.sendKeysBtn.rightWinBtn", // "Right Win Key"
    "actionsMenuBtn.takeScreenshotBtn", // "Take Screenshot"
    "fileMenuBtn", // "File transfer"
    "fileMenuBtn.fileManBtn", // "File Manager"
    "fileMenuBtn.uploadBtn", // "Upload"
    "fileMenuBtn.downloadBtn", // "Download"
    "optionsMenuBtn", // "Options"
    "optionsMenuBtn.scaleBtn", // "Scale"
    "optionsMenuBtn.imgQualityBtn", // "Image Quality"
    "optionsMenuBtn.imgQualityBtn.imgQualityHigh", // "Highest"
    "optionsMenuBtn.imgQualityBtn.imgQualityOptimum", // "Optimum"
    "optionsMenuBtn.imgQualityBtn.imgQualityGood", // "Good"
    "optionsMenuBtn.imgQualityBtn.imgQualityFastest", // "Fastest"
    "optionsMenuBtn.keyboardMode", // "Disable Shortcuts"
    "optionsMenuBtn.fullScreen", // "Full Screen"
    "disconnectBtn", // "Disconnect"
  ]
};
```

```
}; ]
```

When you are done, close the file and save the settings. Don't change the file's location. The changes will be taken by Thinfinity® Remote Desktop Server immediately. Remember that settings in customsettings.js file will override those in the [connect method](#).

The toolbar customization is not the only thing you can do with customsettings.js. Read more about all the parameters you can include in [Custom Settings](#).

8.5.2 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 [Thinfinity® Remote Desktop Server SDK library](#).

Here is the syntax for the toolbar parameters:

```
mythinrdp.connect({
  createToolbar:    true,
  toolbarVisible:  true,
  toolbarRestrictions: [
    "actionsMenuBtn",           //"Actions"
    "actionsMenuBtn.refresh",   //"Refresh"
    "actionsMenuBtn.ssnShareBtn", //"Share session"
    "actionsMenuBtn.sendKeysBtn", //"Send Keys..."
    "actionsMenuBtn.sendKeysBtn.ctrlAl//"Ctrl + Alt + Del"
    tDelBtn",
    "actionsMenuBtn.sendKeysBtn.ctrlEs//"Ctrl + Esc"
    cBtn",
    "actionsMenuBtn.sendKeysBtn.shiftC//"Shift + Ctrl + Esc"
    trlEscBtn",
    "actionsMenuBtn.sendKeysBtn.window//"Shell Explorer"
    sExplorerBtn",
    "actionsMenuBtn.sendKeysBtn.runBtn//"Run"
    ",
    "actionsMenuBtn.sendKeysBtn.altTab//"Alt + Tab"
    Btn",
    "actionsMenuBtn.sendKeysBtn.altShi//"Alt + Shift + Tab"
    ftTabBtn",
    "actionsMenuBtn.sendKeysBtn.altEsc//"Alt + Esc"
    Btn",
    "actionsMenuBtn.sendKeysBtn.leftWi//"Left Win Key"
    nBtn",
    "actionsMenuBtn.sendKeysBtn.rightW//"Right Win Key"
    inBtn",
    "actionsMenuBtn.viewOptionsBtn", //"View params & layout"
    "fileMenuBtn",                  //"File transfer"
    "fileMenuBtn.fileManBtn",       //"File Manager"
    "fileMenuBtn.uploadBtn",        //"Upload"
    "fileMenuBtn.downloadBtn",      //"Download"
    "optionsMenuBtn",              //"Options"
    "optionsMenuBtn.scaleBtn",       //"Scale"
    "optionsMenuBtn.imgQualityBtn",  //"Image Quality"
    "optionsMenuBtn.imgQualityBtn.imgQ//"Highest"
    HighestBtn",
  ],
});
```

```
        "optionsMenuBtn.imgQualityBtn.imgQ//\"Optimal\"
        OptimalBtn",
        "optionsMenuBtn.imgQualityBtn.imgQ//\"Good\"
        GoodBtn",
        "optionsMenuBtn.imgQualityBtn.imgQ//\"Poor\"
        PoorBtn",
        "optionsMenuBtn.keyboardMode",    //\"Disable Shortcuts\"
        "disconnectBtn",                  //\"Disconnect\"
    ]
}
```



Please note that in this example all the options for toolbarRestrictions are included, which would result in a blank toolbar. Include in the toolbarRestriction parameter only the buttons you want to exclude from the Thinfinity® Remote Desktop Server toolbar.

Remember that these settings will be overridden by those in the customsettings.js file.

8.6 Remote FX

The RemoteFX Codec implemented in Thinfinity® Remote Desktop Server enables Microsoft® RemoteFX™, which is an RDP extension. Remote FX attempts to provide an experience similar to a local computer, enabling the delivery of a full Windows user experience. This enables end users to run graphical applications on a virtual machine: Youtube videos, games, animations or moving images can be seen with much more fluidity than when using the RDP traditional mode.

Changing the data compression and transmission, it checks screen content changes between frames and transmits the changed bits for encoding; it also tracks network speed and then dynamically adjusts according to the available bandwidth.

Thinfinity® Remote Desktop Server is set by default to choose the best user experience. The 'Enable Remote FX' option is set to true by default and comes into effect when the host and guest are configured properly. Otherwise, the Thinfinity® Remote Desktop Server connection will be established without Remote FX.

When Remote FX is enabled, it will override the settings in the 'Experience' tab and the 'Color Depth' option in the 'Display' tab. All the settings in the 'Experience' tab will work as if they were enabled and the color depth will be 32, regardless of the values configured in Thinfinity® Remote Desktop Server, because they are part of the RemoteFX experience.

Remote FX is a Microsoft extension that has several requirements in order to work. When Remote FX is working with traditional RDP, that means it's ready to be enabled with Thinfinity® Remote Desktop Server using our Remote FX Codec. Please contact Microsoft Support to get it started!

If you are using Windows Server 2012 in the host, you will also need to configure some policies for RemoteFX to work. If these policies are not enabled the connection will not use Remote FX nor tell the user or administrator, either

Follow these steps to configure Windows Server 2012 to work with Thinfinity® Remote Desktop Server Remote FX Codec

- 1) Run gpedit.msc
- 2) Search for the RDP settings in the "Local Group Policy Editor": Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Remote Session Environment"
- 3) Set the "Enable RemoteFX encoding for RemoteFX clients designed for Windows Server 2008 R2 SP1" option to [Enabled]
- 4) Set the "Limit maximum color depth" option to [Enabled] and the "Client Depth" option to [Client Compatible]

These are the required features your browser must support in order to use RemoteFX:

- WebSockets.
- ArrayBuffers and the Uint8Array, Uint16Array, Uint32Array types

Read more:

- [Enable Remote FX in the web interface](#)
- [Enable Remote FX for profiles](#)
- [Enable Remote FX using the SDK library](#)

8.7 Save Session

Thinfinity® Remote Desktop Server introduces this feature to help users have a record of their actions in the Thinfinity® Remote Desktop Server session. The sessions are available for watching within the Thinfinity® Remote Desktop Server web interface, from any HTML5 browser.

You can now record the sessions in a lightweight format that will be interpreted by Thinfinity® Remote Desktop Server and available for watching seamlessly in the browser. You can enable the recording of the session from each profile or from the web interface before connecting. The sessions will be stored for each user and will be displayed for the user with the appropriate permissions. As a user you can have permission to either view only sessions you have recorded under the same username, or sessions recorded under any username; both in the same Thinfinity® Remote Desktop Server server.

Read more:

- [Record a Session](#)
- [Play Recorded Sessions](#)

8.7.1 Record a Session

Enable a user's permission to play saved sessions in the manager's ['Permissions' tab](#). This setting is also necessary for a user to record sessions. This permission will be applied to the user that authenticates against Thinfinity Remote Desktop Server, not the rdp session user.

If the user has permission to record a session, then it can be enabled in the ['Advanced' tab](#) of an access profile or the [web interface](#). This parameter is also available in the connect method.

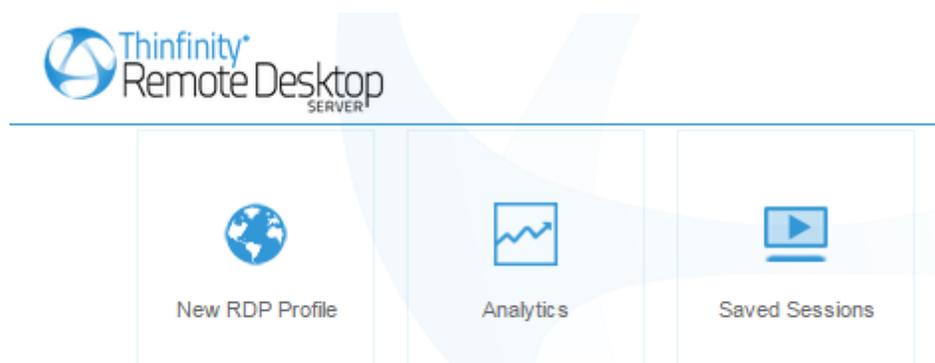
After checking this option, the connections will be recorded and listed to be viewed by the corresponding users.

Read more:

- [Play recorded sessions](#)

8.7.2 Play Recorded Sessions

When a user has the appropriate permissions to see sessions, they will see an icon together with the profiles.



By clicking on this icon, you will access the Saves Sessions screen:

Saved Sessions

Host	User	Start Date	End Date	Duration	
▶ herman leaderadmin	leadersoft\iloew	17/3/2015 18:06:44	17/3/2015 18:08:01	00:01:16.906	☐
▶ ym-server iloew	leadersoft\iloew	17/3/2015 18:06:39	17/3/2015 18:06:39	01:00:39.026	☐
▶ ym-server iloew	leadersoft\iloew	17/3/2015 18:05:33	17/3/2015 18:05:33	00:50:00.107	☐
▶ ym-server iloew	leadersoft\iloew	17/3/2015 18:05:26	17/3/2015 18:05:26	00:07:05.030	☐
▶ ym-server iloew	leadersoft\iloew	17/3/2015 18:05:17	17/3/2015 18:05:17	00:01:00.070	☐
▶ ym-server iloew	leadersoft\iloew	17/3/2015 18:05:05	17/3/2015 18:05:05	00:10:00.310	☐
▶ ym-server	leadersoft\iloew	14/10/2015 18:08:47	14/10/2015 18:09:15	00:00:28.127	☐

▶	Play a saved session.
↻	Refresh the session view.
⌵	Filter by user or by host name/ip address.
🗑️	Delete a saved session.

8.8 Multitouch Redirection

Multi-touch Redirection for desktop touch devices:

Thinfinity® Remote Desktop Server now supports Multi-touch input in desktop touch devices. This means you can use touch options remotely, as long as the Windows version of the remote desktop supports touch input.

Where multitouch is supported, the remote Windows desktop will receive your touch input and interpret it as if you were touching the remote screen.

Multi-touch Redirection will work in desktop touch devices as long as the browser supports touch features and the OS of the remote desktop can interpret it. Otherwise, or if you disable this option, all touch input will be interpreted as mouse movements.

Thinfinity® Remote Desktop Server will redirect the touch of up to 10 simultaneous fingers for it to be interpreted by Windows.

Mouse Gestures for mobile devices:

When you are using a mobile device, the mouse movements are replaced with touch. Using mouse gestures, you can combine mouse movements and clicks which Thinfinity® Remote Desktop Server recognizes as a specific command. Mouse gestures can provide quick access to common functions of a program. They can also be useful for people who have difficulties typing on a keyboard.

Read More

- [Multi-touch options in the web interface.](#)
- [Multi-touch options per profile in the Thinfinity® Remote Desktop Server Manager.](#)
- [Gestures.](#)

8.9 Enhanced Browser and DPI Support

Among the wide range of valid resolutions that Thinfinity Remote Desktop offers, the most commonly used—for its flexibility and simplicity—is “Fit to Browser”. This configuration allows you to adjust the remote desktop/remote application to fit the available browser size. However, when it comes to accessing a desktop from different devices, the sometimes huge differences between screen sizes and pixel resolutions (i.e. iPhone 4 vs a 27 inch iMac Retina Display) make it impossible to have a simple rule to determine the best remote desktop size. Even when the application is adjusting properly to the available size, the screen rendered might still look tiny or disproportionate, making the user experience not as satisfactory as expected.

Tailoring "Fit to browser"

Now, using a new configurable browser detection ruleset, we can tailor the way we want to see of the remote desktop/application on every device. This ruleset allows you to specify rules that will detect the web browser, device and display characteristics, and set parameters that adjust the remote desktop/application resolution according to your own taste.

The main characteristics that need to be taken into account are:

- The browser User Agent, that tells about the web browser and device
- The device pixel ratio, that tells about the real display resolution
- The device display size
- The display orientation (landscape or portrait)

The browser detection ruleset is stored in a file with entries that contain specifications (rules) that match general or specific devices. Each entry (model) can inherit matching parameters (properties) from a more general model. For example, you can define an iOS model and an iPhone4 can inherit the iOS model properties.

A default ruleset file named BrowserRules.ini is installed in the Thinfinity Remote Desktop program folder. Then, if it doesn't exist there yet, it is copied to "\programData\Cybele Software\Thinfinity \Remote Desktop Server\" and renamed as Thinfinity.RemoteDesktop.BrowserRules.ini. You can safely customize this file as it won't be overridden with a program update.

The structure of this file is as follow:

```
[default]
min-width = 640
min-height = 480
max-width = 2560
max-height = 1600
max-device-pixel-ratio = 1

[mobile]
parent-model = default
match-mobile = true
max-device-pixel-ratio = 2
```

Note: for these setting to apply, the connection's 'Resolution' property must be set to 'Fit to browser'.

Configure this setting in [the 'Display' tab of the Access Profiles](#), or [the 'Display' tab of the web](#)

[interface](#).

Or, if you are using the [SDK](#), set:

```
resolution:"fittobrowser",
```

Read More:

- [Model Inheritance](#)
- [Property Reference](#)
- [The Calculation Process](#)
- [Examples](#)

8.9.1 Model Inheritance

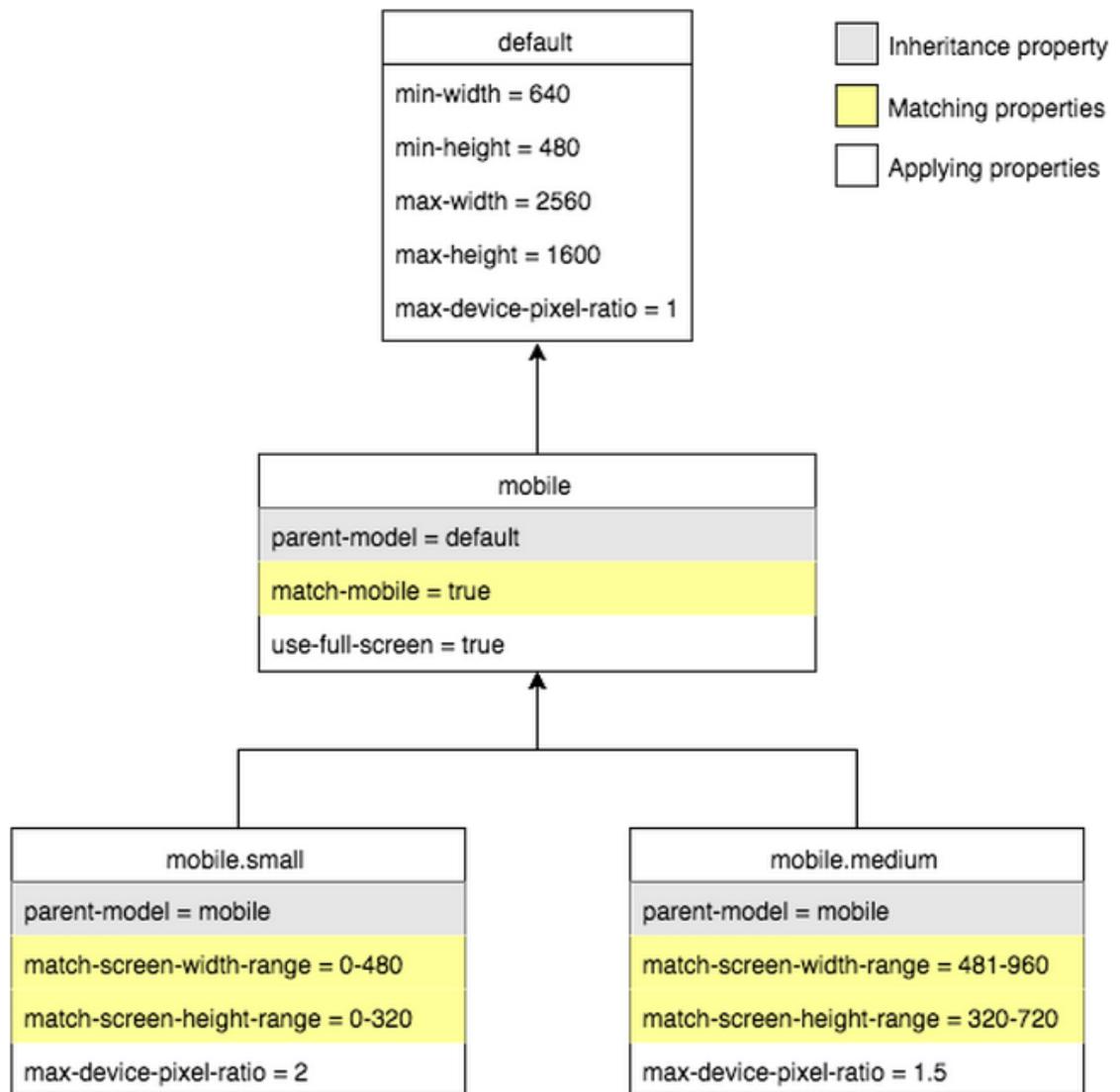
A section defines a **model**, and each model contains a set of properties divided in two groups: *matching properties* and *applying properties*.

Models are organized in an inheritance tree. The relationship between models is defined by a special property rule called *parent-model*, present in all models except in the **[default]** model, which is the tree's root node and includes some basic properties.

Every other model must directly or indirectly inherit from the **[default]** model. Also, each model contains its own rules that match general or specific devices, and inherits all specifications (including matching parameters) from its ancestors.

When more than one criteria is met for a device, a scoring system is used to resolve this conflict.

This is the in-the-box models tree:

**Read More:**

- [Property Reference](#)
- [The Calculation Process](#)
- [Examples](#)

8.9.2 Property Reference

Properties can be divided in two groups: *matching properties* and *applying properties*.

Matching properties are those used to test the browser and device properties (such as the browser user agent, the device pixel ratio, the display orientation width and height, etc.) in order to choose the best model for each case.

<code>match-device-pixel-ratio</code>	Matches any device with a specific pixel ratio.
<code>match-mobile</code>	Matches any mobile device.
<code>match-orientation</code>	Matches any device with the specified orientation: landscape or portrait.
<code>match-screen-height-range</code>	Matches any device with a screen height in the specified range. This range is expressed as From-To (for example, 900-1200).
<code>match-screen-width-range</code>	Matches any device with a screen width in the specified range. This range is expressed as From-To (for example, 400-600).
<code>match-screen-height</code>	Matches any device with a specified screen height.
<code>match-screen-width</code>	Matches any device with a specified screen width.
<code>match-user-agent</code>	Matches devices by comparing the device browser user agent to the string value supplied. This string is a regular expression.

Applying properties are those used to determine the final size and resolution.

Use the `parent-model` property to set the parent model:

<code>parent-model</code>	Establish the parent model for this model.
---------------------------	--

The following properties deal with the display resolution:

<code>device-pixel-ratio</code>	Overrides the original device pixel ratio, scaling the content accordingly.
<code>max-device-pixel-ratio</code>	This property determines the maximum device pixel ratio accepted. The lesser of the device's device pixel ratio and this value is applied to scale the display.

The following properties deal with the screen size of the remote desktop, in pixels. You can determine it by setting the actual height and width, or by establishing maximum and minimum values for these properties.

<code>height</code>	Remote desktop height.
<code>width</code>	Remote desktop width.
<code>max-height</code>	Remote desktop maximum height.
<code>max-width</code>	Remote desktop maximum width.
<code>min-height</code>	Remote desktop minimum height.
<code>min-width</code>	Remote desktop minimum width.

The following properties allow you to specify device screen areas that will never be used for displaying the remote connection, such as when a browser or device bar cannot be hidden and uses up screen space. These margins will be excluded for screen size calculations.

<code>margin-left</code>	Width of an area at the left of the device screen that will not be used for displaying the remote desktop.
<code>margin-bottom</code>	Width of an area at the bottom of the device screen that will not be used for displaying the connection.
<code>margin-right</code>	Width of an area at the right of the device screen that will not be used for displaying the connection.
<code>margin-top</code>	Width of an area at the top of the device screen that will not be used for displaying the connection.

Miscellaneous properties:

<code>use-full-screen</code>	For mobile only. If the device's browser supports the full-screen mode, this property indicates the remote desktop size should be calculated to occupy the whole screen. When not in full screen, the content will be scaled.
------------------------------	---

Read More:

- [The Calculation Process](#)
- [Examples](#)

8.9.3 The Calculation Process

In order to choose a model from the ruleset, Thinfinity uses the client device type, dimensions, resolution, orientation and browser:

1. If match-mobile exists, it tests if device is a mobile.
2. If match-user-agent exists, it tests the browser's User Agent.
3. If match-device-pixel-ratio exists, it tests the device's pixel ratio.
4. If match-orientation exists, it tests the device's orientation.
5. If match-screen-width-range or match-screen-height-range exist, it tests to see if the screen size is in range.
6. If match-screen-width or match-screen-height exist, it tests the exact screen size.

Once the model is selected, the parameters are applied in this way:

1. If the width and height properties exist, then it applies them.
2. If the browser width is less than the min-width, it applies min-width.
3. If the browser height is less than the min-height, it applies min-height.
4. If the browser width is greater than the max-width, it applies max-width.
5. If the browser height is greater than the max-height, it applies max-height.
6. If a specific device-pixel-ratio was specified, it applies it.
7. If a max-device-ratio was specified, it takes the minimum of the real device pixel ratio and max-device-ratio property and applies it.

Read More:

- [Examples](#)

8.9.4 Examples

This example shows a possible ruleset and how it will affect different devices:

```
[default]
min-width = 640
min-height = 480
max-width = 2560
max-height = 1600
max-device-pixel-ratio = 1

[mobile]
parent-model = default
match-mobile = true
max-device-pixel-ratio = 2

[ipad]
parent-model = mobile
match-user-agent = ipad

[iphone4]
parent-model = mobile
match-user-agent = iphone
match-screen-width = 480
```

```
match-screen-height = 320  
device-pixel-ratio = 1.5
```

In this case, when connecting with an ipad, the following models will be matched:

[default]: This model applies to all devices.

[mobile]: The ipad will match the match-mobile property.

[ipad]: The ipad will match the user agent keyword 'ipad' specified in the match-user-agent property.

The resulting properties for this device will be:

```
min-width = 640  
min-height = 480  
max-width = 2560  
max-height = 1600  
max-device-pixel-ratio = 2
```

Using the same ruleset, when connecting with an iphone4, the following models will be matched:

[default]: This model applies to all devices.

[mobile]: The iphone will match the match-mobile property.

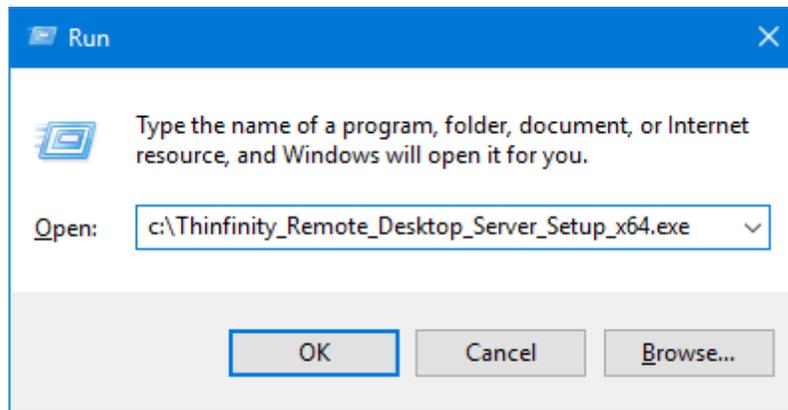
[iphone4]: The iphone will match the user agent keyword 'iphone' specified in the match-user-agent property, together with the match-screen-width and match-screen-height properties. An iphone6, with a screen width of 667px, and a screen height of 375px, would match the 'iphone' user agent keyword, but not the size.

The resulting properties for this device will be:

```
min-width = 640  
min-height = 480  
max-width = 2560  
max-height = 1600  
max-device-pixel-ratio = 2  
device-pixel-ratio = 1.5
```

8.10 Silent Install Options

The Thinfinity Remote Desktop Server installation can be run in 'silent' mode, that is, without the need for user interaction. This can be useful if you are a system administrator and you want to automate the Thinfinity Remote Desktop Server installation or if you are deploying it over your local network.



Thinfinity Remote Desktop Server Line Switches

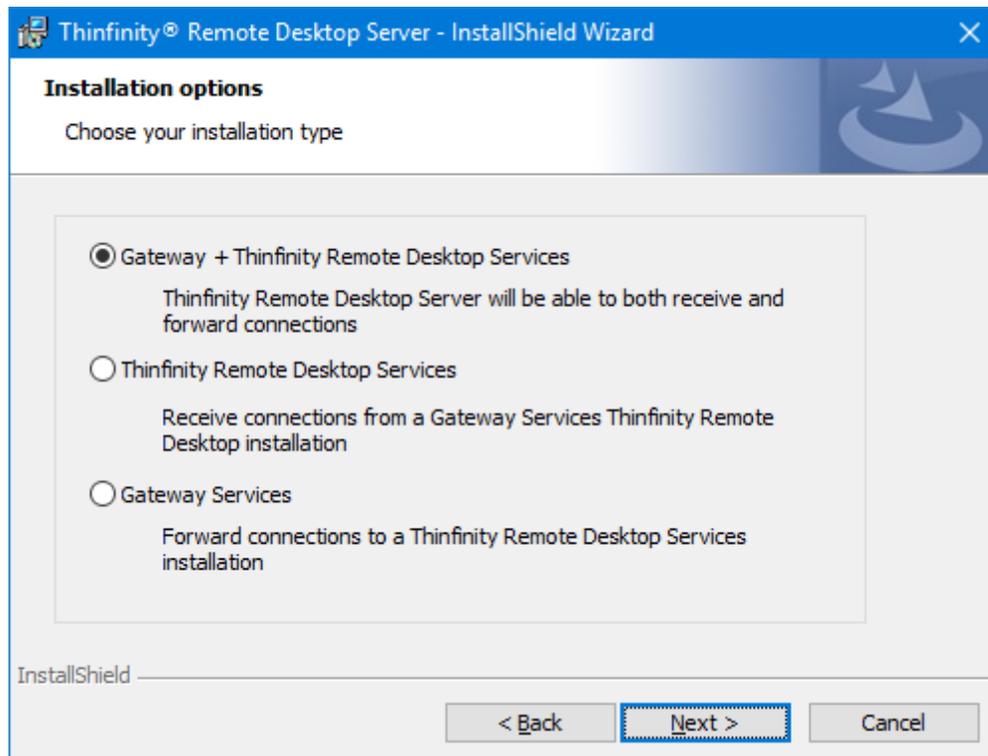
In order to perform a silent installation, use this command line:

```
c:\Thinfinity_Remote_Desktop_Server_Setup_x64.exe /s /v/qn
```

These are additional command line switches that you can pass on to the setup file:

Variable	Description	Default value
<i>SM_TYPE</i>	Values: - SM_Complete : Installs Server and Gateway components - SM_Broker: Installs only Server components - SM_Gateway: Installs only Gateway components.	SM_Complete
<i>EMAIL</i>	Complete this variable with your registration email. Also make sure to include the <i>SERIAL</i> parameter in order for the registration to work.	
<i>SERIAL</i>	Complete this variable with your registration serial. Also make sure to include the <i>EMAIL</i> parameter in order for the registration to work.	

The *SM_TYPE* parameter corresponds to these installation wizard options:



The default installation will install the Gateway + Thinfinity Remote Desktop Services option.

Examples

- Installing Thinfinity Remote Desktop Services only:

```
c:\Thinfinity_Remote_Desktop_Server_Setup_x64.exe /s /v/qn SM_TYPE="SM_Broker"
```

- Installing Thinfinity Gateway Services only:

```
c:\Thinfinity_Remote_Desktop_Server_Setup_x64.exe /s /v/qn SM_TYPE="SM_Gateway"
```

- Installing Thinfinity Gateway + Remote Desktop Services and passing the registration parameters:

```
c:\Thinfinity_Remote_Desktop_Server_Setup_x64.exe /s /v/qn EMAIL=  
"yourmail@domain.com" SERIAL="POIT-NNMG-PATV-54AQ-MBVT-MNAI-EQCI-MCTV"
```

8.11 Credentials Management

With the new 4.0 version , your users can now manage their credentials on a user-by-user basis.

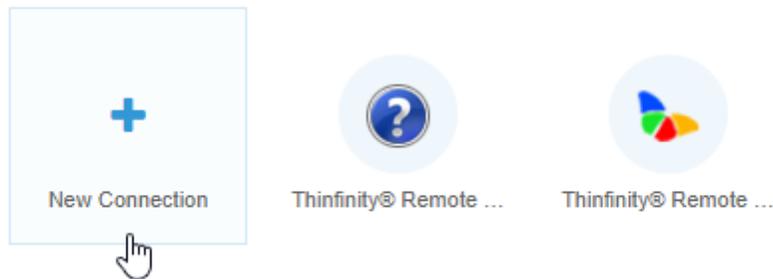
Read More:

- [User-based Access Profiles](#)
- [Credentials Management](#)

8.11.1 User-based Access Profiles

With the new Thinfinity Remote Desktop Server 4.0 version, the "Any computer" functionality (present in previous versions) has been reworked.

Now, instead of separate tabs accessed using the arrow keys on the web interface, the users will find a new button on the index.html screen: The "New Connection" button.



Once it's clicked, you will see the [connecting with open parameters](#) menu :

General Display Resources Program Experience Advanced

Computer: 192.168.0.52

Username: MyAdminUser

Password:

CONNECT BACK

If you are logged in with a user , you will also see the "Saves As" menu, as shown below :

General Display Resources Program Experience Advanced

Computer: 192.168.0.52

Username: MyAdminUser

Password:

Save As

Connection Name: MyAccessProfile

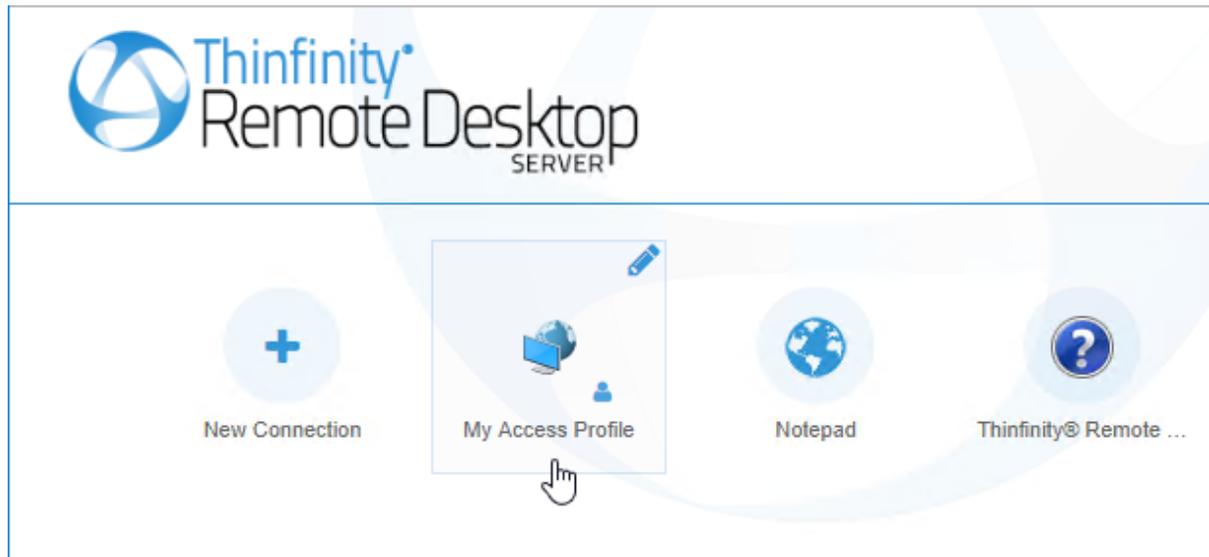
Virtual Path: 192.168.0.52

Connection Icon: 

SAVE

CONNECT BACK

If you press the "Save" button, it will save this Access Profile and bind it to your user . This will store it for you for future use :

**Read More:**

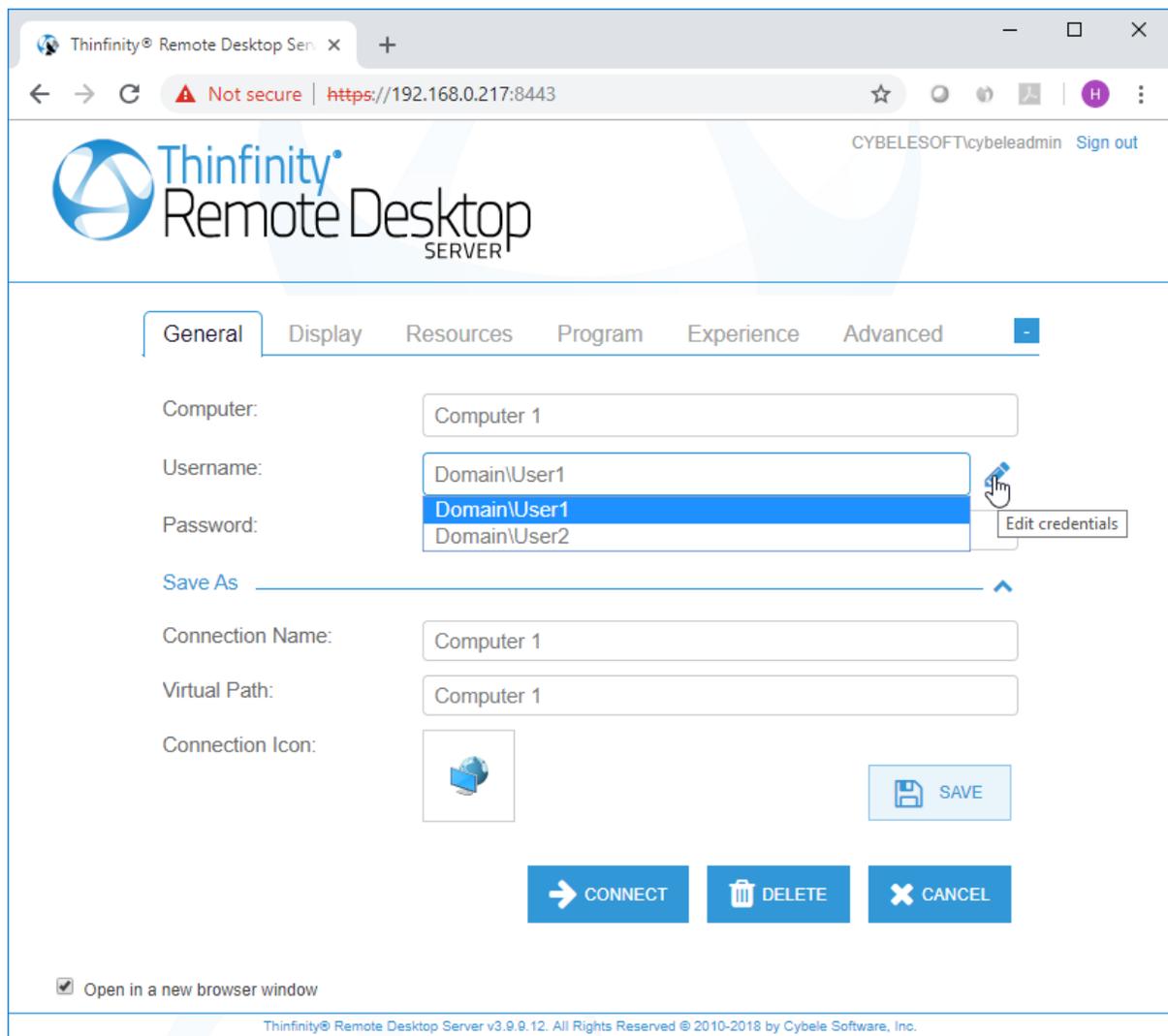
- [Credentials Management](#)

8.11.2 Credentials Management

The functionality of Access Profiles, with "Ask for new credentials" configured on the Credentials level, has been reworked.

It now allows you save your credentials on a profile configured to "Ask for new credentials".

These credentials will be available for other profiles as well. To see stored credentials you have to click on the little edition icon at the right of the users field:



To clear the user from this menu, you must delete the user from all your profiles.

Read More:

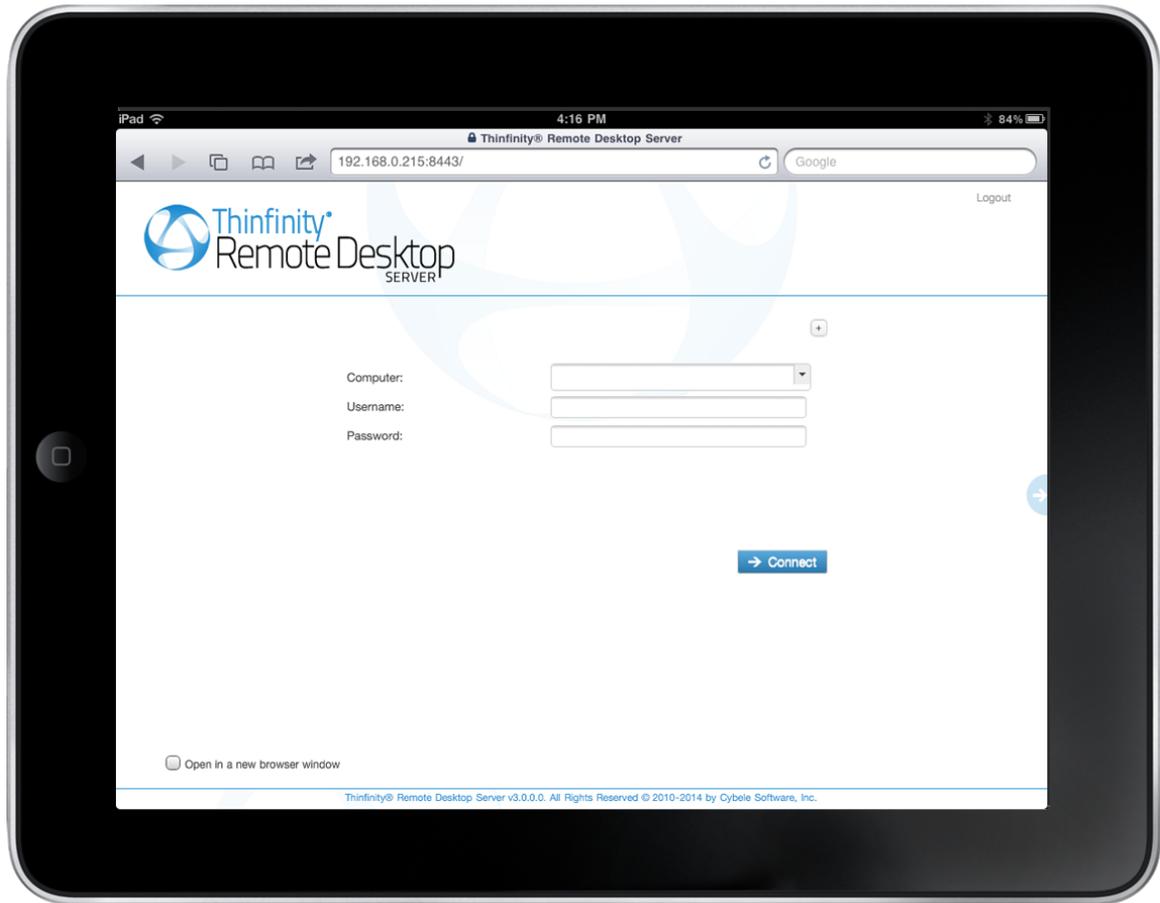
- [User-based Access Profiles](#)

9 Mobile Devices

Using Thinfinity® Remote Desktop Server, you can access remote desktops and applications from many different devices.

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

Access the Thinfinity® Remote Desktop Server 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](#).

Read more:

- [Getting into Thinfinity Remote Desktop Server](#)
- [Mouse Control](#)
- [Keyboards and Toolbars](#)
- [Gestures](#)
- [Disconnecting from Thinfinity Remote Desktop Server](#)
- [Disconnecting](#)

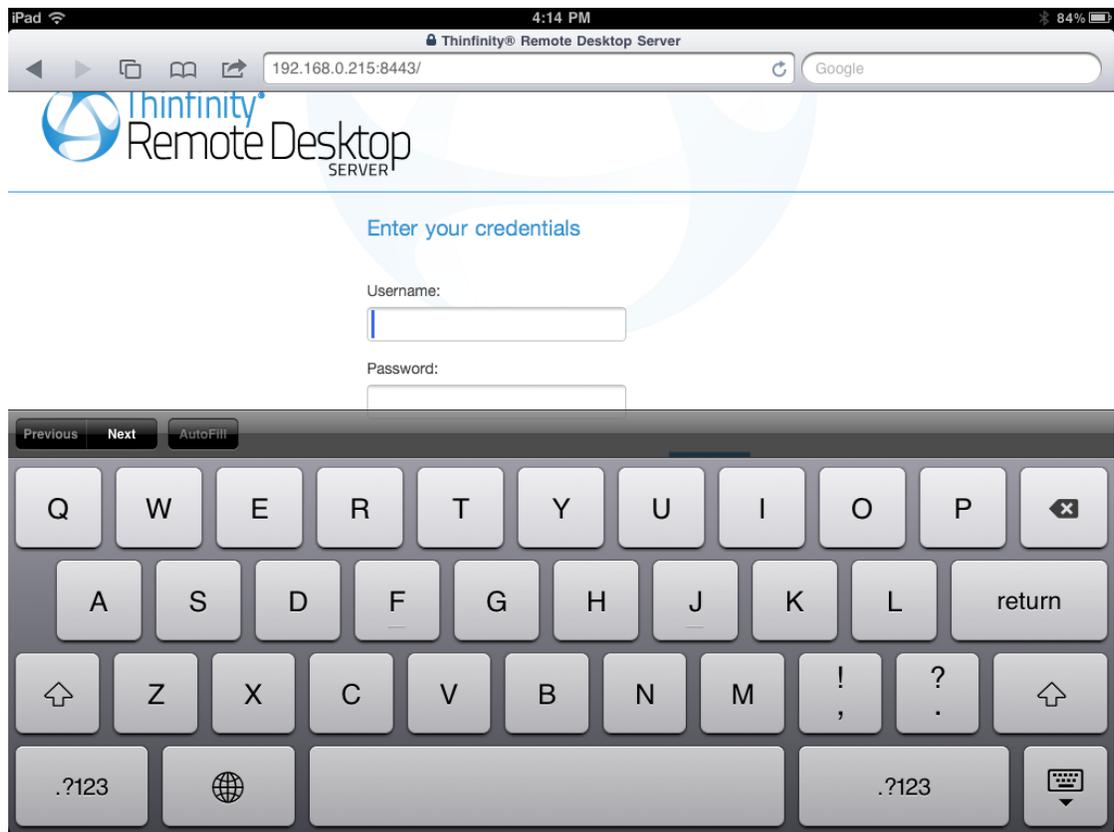
9.1 Getting into Thinfinity® Remote Desktop Server

When you access Thinfinity® Remote Desktop Server 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 more:

- [Mouse Control](#)
- [Keyboards and Toolbars](#)
- [Gestures](#)
- [Disconnecting from Thinfinity Remote Desktop Server](#)

9.2 Mouse Control

Right after you get connected to a remote desktop or application the remote desktop mouse will be available.

Take a look on the table below to see how you can control the remote mouse through the mobile screen. The third column specifies the mobile gesture that corresponds to the described mouse action.

<p>Moving the mouse around</p>	<p>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.</p> <p>Sometimes the mouse is hidden. In that case, keep dragging the finger towards different directions until you can see it on the screen.</p>	<p>-</p>
<p>Regular click</p>	<p>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).</p> <p>Once you have position the mouse draw over the element, give a quick touch on the element.</p>	<p>Tap gesture</p>
<p>Double click</p>	<p>Just like on the regular click you need to first position the mouse draw over this element you want to double click.</p> <p>After that give two quick touches on the element.</p>	<p>Double-tap</p>
<p>Right click</p>	<p>When you open a connection through a mobile, Thinfinity® Remote Desktop Server provides a especial side menu. The second button is used exactly to right click an element of the remote desktop.</p> <p>As for the regular and double click, first of all you need to position the mouse over the element you want to right click.</p> <p>After that touch the second side menu button (the button has a mouse picture with the right button highlighted in red).</p>	<p>-</p>
<p>Drag and drop</p>	<p>To drag and drop elements of the remote desktop to the following:</p> <ol style="list-style-type: none"> Touch the element you want to drag. Do not release your finger. Drag the finger towards the position you want to take the element to. When you get to the position you wanted, release the finger from the screen. 	<p>Press and drag</p>

Read more:

- [Keyboards and Toolbars](#)
- [Gestures](#)
- [Disconnecting from Thinfinity Remote Desktop Server](#)

9.3 Keyboards and Toolbars

1. Right Side Toolbar

The right side toolbar will be visible from the moment you establish your remote desktop connection.



	This button disconnects the remote session. You will be prompted for confirmation.
	This button toggles the remote mouse function to send a right button mouse click or a left button mouse click.
	This button opens the Thinfinity® Remote Desktop Server Extended Keyboard. Read more about it below.
	This button opens the native regular mobile keyboard existing in the device. Read more about it below.
	This button enables the remote desktop full screen, hiding the browser toolbar. Only available for Android devices.

1. Regular Mobile Keyboard

Along with most mobile devices comes a logical keyboard comprised by the keys that are most used by mobile applications.

With Thinfinity® Remote Desktop Server you can use any kind of application located on a remote desktop and that is why Thinfinity® Remote Desktop Server has two additional keyboards with all the keys the device keyboard might not support.

a. Enabling the regular keyboard:

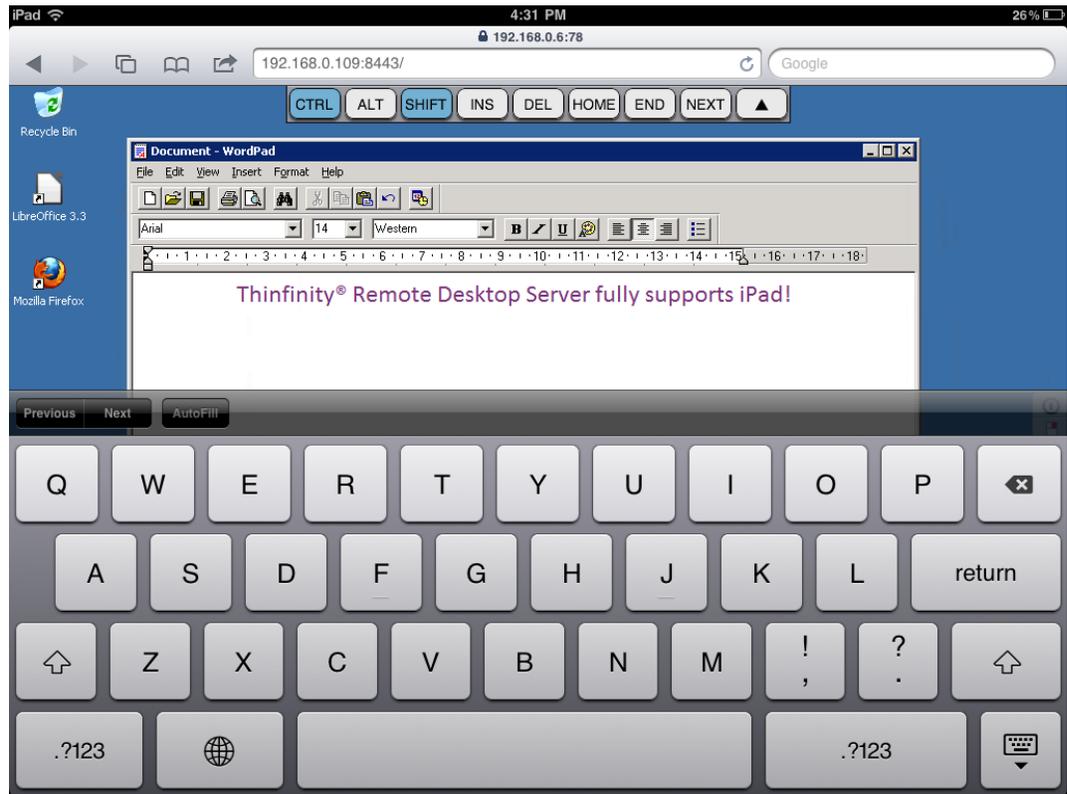
I. If you are on the "Login" or on the "Settings" screen, this keyboard will get automatically enabled every time you enter a text field.

II. Once you get connected to a remote desktop or application, you should touch the last Thinfinity® Remote Desktop Server side menu button, in order to enable the regular keyboard.

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 characters, touch the ".?123" key.



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

2. Thinfinity® Remote Desktop Server Extended Keyboard

Thinfinity® Remote Desktop Server has two additional keyboards.

In order to enable them you should touch the first up-down keyboard button, on the Thinfinity® Remote Desktop Server side menu.

a. Upper keyboard

The upper Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server additional keyboards, press the last bottom keyboard key (the one with a keyboard and a down arrow below draw).

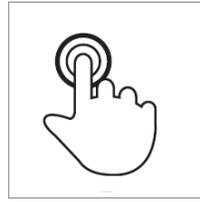
Read more:

- [Gestures](#)
- [Disconnecting from Thinfinity Remote Desktop Server](#)

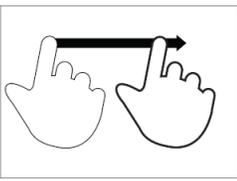
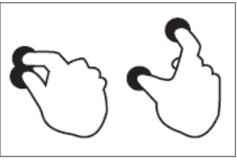
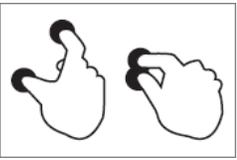
9.4 Gestures

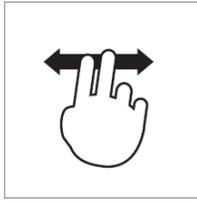
These are the gestures Thinfinity® Remote Desktop Server provides to improve the experience of mobile device users. Learn which they are and what are the circumstances you can use them:

Regular known gestures:

	<p>Tap Briefly touch surface with fingertip</p>	<p>Mouse correspondent Single-click</p>
	<p>Double-tap Rapidly touch surface twice with fingertip</p>	<p>Mouse correspondent Double-click</p>

Special gestures:

	<p>Press and Drag Move one fingerprint over surface without losing contact</p>	<p>Where On the Connection Screen you can drag and drop an object using the Press and Drag gesture.</p>
	<p>Spread (zoom in)</p>	<p>Where On the Connection Screen you can use the Spread gesture to zoom the screen in.</p>
	<p>Pinch (zoom out)</p>	<p>Where On the Connection Screen you can use the Pinch gesture to zoom the screen out.</p>

**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 scroll the screen in different directions.

Read more:

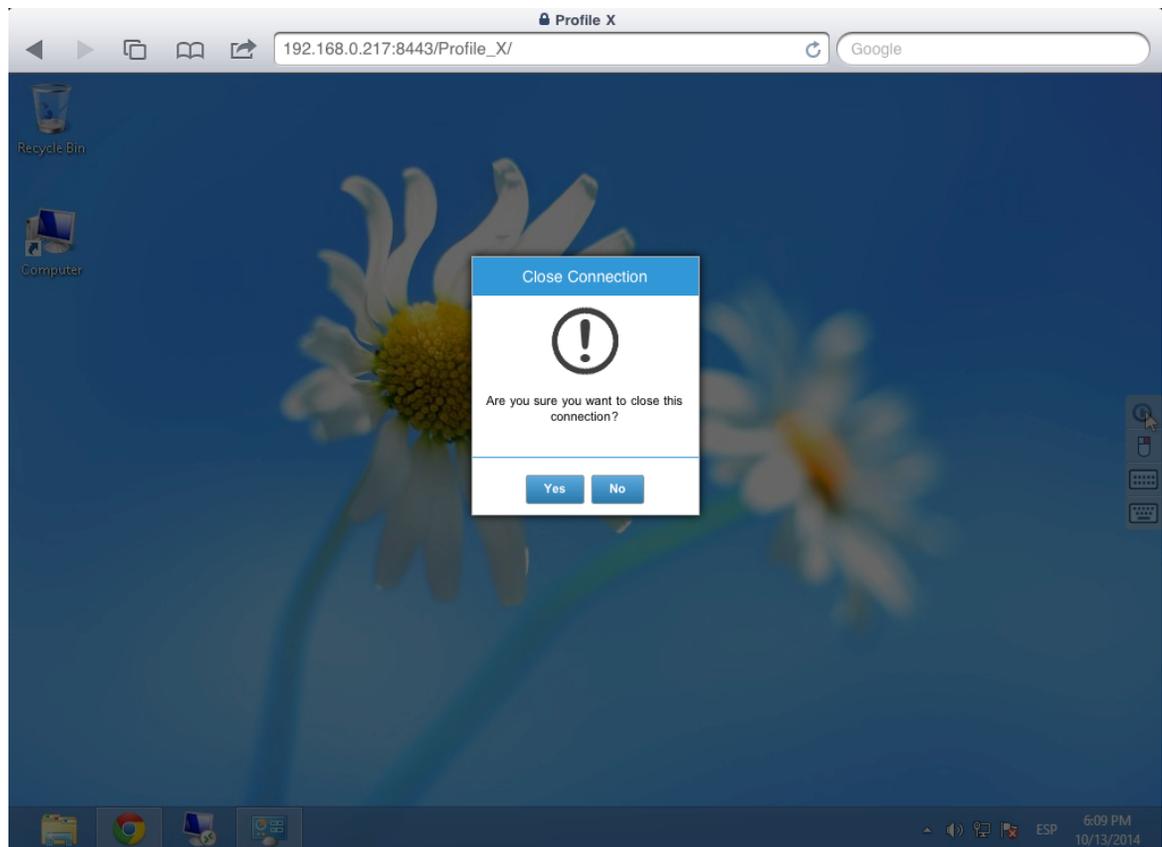
- [Disconnecting from Thinfinity Remote Desktop Server](#)

9.5 Disconnecting from Thinfinity® Remote Desktop Server

1. In order to disconnect from the remote desktop touch the upper button located on the Thinfinity® Remote Desktop Server 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".



Read more:

- [Disconnecting](#)

10 Scaling and Load Balancing

Scaling and load balancing come into play when one machine is not capable of managing all the required resources. Too many concurrent connections or connections to applications that handle a lot of graphics, sound or other elements that require a great availability of resources may cause an overload.

Thinfinity Remote Desktop Server provides components that allow you to distribute the workload across multiple Windows sessions, as well as multiple servers. You can scale the application availability in terms of applications instances —and user accesses— and failover scenarios. In order to achieve optimal resource utilization and avoid overload.

Some of the benefits of load balancing:

- Avoids the overload by distributing the connections among different servers
- Minimizes response time
- More reliability (redundancy)
- Fail over control

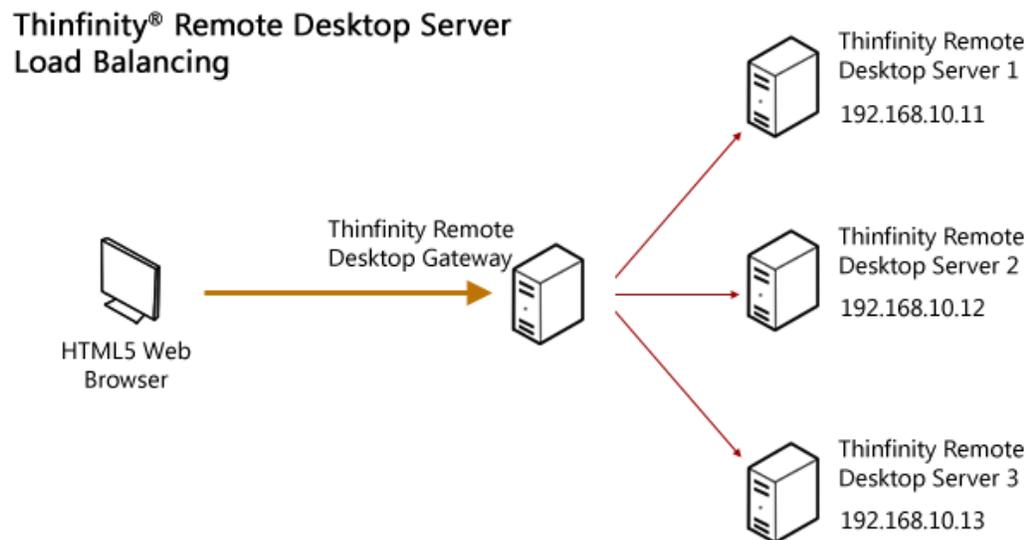
Read More:

- [Scaling and Load Balancing Configurations](#)
- [Installing components](#)
- [Configuring a Load Balancing scenario](#)

10.1 Scaling and Load Balancing Configurations

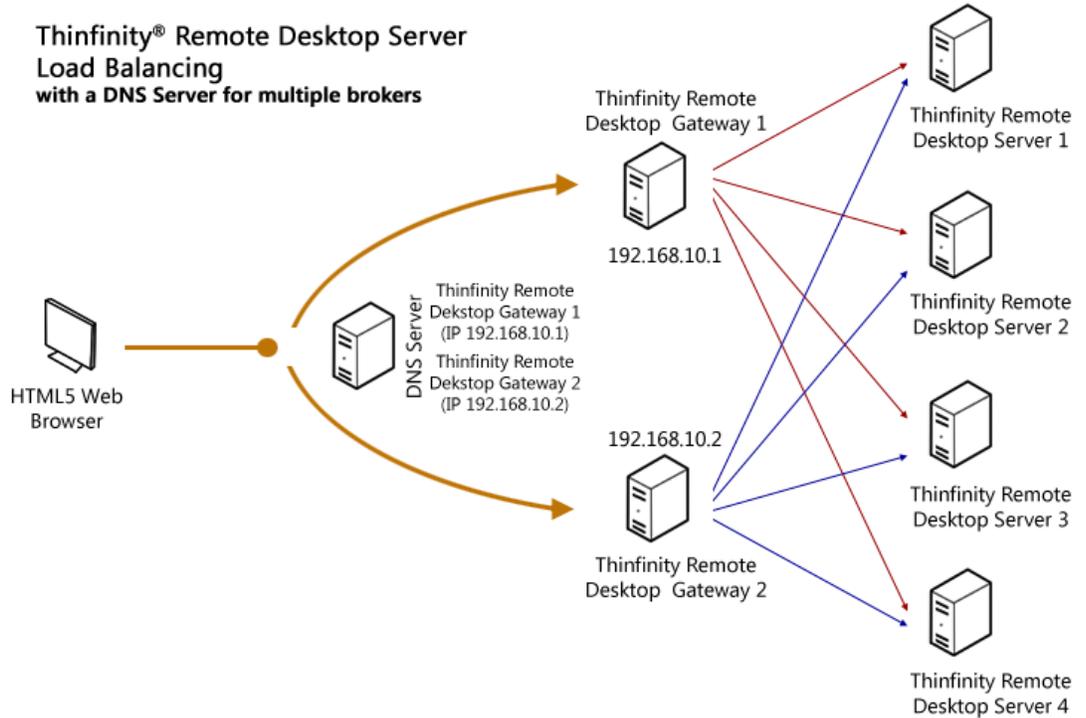
If you arrive to the conclusion that your Thinfinity® Remote Desktop environment would benefit from using load balancing, you can choose between two possible architectures. This decision is an essential step in planning the hardware scheme and configuring the system to work in a distributed way.

Scenario 1: One Gateway and multiple Servers



In this simple scenario, a single Gateway distributes the connection load between a number of Servers.

Scenario 2: Multiple Gateways and multiple Servers



This second scheme is composed by multiple Servers, multiple Gateways and the DNS Server, its domain name associated to all the available Gateways' IPs.

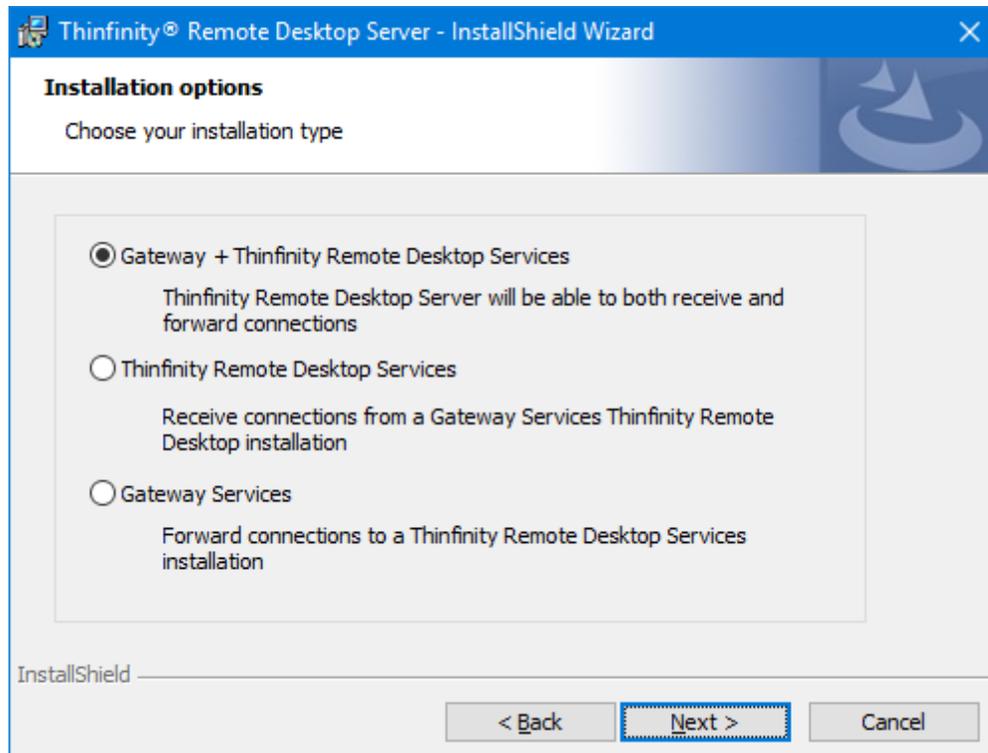
Read More:

- [Installing Components](#)
- [Configuring a Load Balancing scenario](#)

10.2 Installing Components

In this section you will learn how to set up Thinfinity Remote Desktop Server's components in a load-balancing network configuration.

Thinfinity Remote Desktop Server has two basic services: Gateway Services and Thinfinity Remote Desktop Services.



Gateway Services: Under this role, Thinfinity Gateway services respond to all web-page requests and, when a connection is solicited, it selects the appropriate Server to forward that request to. In case any established connection fails, or a Server falls down, the Gateway will be able to reconnect to the Server that has the highest availability at the moment. All the system settings and profiles are centralized and shared between the Servers.

Thinfinity Remote Desktop Services: Under this role, Thinfinity Remote Desktop Server only processes forwarded connections. The Server is responsible for establishing and processing the connections assigned by the Gateway.

Before configuring a distributed environment, you should go over some steps:

1. Choose out of the possible [Scaling and Load Balancing Configurations](#) the one that best fits your needs.
2. Plan which machines will run Thinfinity Remote Desktop Services, and which will run Gateway Services and DNS Servers.
3. Make sure all the IP addresses are public to the web browsers that will access Thinfinity® Remote Desktop Server.

Read More:

- [Configuring a Load Balancing Scenario](#)

10.3 Configuring a Load Balancing Scenario

In order to configure a load balancing scenario, you need at least one Gateway installation and two Server installations.

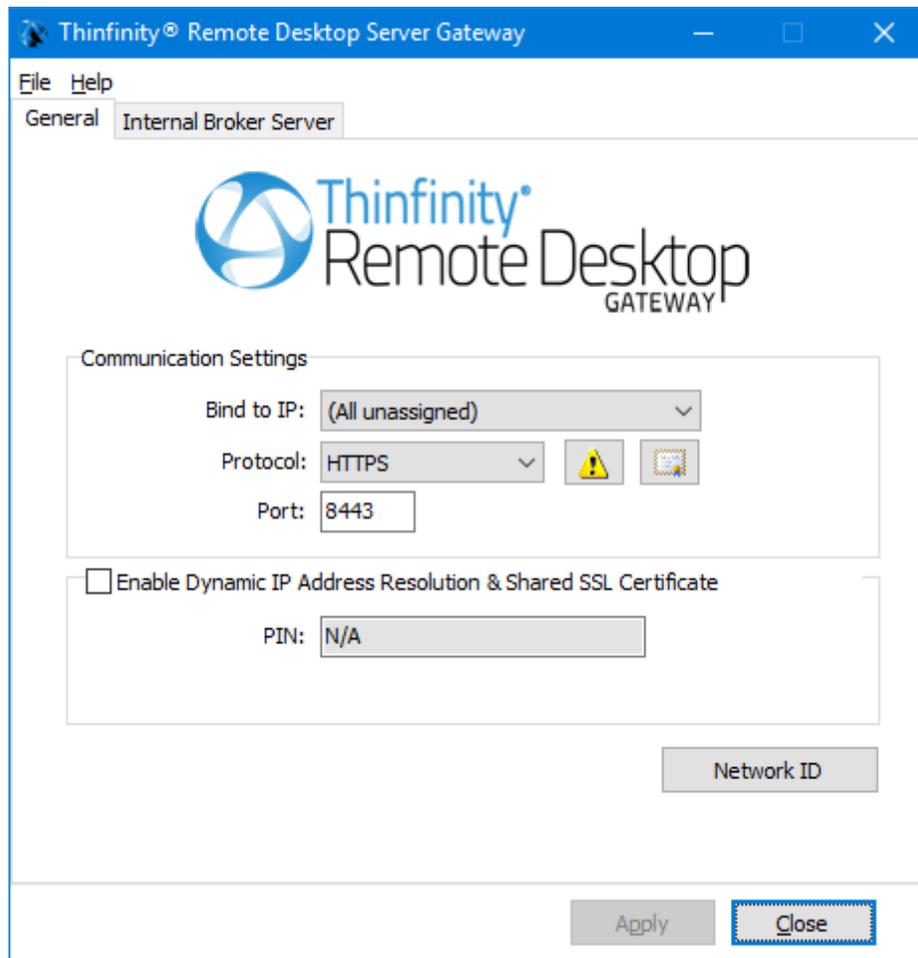
Configuring the Gateway

Under this role, Thinfinity Remote Desktop Gateway responds to all web-page requests and, when a connection is solicited, it selects the appropriate Server to forward that request to.

To configure the Gateway, open the Gateway Manager. Set the IP and port where the Gateway will run. If you only have one gateway, this is where the users will connect to. If you use more than one Gateway in your architecture, you will use this IP in the DNS server you set up to distribute the connection between the Gateways.

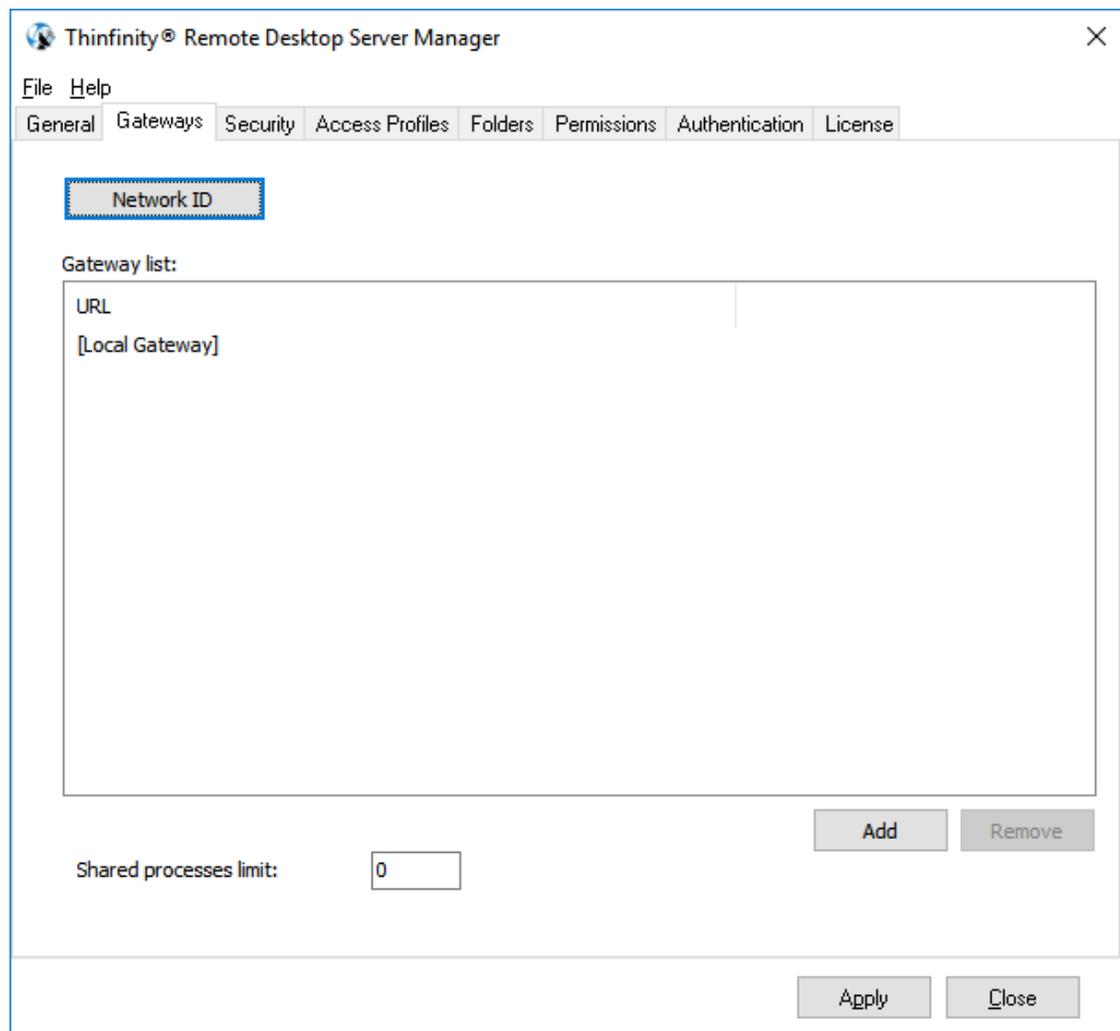
Also, set the Network ID. All the Gateway and Server installations involved in a Load Balancing architecture share the same network ID.

Also, make sure all the Gateways' IPs are public to the locations that will access Thinfinity Remote Desktop Server through a web browser.



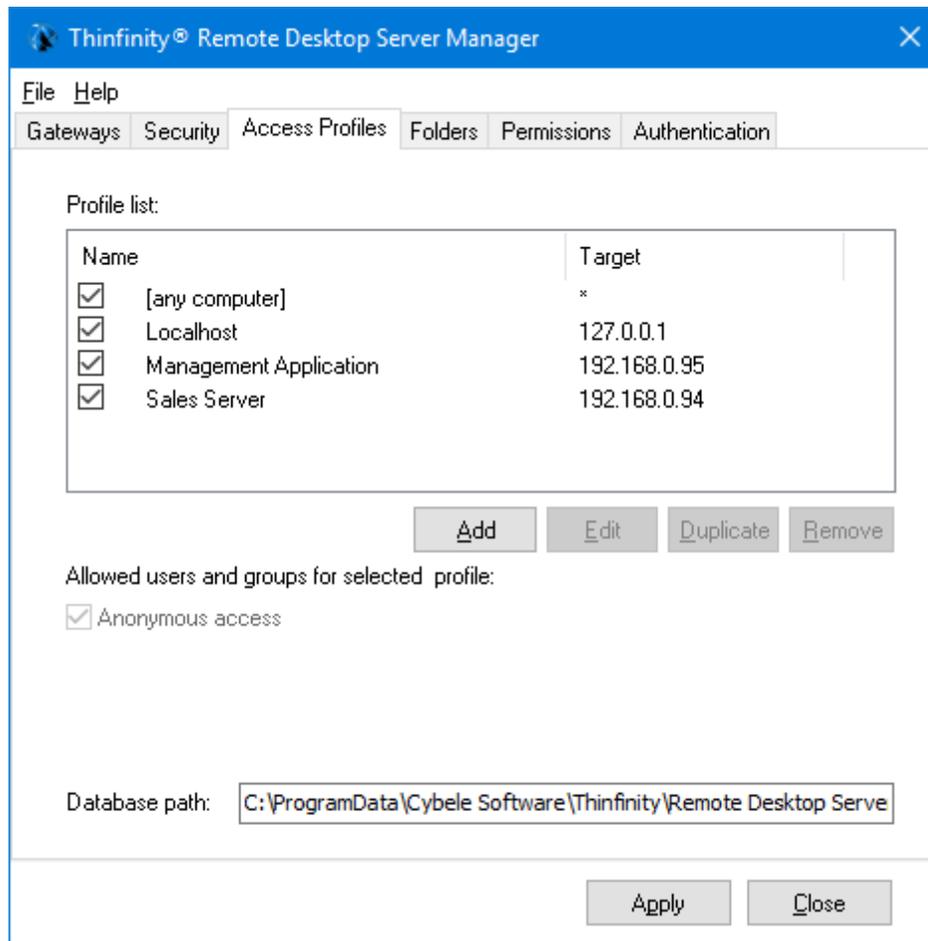
Configuring the Server

Under this role, Thinfinity Remote Desktop Server only processes forwarded connections. The Server is responsible for establishing and processing the connections assigned by the Gateway. To configure the Server, open the Server Manager and go the 'Gateways' tab.



Press the 'Add' button to add a gateway to the Gateway List. This means that now this server's resources can be accessed through the listed gateways. Make sure that the Network ID is the same for all the gateways and servers involved in this load balancing architecture.

Then, go to the 'Access Profiles' tab:



Share the configuration

Set the 'Database Path' field in a network location that you can access from the other Server installations.

Once you share the database path, all the information in the 'Applications' tab will be shared with other Thinfinity Remote Desktop Server installations. Make sure you modify the applications' information from one location at a time, as all changes will be reflected in the other installations.

Share the license

In order to share your license over multiple servers, you'll need to install the License Server Manager. Please contact support@cybelesoft.com for more information.

Read More:

- [The Gateway Manager](#)
- [Scaling and Load Balancing Configurations](#)
- [Configuring the General Tab](#)
- [Configuring the Access Profiles Tab](#)
- [Configuring the Licenses](#)

11 Integrating Thinfinity® Remote Desktop Server

Thinfinity® Remote Desktop Server was designed to interoperate with many different applications. Find below the ways you can integrate Thinfinity® Remote Desktop Server with other applications:

[Integration through the SDK library](#)

[Performing an External Authentication to Thinfinity® Remote Desktop Server](#)

[Integrating Thinfinity® Remote Desktop Server in a Single-Sign-On schema](#)

[Customizing the Web Interface](#)

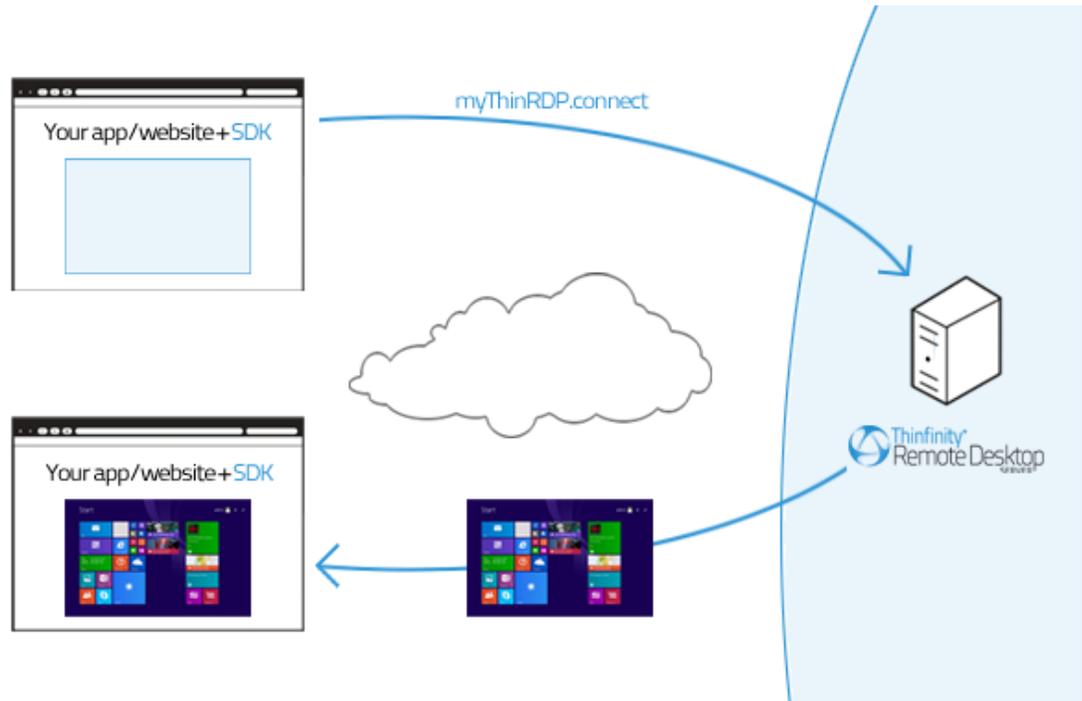
[Integration through the Web Service API](#)

[Allowing access through the One-Time-URL](#)

If you need to integrate Thinfinity® Remote Desktop Server 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.

11.1 SDK

The SDK library allows you to integrate your own website or web application with *Thinfinity® Remote Desktop 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 Thinfinity® Remote Desktop Server authentication mode: [None](#), [Username/password](#) or [Access Profiles](#).

The integration of Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server installed and configured. Otherwise, please go back to the [Getting Started](#) topic.

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

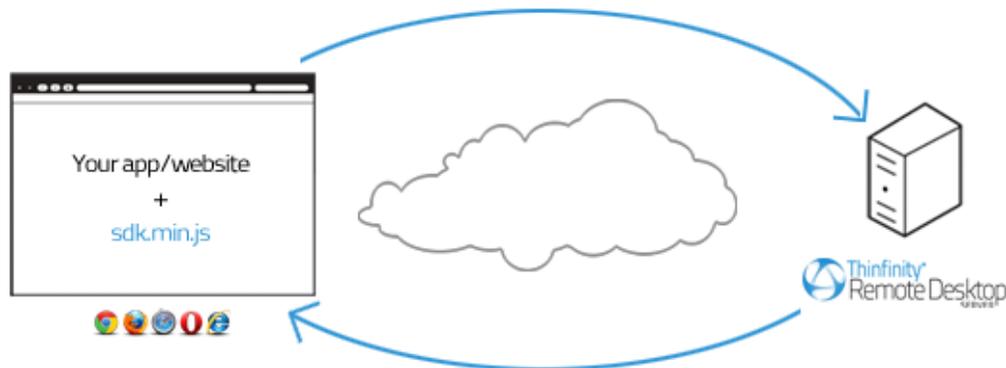
- [Deploying](#)
- [Using the SDK](#)
- [The Connect Method](#)
- [Events](#)
- [Keystrokes methods](#)

[SSL Certificate
Demo](#)

Tip: You can also take a look at the sdk.html file available in the Thinfinity® Remote Desktop 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 https://server_IP:port/sdk.html url.

11.1.1 Deploying

In order for Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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 using local connection mode:

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 Thinfinity® Remote Desktop 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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server in.

Read more:

- [Using the SDK](#)
- [SDK Login](#)
- [Connect Method](#)
- [Browser Resizing](#)
- [Keystroke Methods](#)
- [SSL Certificate](#)
- [Demo](#)

11.1.2 Using the SDK

Before you actually begin to code:

1) Verify in the Thinfinity® Remote Desktop 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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server SDK functionality. It has two arguments: the Thinfinity® Remote Desktop Server URL and the connection mode in which Thinfinity® Remote Desktop Server 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("Thinfinity® Remote Desktop Server URL", connection
mode);
  mythinrdp.connect({
    //Read the "The connect method" to complete all the
    expected parameters
  });
});
</script>
```

- a. Substitute the "Thinfinity® Remote Desktop Server URL" argument for the getThinRDP method with the [Thinfinity® Remote Desktop Server protocol + Computer's IP + Port](#), following this format: <https://127.0.0.1:8443>.

- b. Substitute the second GetThinRDP 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)	sdk.min.js posts into Thinfinity® Remote Desktop Server and all the remote desktop data is exchanged through the Thinfinity® Remote Desktop 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 Thinfinity® Remote Desktop Server SDK [events](#) and [keystrokes](#).

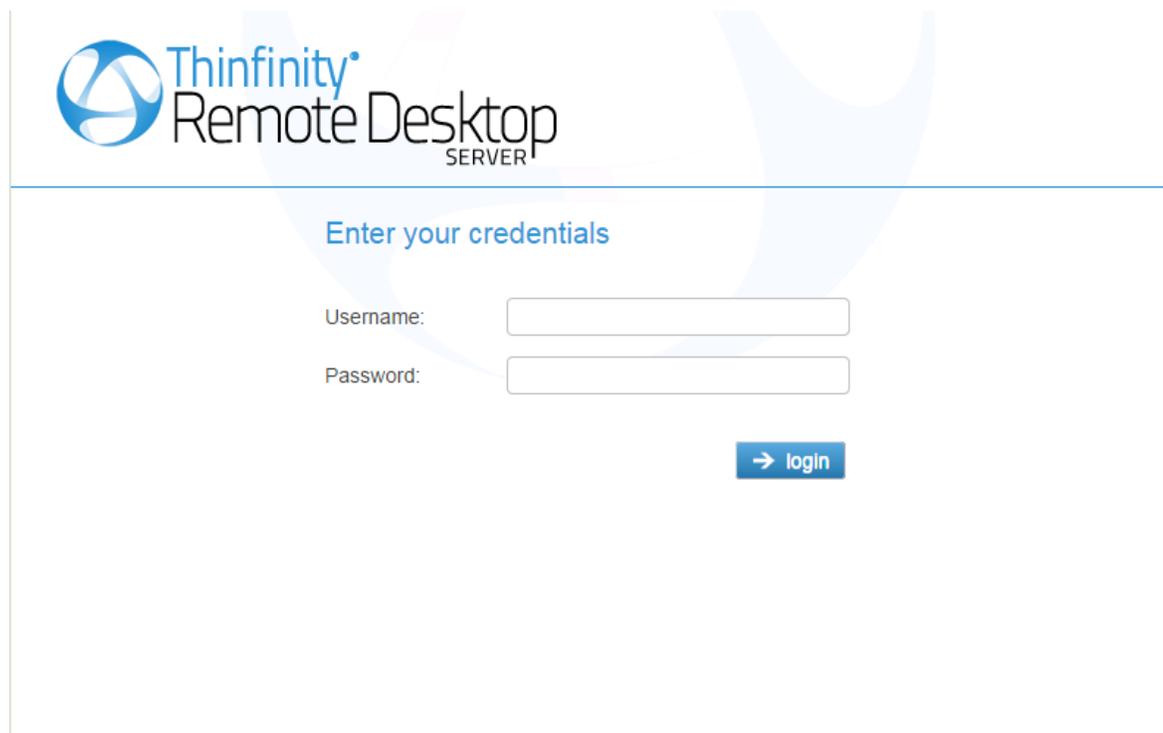
Read more:

- [SDK Login](#)
- [Connect Method](#)
- [Browser Resizing](#)
- [Keystroke Methods](#)
- [SSL Certificate](#)
- [Demo](#)

11.1.3 SDK Login

If you access the SDK.html file without establishing a previous authentication method that sends the proper credentials, the browser will show the browser's anonymous authentication popup. This popup is not created by Thinfinity® Remote Desktop Server so it doesn't show specific information like where the user is connecting to, or the company name.

Thinfinity® Remote Desktop Server now distributes SDKLogin.html. This page is a ready to use example of a login form:



The screenshot shows a login form for Thinfinity Remote Desktop Server. At the top left is the logo, which consists of a blue circular icon with a white geometric shape inside, followed by the text "Thinfinity" in blue and "Remote Desktop SERVER" in black. Below the logo is a horizontal blue line. Underneath the line, the text "Enter your credentials" is displayed in blue. There are two input fields: "Username:" followed by a white text box, and "Password:" followed by a white text box. Below the password field is a blue button with a white right-pointing arrow and the text "login".

You can find SDKLogin.html in the 'webrdp' folder in the Thinfinity® Remote Desktop Server installation directory. You can open it and customize it to have your company logo, or use the form as an example to include in your pre existing webpage.

Read more:

- [Connect Method](#)
- [Browser Resizing](#)
- [Keystroke Methods](#)
- [SSL Certificate](#)
- [Demo](#)

11.1.4 Connect method

The 'connect' method creates a remote desktop connection to the remote machine and positions it 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](#)

[Toolbar customization parameters](#)

Right below you will find a code excerpt showing the connect method and all its possible parameters set. Note: they should not be used all at the same time, because each environment will require different parameters:

- The [Placement parameters](#) may be required or not, depending on the connection mode (remote or local).
- The [Destination and Authentication parameters](#) will be required depending on the authentication mode set on Thinfinity® Remote Desktop Server manager.
- The rest of the parameters ([Settings](#), [Features](#), [Events](#) and [Toolbar Customization](#)) are optional and should be sent whenever you need to change a determined Thinfinity® Remote Desktop Server 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,  
    touchControl: true,  
    tcpReadCount: true,  
    tcpReadWait:  true,  
    checkBeforeWindowC true,  
    lose:  
  
    // 'General' tab  
    profileKey:   "substitute with the profileKey when 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)",

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

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

    // 'Experience' tab
experience: {
  enableRemoteFx: true,
  desktopbackground false,
  :
  visualstyles: false,
  menuwindowanimati false,
  on:
  fontsmoothing: false,
  showwindowcontent false,
  :
  desktopcompositio false
  n:
},

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

    // 'Resources' tab
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: {
    onServerConnect: function (reconnecting) { },
    onServerConnect: function () { },
    onQueryDisconn: function () { },
    onServerConnect: function (errMessage) { },
    onServerError: function () { },
    onServerDisconn: function () { },
    onExecResult : function (cmd) { },
    onExecRemoteApp: function (cmd) { },
    onInteractionRequired: function () { },
    onSessionStart : function () { },
    onSessionEnd : function (message) { }
  },

  // Toolbar customization
  createToolbar: true,
  toolbarVisible: true,
  toolbarRestrictions: [
    "actionsMenuBtn", // "Actions"
    "actionsMenuBtn.refresh", // "Refresh"
    "actionsMenuBtn.ssnShareBtn", // "Share session"
    "actionsMenuBtn.sendKeysBtn", // "Send Keys..."
    "actionsMenuBtn.sendKeysBtn.ctrlAltDelBtn", // "Ctrl + Alt + Del"
    "actionsMenuBtn.sendKeysBtn.ctrlEscBtn", // "Ctrl + Esc"
    "actionsMenuBtn.sendKeysBtn.shiftCtrlEscBtn", // "Shift + Ctrl + Esc"
    "actionsMenuBtn.sendKeysBtn.windowsExplorerBtn", // "Shell Explorer"
    "actionsMenuBtn.sendKeysBtn.runBtn", // "Run"
    "actionsMenuBtn.sendKeysBtn.altTabBtn", // "Alt + Tab"
    "actionsMenuBtn.sendKeysBtn.altShiftTabBtn", // "Alt + Shift + Tab"
    "actionsMenuBtn.sendKeysBtn.altEscBtn", // "Alt + Esc"
    "actionsMenuBtn.sendKeysBtn.leftWinBtn", // "Left Win Key"
    "actionsMenuBtn.sendKeysBtn.rightWinBtn", // "Right Win Key"
    "actionsMenuBtn.viewOptionsBtn", // "View params & layout"
    "fileMenuBtn", // "File transfer"
    "fileMenuBtn.fileManBtn", // "File Manager"
    "fileMenuBtn.uploadBtn", // "Upload"
    "fileMenuBtn.downloadBtn", // "Download"
    "optionsMenuBtn", // "Options"
    "optionsMenuBtn.scaleBtn", // "Scale"
    "optionsMenuBtn.imgQualityBtn", // "Image Quality"
    "optionsMenuBtn.imgQualityBtn.imgQHighestBtn", // "Highest"
    "optionsMenuBtn.imgQualityBtn.imgQOptimalBtn", // "Optimal"
    "optionsMenuBtn.imgQualityBtn.imgQGoodBtn", // "Good"
    "optionsMenuBtn.imgQualityBtn.imgQPoorBtn", // "Poor"
    "optionsMenuBtn.keyboardMode", // "Disable Shortcuts"
    "disconnectBtn", // "Disconnect"
  ]
});

```

Note: If you are using the connect method and the customsettings.js file, remember that the latter overrides the connect method's settings.

Read more:

- [Placement](#)
- [Destination and Authentication](#)
- [Settings](#)
- [Features](#)
- [Events](#)
- [Toolbar Customization](#)
- [Browser Resizing](#)
- [Keystroke Methods](#)
- [SSL Certificate](#)
- [Demo](#)

11.1.4.1 Placement

These are all the parameters related to the Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server. If you inform an existing window name or iframe id, Thinfinity® Remote Desktop Server 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

Read more:

- [Destination and Authentication](#)
- [Settings](#)
- [Features](#)
- [Events](#)

11.1.4.2 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		could	could	could

		username				
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, Thinfinity® Remote Desktop Server 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 authenticate, the user will not be able to log in.	boolean true,false	false	could	could	could
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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server if you are not using profiles as authentication mode, or if you are connecting through the any computer profile.

Read more:

- [Settings](#)
- [Features](#)
- [Events](#)
- [Toolbar Customization](#)

11.1.4.3 Settings

These are all the settings that can be configured through Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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	"fitbrowser", "fittoScreen", "fixed". When fixed, the width and height parameters will be considered.	string toolbar size	"fitbrowser"
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 Thinfinity® Remote Desktop Server 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

touchControl	Enables or disable touch capabilities.	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 milliseconds	20
saveSession	Enable this setting to record the remote desktop session.	boolean true,false	false
checkBeforeWindowClose	Set to false to skip the user confirmation popup of the onBeforeUnload event	boolean true,false	true

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 redirect the desktop drawing to off-screen surfaces in video memory. The desktop will also present many visual effects.	boolean true,false	false
experience.enableRemoteFx	Set to false to disable Remote FX. Remote FX is the most efficient data transmission mode, but it might interact badly with other configurations. Warning: this setting affects other experience settings. Learn more about Remote FX .	boolean true,false	true

Read more:

- [kbdLayout Values](#)
- [Features](#)
- [Events](#)
- [Toolbar Customization](#)

11.1.4.3.1 kbdLayout Values

This option ultimately depends 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

Read more:

- [Features](#)

11.1.4.4 Features

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

Clipboard:

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

Printer:

Parameter	What it means	Type/format	Default
printer.enabled	Set to true in order to enable Thinfinity® Remote Desktop Server PDF printer.	boolean true,false	false
printer.setasdefault	Thinfinity® Remote Desktop Server printer as the remote default printer.	boolean true,false	true
printer.name	Specify the printer name that you want to be shown on the remote machine's printer list.	string name	
printer.driver	Mark this option to set Thinfinity® Remote Desktop Server 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 want to be shown 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

Read more:

- [Events](#)

- [Toolbar Customization](#)

11.1.4.5 Events

The events parameter allows you to handle each one of the available Thinfinity® Remote Desktop Server events from the SDK.

```

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

```

Observe in the code above that all the event functions are empty. In 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
events.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.	<pre> onServerConnecting : function (reconnecting) { \$.blockUI("Establishing connection"); } </pre>
events.onServerConnect	obj	The "onServerConnect" event is fired every time a "connect" command is exchanged between the browser and Thinfinity® Remote Desktop 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	<pre> onServerConnect : function (obj) { \$.unblockUI(); } </pre>

		<pre>(\$.unlockUI());</pre> <p>The 'obj' parameter ships the generated connection object.</p>	
events.onQueryDisconnect	-	<p>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.</p>	<pre>onQueryDisconnect: function () { if (confirm("A remote session is active. Are you sure you want to disconnect?")) { mythinrdp.disconnect(); } }</pre>
events.onServerConnectionError	errMessage	<p>If an error prevents the client connection to be established, this event will be fired. The errMessage argument brings the error message.</p>	<pre>onServerConnectionError: function (errMessage){ alert("connect error: " + errMessage); }</pre>
events.onServerDisconnect	-	<p>Anytime the Web client gets disconnected from Thinfinity® Remote Desktop 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.</p>	<pre>onServerDisconnect: function () { alert("disconnect"); \$.unlockUI(); mythinrdp.updateTools(); \$("#" + mythinrdp.rcParams.divId).hide(); }</pre>

events.onExecResult	cmd	<p>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.</p>	<pre>onExecResult: function (cmd) { alert("exename: " + cmd.exename + " rc: " + cmd.rc); }</pre>
event.onExecRemoteApp		<p>This event is fired when the remote server starts the execution of a RemoteApp.</p>	<pre>onExecRemoteApp: function (cmd) { alert("The application is starting"); }</pre>
event.onInteractionRequired		<p>This event is fired during the connection process to a RemoteApp either when the systems requires a user interaction to proceed before being able to open the application – such as a UAC prompt–; or when the application is ready. In some cases, the application might be starting and the user might not have access to the blocked screen, so it might need to be</p>	<pre>onInteractionRequired: function () { \$.UnBlockUI(); }</pre>

		unlocked programatically.	
events.onSessionStart	-	This event will be fired when the client session has been started in Thinfinity® Remote Desktop Server.	<pre>onSessionStart: function () { \$("#" + mythinrdp.rcParams.divId).show(); mythinrdp.updateTools(); }</pre>
events.onSessionEnd	message	As soon as the client Session is closed, the "onSessionEnd" event will be fired.	<pre>onSessionEnd: function (message) { alert(message); },</pre>

 This 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 syntax 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	events.onServerConnecting
serverConnect	events.onServerConnect
execResult	events.onServerConnect
sessionStart	events.onSessionStart
serverConnectionError	events.onServerConnectionError
disconnectConfirmRequest	events.onQueryDisconnect
serverDisconnect	events.onServerDisconnect
sessionEnd	events.onSessionEnd

Read more:

- [Toolbar Customization](#)

11.1.4.6 Toolbar Customization

The toolbar customization parameters allow you to restrict partially or totally the user's options by eliminating buttons from the Thinfinity® Remote Desktop Server toolbar's defaults.

```
// Toolbar customization
createToolbar: true,
toolbarVisible: true,
toolbarRestrictions: [
    "actionsMenuBtn", // "Actions"
    "actionsMenuBtn.refresh", // "Refresh"
    "actionsMenuBtn.ssnShareBtn", // "Share session"
    "actionsMenuBtn.sendKeysBtn", // "Send Keys..."
    "actionsMenuBtn.sendKeysBtn.ctrlAltDelBtn", // "Ctrl + Alt + Del"
    "actionsMenuBtn.sendKeysBtn.ctrlEscBtn", // "Ctrl + Esc"
    "actionsMenuBtn.sendKeysBtn.shiftCtrlEscBtn", // "Shift + Ctrl + Esc"
    "actionsMenuBtn.sendKeysBtn.windowsExplorerBtn", // "Shell Explorer"
    "actionsMenuBtn.sendKeysBtn.runBtn", // "Run"
    "actionsMenuBtn.sendKeysBtn.altTabBtn", // "Alt + Tab"
    "actionsMenuBtn.sendKeysBtn.altShiftTabBtn", // "Alt + Shift + Tab"
    "actionsMenuBtn.sendKeysBtn.altEscBtn", // "Alt + Esc"
    "actionsMenuBtn.sendKeysBtn.leftWinBtn", // "Left Win Key"
    "actionsMenuBtn.sendKeysBtn.rightWinBtn", // "Right Win Key"
    "actionsMenuBtn.viewOptionsBtn", // "View params & layout"
    "fileMenuBtn", // "File transfer"
    "fileMenuBtn.fileManBtn", // "File Manager"
    "fileMenuBtn.uploadBtn", // "Upload"
    "fileMenuBtn.downloadBtn", // "Download"
    "optionsMenuBtn", // "Options"
    "optionsMenuBtn.scaleBtn", // "Scale"
    "optionsMenuBtn.imgQualityBtn", // "Image Quality"
    "optionsMenuBtn.imgQualityBtn.imgQHighestBtn", // "Highest"
    "optionsMenuBtn.imgQualityBtn.imgQOptimalBtn", // "Optimal"
    "optionsMenuBtn.imgQualityBtn.imgQGoodBtn", // "Good"
    "optionsMenuBtn.imgQualityBtn.imgQPoorBtn", // "Poor"
    "optionsMenuBtn.keyboardMode", // "Disable Shortcuts"
    "disconnectBtn", // "Disconnect"
]
```

Observe on the code above that for the toolbarRestrictions parameter all the options are included for

visibility purposes. 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 Thinfinity® Remote Desktop Server connections not have the Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server toolbar start expanded. Without modifying this value, the toolbar will start collapsed and the user needs to click on a button to expand it. This is useful if you think the Thinfinity® Remote Desktop Server toolbar settings should be displayed so it's more evident to users.	boolean true,false	true
toolbarRestrictions	Use this parameter to eliminate specific buttons from the Thinfinity® Remote Desktop Server toolbar. Each button is explained in detail in the table below	array true,false	[]

In the following table you can find a description of each of the toolbarRestrictions values you can use to restrict certain buttons or menus of the Thinfinity® Remote Desktop Server toolbar. Notice that sub menus and options within menus have the parent menu name as part of their name. This will help you read the value list.

Value	What it means
"actionsMenuBtn"	Eliminates the 'Actions' menu and all its options from the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.refresh"	Eliminates the 'Refresh' option from the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.ssnShareBtn"	Eliminates the 'Share Session' option from the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.sendKeysBtn"	Eliminates the 'Send Keys...' sub menu and all its options from the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.sendKeysBtn.ctrlAltDelBtn"	Eliminates the 'Ctrl + Alt + Del' option from the 'Send Keys...' sub menu in the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.sendKeysBtn.ctrlEscBtn"	Eliminates the 'Ctrl + Esc' option from the 'Send Keys...' sub menu in the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.sendKeysBtn.shiftCtrlEscBtn"	Eliminates the 'Shift + Ctrl + Esc' option from the 'Send Keys...' sub menu in the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.sendKeysBtn.windowsExplorerBtn"	Eliminates the 'Shell Explorer' option from the 'Send Keys...' sub menu in the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.sendKeysBtn.runBtn"	Eliminates the 'Shell Explorer' option from the 'Send Keys...' sub menu in the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.

"actionsMenuBtn.sendKeysBtn.altTabBtn"	Eliminates the 'Alt + Tab' option from the 'Send Keys...' sub menu in the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.sendKeysBtn.altShiftTabBtn"	Eliminates the 'Alt + Shift + Tab' option from the 'Send Keys...' sub menu in the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.sendKeysBtn.altEscBtn"	Eliminates the 'Alt + Esc' option from the 'Send Keys...' sub menu in the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.sendKeysBtn.leftWinBtn"	Eliminates the 'Left Win Key' option from the 'Send Keys...' sub menu in the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.sendKeysBtn.rightWinBtn"	Eliminates the 'Right Win Key' option from the 'Send Keys...' sub menu in the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"actionsMenuBtn.viewOptionsBtn"	Eliminates the 'View params & layout' option from the 'Actions' menu in the Thinfinity® Remote Desktop Server toolbar.
"fileMenuBtn"	Eliminates the 'File Transfer' menu and all its options from the Thinfinity® Remote Desktop Server toolbar.
"fileMenuBtn.fileManBtn"	Eliminates the 'File Manager' option from the 'File Transfer' menu in the Thinfinity® Remote Desktop Server toolbar.
"fileMenuBtn.uploadBtn"	Eliminates the 'Upload' option from the 'File Transfer' menu in the Thinfinity® Remote Desktop Server toolbar.
"fileMenuBtn.downloadBtn"	Eliminates the 'Download' option from the 'File Transfer' menu in the Thinfinity® Remote Desktop Server toolbar.
"optionsMenuBtn"	Eliminates the 'Options' menu and all its options from the Thinfinity® Remote Desktop Server toolbar.
"optionsMenuBtn.scaleBtn"	Eliminates the 'Scale' option from the 'Options' menu in the Thinfinity® Remote Desktop Server toolbar.
"optionsMenuBtn.imgQualityBtn"	Eliminates the 'Image Quality' sub menu and all its options from the 'Options' menu in the Thinfinity® Remote Desktop Server toolbar.
"optionsMenuBtn.imgQualityBtn.imgQHighestBtn"	Eliminates the 'Highest' option from the 'Image Quality' sub menu in the 'Options' menu in the Thinfinity® Remote Desktop Server toolbar.
"optionsMenuBtn.imgQualityBtn.imgQOptimalBtn"	Eliminates the 'Optimal' option from the 'Image Quality' sub menu in the 'Options' menu in the Thinfinity® Remote Desktop Server toolbar.
"optionsMenuBtn.imgQualityBtn.imgQGoodBtn"	Eliminates the 'Good' option from the 'Image Quality' sub menu in the 'Options' menu in the Thinfinity® Remote Desktop Server toolbar.
"optionsMenuBtn.imgQualityBtn.imgQPoorBtn"	Eliminates the 'Poor' option from the 'Image Quality' sub menu in the 'Options' menu in the Thinfinity® Remote Desktop Server toolbar.
"optionsMenuBtn.keyboardMode"	Eliminates the 'Disable Shortcuts' option from the 'Options' menu in the Thinfinity® Remote Desktop Server toolbar.
"disconnectBtn"	Eliminates the 'Disconnect' menu from the Thinfinity® Remote Desktop Server toolbar.

[Read more about the Thinfinity® Remote Desktop Server toolbar and how to customize it.](#)

Read more:

- [Thinfinity® Remote Desktop Server toolbar and how to customize it](#)
- [Browser Resizing](#)

11.1.5 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 Thinfinity® Remote Desktop 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);

    }

}
```

Read more:

- [Keystroke Methods](#)
- [SSL Certificate](#)
- [Demo](#)

11.1.6 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 Thinfinity® Remote Desktop Server SDK library it is possible to send any keystroke combination to the server by using a list of methods available in any Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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();  
  }  
}
```

Read more:

- [SSL Certificate](#)
- [Demo](#)

11.1.7 SSL Certificate

When you embed Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server IP separated by underlines instead of dots, following the example below:

Suppose your Thinfinity® Remote Desktop 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.

Read more:

- [Demo](#)

11.1.8 Demo

Along with the Thinfinity® Remote Desktop Server installation we have shipped an html demo.

This demo is an HTML page that has an example of SDK usage in "[Local mode](#)". Thinfinity® Remote Desktop Server is embedded in a div placed inside the same web page.

This HTML example is located in the 'sdk.html' file inside the Thinfinity® Remote Desktop Server web directory under the Thinfinity® Remote Desktop Server installation directory (e.g.: C:/Program Files/Thinfinity/Remote Desktop Server/webrdp).

You can try this demo directly from Thinfinity® Remote Desktop Server, by opening on your web browser the Thinfinity® Remote Desktop 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](#).

11.2 External Authentication

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

How to authenticate against Thinfinity® Remote Desktop Server from external applications:

The authentication against Thinfinity® Remote Desktop Server can be done using:

- username and password or
- username and an [ApiKey](#).

Every time you call Thinfinity® Remote Desktop 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 browser 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 Thinfinity® Remote Desktop Server enables external applications to dynamically negotiate a key to use the Diffie Hellman Key Exchange method for posterior encryption.

Read more:

[Apikey](#)

Learn also about these single-sign-on methods Thinfinity® Remote Desktop Server is compatible with:

[OAuth/2](#)
[CAS](#)

11.2.1 Apikey

The ApiKey is a secret value, known only by Thinfinity® Remote Desktop Server and a corporate application that connects to it.

By sending the ApiKey, the corporate application is identifying itself as trusted. In some cases, Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server ini configuration file. The location of this file depends on the Windows version Thinfinity® Remote Desktop Server is running at:

C:\ProgramData\Cybele Software\Thinfinity\Remote Desktop Server
\Thinfinity.RemoteDesktop.Server.ini

or

C:\Documents and Settings\All Users\Application Data\Cybele Software\Thinfinity\Remote Desktop Server\Thinfinity.RemoteDesktop.Server.ini (older Windows versions)

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](#) .

11.3 Single Sign On

In 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, Thinfinity® Remote Desktop Server has to internally [translate and store different credentials](#) for the supported single-sign-on methods, in order to interpret them into the Thinfinity® Remote Desktop Server local credentials

OAuth 2.0 integration:

The configuration options for OAuth 2.0 have been expanded. Now, OAuth /2 authentication servers other than Google are also supported by Thinfinity Remote Desktop Server. OAuth 2.0 is a protocol that validates users against a remote server. This means that Thinfinity Remote Desktop Server doesn't validate the user internally, using a username and password. The user authentication is relayed to the OAuth 2.0 server. Once the OAuth 2.0 server validates the user, it returns a validation code to Thinfinity Remote Desktop Server. This code will allow Thinfinity Remote Desktop Server to access a token. This token provides access to user information —such as the user email— in the OAuth 2.0 authentication server. Thinfinity Remote Desktop Server uses this token to request this information. Although not specified by the OAuth 2.0 normative, the Profile information server usually returns a JSON object. This JSON object includes values that can be used in Thinfinity Remote Desktop Server to validate the user. These values are mapped to Windows users, so that the corresponding Thinfinity Remote Desktop Server permissions are applied.

In order to use OAuth 2.0 in Thinfinity Remote Desktop Server, add “/oauth2” or “/google” to the Thinfinity Remote Desktop Server URL:

`https://<ThinfinityRDServer>/oauth2`

This is the callback URL that has to be configured in the OAuth 2.0 server in order to return the user validation code so that Thinfinity Remote Desktop Server can continue with the validation process.

Thinfinity Remote Desktop Server gets its address from the route where the browser request is made. This information cannot be modified.

- [Facebook OAuth authentication example](#)
- [Enabling OAuth/2 on Thinfinity® Remote Desktop Server](#)

Google accounts integration:

Thinfinity® Remote Desktop Server authentication can be integrated to the Google accounts. On the links below you will find the information to set up Thinfinity® Remote Desktop Server to work with this method:

- [Google OAuth/2](#)
- [Google ID for web applications](#)
- [Enabling Google OAuth/2 on Thinfinity® Remote Desktop Server](#)

RADIUS integration:

Thinfinity® Remote Desktop Server authentication can be integrated with a RADIUS account. On the links below you will find the information to set up Thinfinity® Remote Desktop Server to work with this method:

- [RADIUS](#)
- [Enabling RADIUS on Thinfinity® Remote Desktop Server](#)

Other single-sign-on methods:

Any other method can also be supported by Thinfinity® Remote Desktop Server. To make any other methods work with Thinfinity® Remote Desktop Server you have to [map external users to Thinfinity® Remote Desktop Server](#) and substitute the password with the [Thinfinity® Remote Desktop Server ApiKey mechanism](#).

11.3.1 Facebook OAuth Authentication Example

This is how an integration with Facebook OAuth 2.0 authentication would work:

First, a user creates an application in <https://developers.facebook.com/>. Their Facebook application App ID and App Secret must be loaded in [the 'General' tab](#) in the 'Client ID' and 'Client Secret' fields, respectively.

In the Facebook application Settings → Advanced menu, they must enter their Thinfinity Remote Desktop Server URL: "https://<ThinfinityRDServer>/oauth2" as "Valid OAuth redirect URIs" under the 'Client OAuth Settings' title.

Then in [the 'Server' tab](#), they must indicate that the Server Kind is 'Custom' and then fill in the rest of the values like this, although Thinfinity comes with different authentication methods already configured :

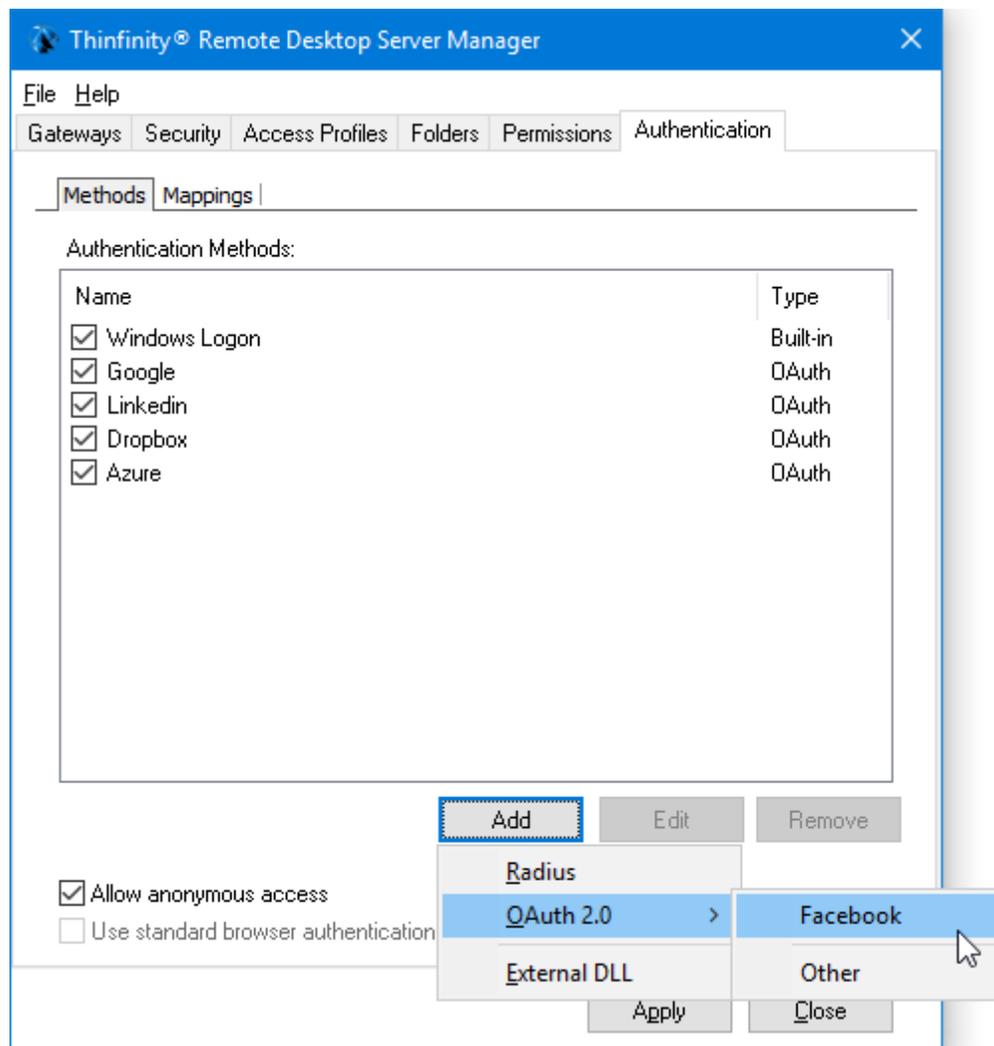
Authorization URL: <https://www.facebook.com/dialog/oauth>

Other Keys: scope=email

Token Validation URL: https://graph.facebook.com/oauth/access_token

Profile Information URL: <https://graph.facebook.com/me?fields=email>

Login Username value in returned JSON: email



The screenshot shows the 'Authentication Method Settings' dialog box. At the top, the 'Name' field is set to 'Facebook' and the 'Virtual Path' field is set to 'facebook'. Below these are two tabs: 'General' and 'Server'. The 'Server' tab is selected, showing the following fields: 'Authorization URL' (https://www.facebook.com/dialog/oauth), 'Authorization parameters' (scope=email), 'Token Validation Server URL' (https://graph.facebook.com/oauth/access_token), 'Token Validation extra parameters' (empty), 'Profile information server URL' (https://graph.facebook.com/me?) with a checked 'Add default parameters' checkbox, and 'Login username value in returned JSON' (email). 'Ok' and 'Cancel' buttons are at the bottom right.

Finally, in [the 'Mapping' tab](#), they must match the emails of the users that will be validated with Facebook with their corresponding Windows user for Thinfinity Remote Desktop Server.

11.3.2 Google OAuth/2

Users can be authenticated in Thinfinity® Remote Desktop Server by using their Google Accounts. This kind of authentication requires the system administrator to configure a few settings on Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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 [Thinfinity® Remote Desktop Server Manager SSO tab](#).
3. Enter the e-mails that will be authenticated against Thinfinity® Remote Desktop Server. This setup will be available under the [Mapping tab](#) in the Thinfinity® Remote Desktop Server Manager.
4. Associate the Active Directory Users/Groups with the authorized e-mails also on the Thinfinity® Remote Desktop Server Manager, in the [Mapping tab](#) also.

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 Thinfinity® Remote Desktop Server application from this tab, using the configured URI (e.g.: <https://ThinfinityRDP/google>).
3. The application will automatically recognize you, but before connecting to Thinfinity® Remote Desktop Server, it will ask permission to access your account information.
4. Press the Allow Access button, and you will be automatically authenticated against Thinfinity® Remote Desktop Server and redirected to the [Start Page](#).

11.3.2.1 Google Client ID for Web Applications

Before configuring the Thinfinity® Remote Desktop 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](#) ▾

[@cybelesoft.com](#) ▾ | [Settings](#) ▾ | [Help](#) | [Sign out](#)

Google apis

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.

[Create project...](#)

© 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](#) ▼ [@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](#)



[Create an OAuth 2.0 client ID...](#)

© 2011 Google - [Code Home](#) - [Privacy Policy](#)

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

- 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.
- The Google account does not have to be changed.
- 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:

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

Product logo:



Max size: 120x60 pixels

[Learn more](#)

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 [\(more options\)](#)

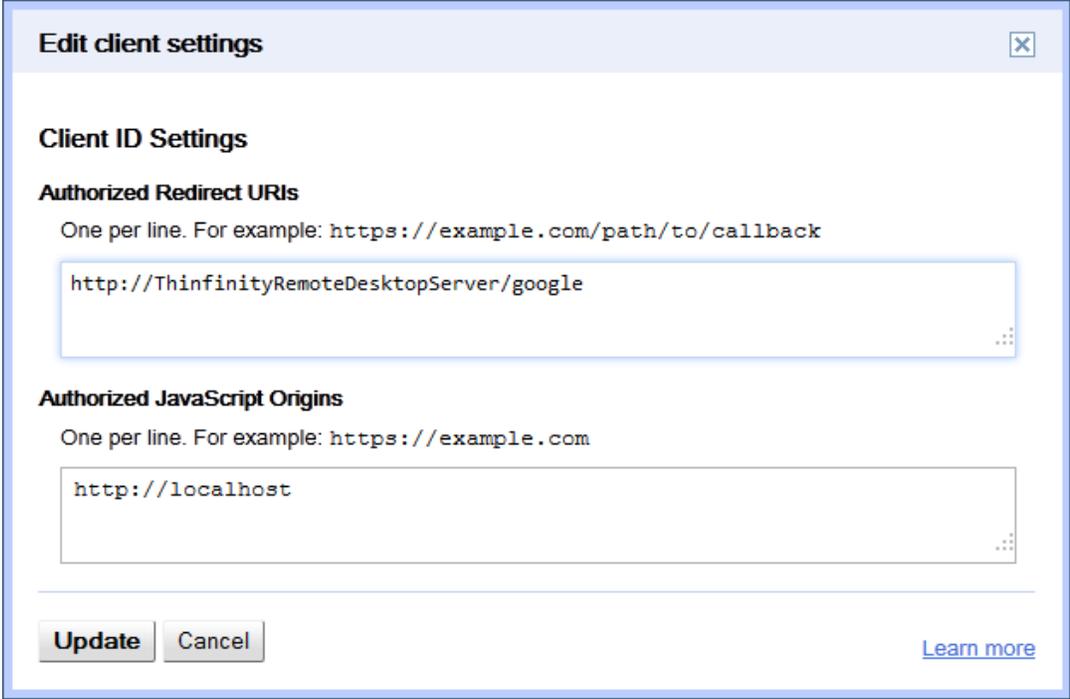
For example: `www.example.com` or `localhost`

Redirect URI

`https://www.example.com/oauth2callback`

[Learn more](#)

8. Once the account is created, click on the "Edit Settings" button and change the URI to `http://ThinfinityRDPServer: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://ThinfinityRemoteDesktopServer/google`

Authorized JavaScript Origins
One per line. For example: `https://example.com`

`http://localhost`

Update **Cancel** [Learn more](#)

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

[Correo](#) [Calendar](#) [Docs](#) [Sites](#) [Grupos](#) [Contactos](#) [Más](#) ▾[@cybelesoft.com](#) ▾ | [Configuración](#) ▾ | [Ayuda](#) | [Cerrar sesión](#)

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: Thinfinity Remote Desktop Server

Google account: kdesouza@cybelesoft.com

[Edit branding information...](#)

Client ID for web applications

Client ID: 964696463302.apps.googleusercontent.com

Email address: 96462232302@developer.gserviceaccount.com

Client secret: c7YssKgCKgCqGiUbjzuWx4LX

Redirect URIs: http://localhost/oauth2callback

JavaScript origins: http://localhost

[Edit settings...](#)[Reset client secret...](#)[Create another client ID...](#)

11.3.3 RADIUS

Users can be authenticated in Thinfinity® Remote Desktop Server by using RADIUS. This kind of authentication requires the system administrator to configure a few settings on the Thinfinity® Remote Desktop Server Manager.

Requirements

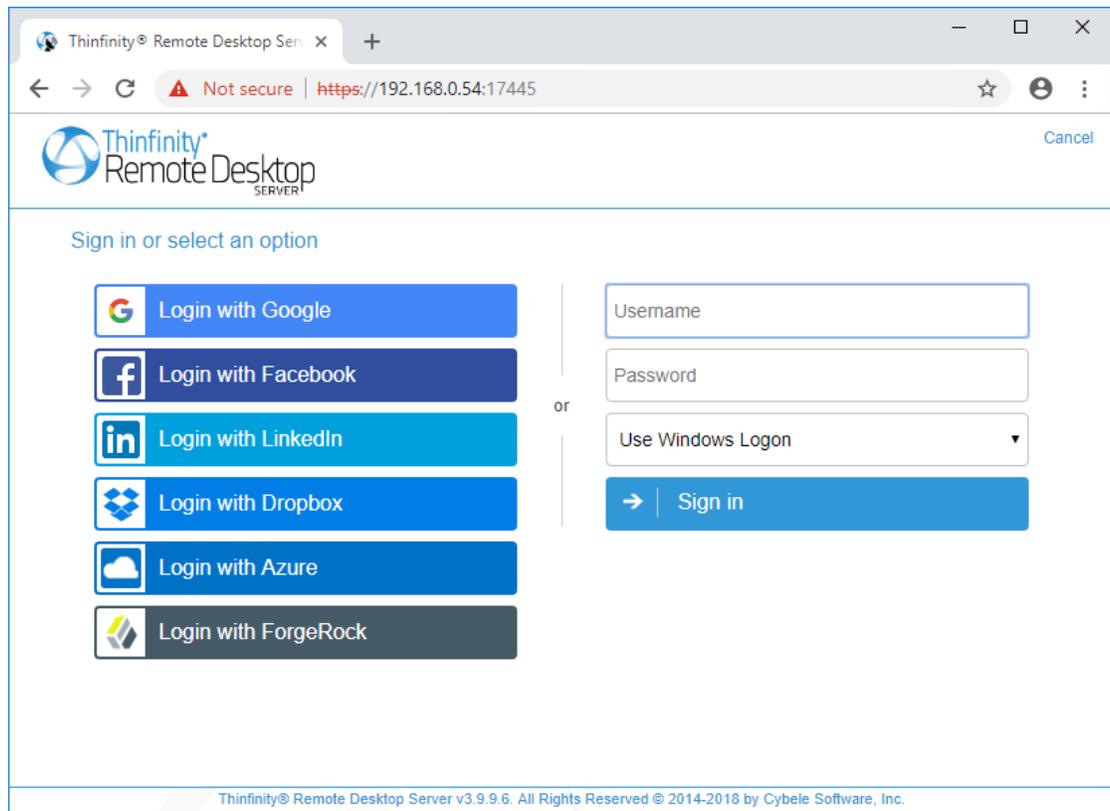
The Thinfinity® Remote Desktop Server authentication level must set to [Access Profiles](#).

Setting up the integration

1. Verify that your RADIUS account is up and running and collect the following information: Server IP, Port, Shared Secret and Authentication type.
2. Enable the Integration through the [Thinfinity® Remote Desktop Server Manager SSO tab](#).
3. Enter the RADIUS remote usernames that will be authenticated against Thinfinity® Remote Desktop Server. This setup will be available under the [Thinfinity® Remote Desktop Server Manager SSO tab](#), in the 'Mapping' tab.
4. Associate the Active Directory Users/Groups with the authorized RADIUS users in the Thinfinity® Remote Desktop Server Manager's [Mapping tab](#) .

How to use it

1. In the Thinfinity® Remote Desktop Server login screen:



Note: Thinfinity Remote Desktop Server allows you to use Windows authentication, external authentication, or both. This option is set in [the 'Security' tab](#) of the Manager. Typically you will not see this, but when both options are enabled, make sure to choose the authentication you will be using:



Enter your credentials

Username:

Password:

Security method: ▼

- Windows Logon
- windows logon
- radius

2. Enter your RADIUS credentials.
3. Press login.

11.4 Customizing the Web Interface

Thinfinity® Remote Desktop 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.

11.4.1 Changing the Logo

Modifying the application logo can be as simple as copying the new logo image and telling Thinfinity® Remote Desktop 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 Thinfinity® Remote Desktop Server installation directory.
(e.g.: C:/Program Files/Thinfinity® Remote Desktop 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/Thinfinity® Remote Desktop 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/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.

11.4.2 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 Thinfinity® Remote Desktop Server installation directory. (e.g.: C:/Program Files/Thinfinity® Remote Desktop 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/Thinfinity® Remote Desktop 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.

11.4.3 Files Location

We recommend that you 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:

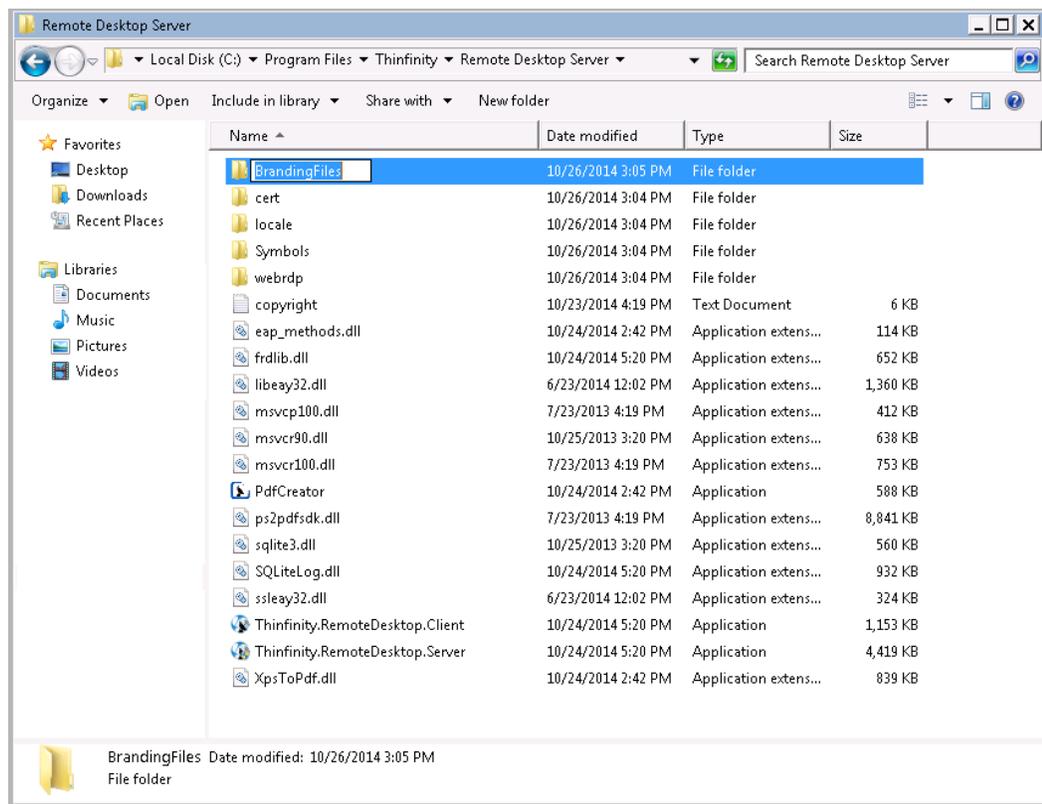
- a) Have the possibility to get back to the original interface configuration, at anytime
- b) Make sure that your files will be safe after a version upgrade.

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](#).



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 a URL.
- 2) The paths to the files, indicated in the "WebAliases.ini" have to be absolute, as shown in the example below:

```
[Alias]

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

11.5 Web Services API

The Web Services API is intended to allow external applications to access and manipulate some of Thinfinity® Remote Desktop Server data and settings.

Thinfinity® Remote Desktop Server has two different Web Services available:

a. Profiles Web Service:

If you need to manipulate Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server Analytics feature is included since version 2.0.0.16. This feature keeps statistic data of Thinfinity® Remote Desktop Server logins, sessions, connections and used browsers. The [Analytics Web Service](#) allows external applications to access these information.

Requirements for the Web Service API:

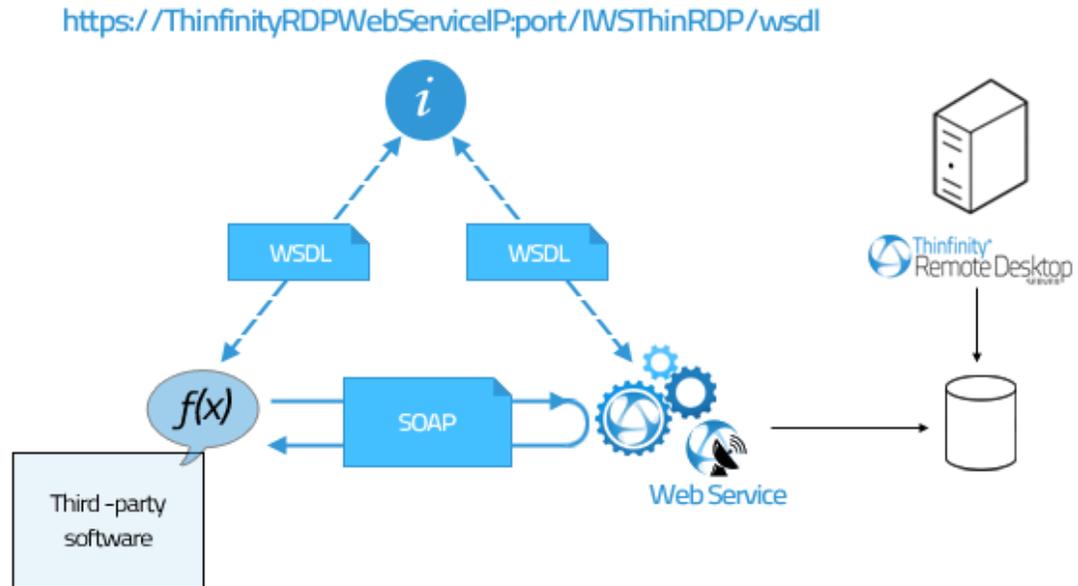
1. The Profiles Web Service is valid for environments using Access Profiles as the Thinfinity® Remote Desktop Server authentication mode.
2. The integration has to be done at a programming level. You will need to develop or modify an application which will act as the Web Service requester and this application will have to implement the Thinfinity® Remote Desktop Server Web Service interface.

Read more:

- [Architecture](#)
- [Installing the Webservice](#)
- [Setting up the communication settings](#)
- [Profiles Web Service](#)
- [Analytics Web Service](#)

11.5.1 Architecture

The Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server on the following address, once the Web Service is installed:

<https://ThinfinityRDPWebServiceIP:port/IWSThinRDP/wsdl>

Read more:

- [Installing the WebService](#)
- [Setting up the communication settings](#)
- [Profiles Web Service](#)
- [Analytics Web Service](#)

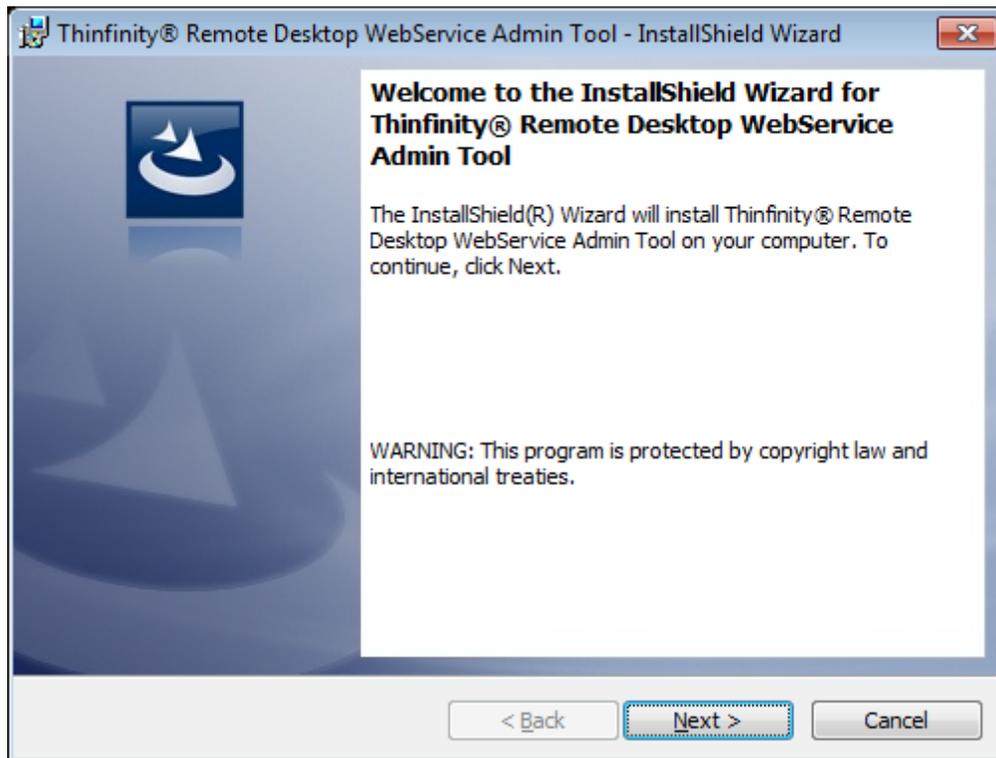
11.5.2 Installing the Web Service

The first step to start developing the integration with Thinfinity® Remote Desktop Server Web Service API is to install it:

1. Download the installer from the link below:

<http://www.cybelesoft.com/download/>

2. Execute the installer on the same machine where Thinfinity® Remote Desktop Server is installed.



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

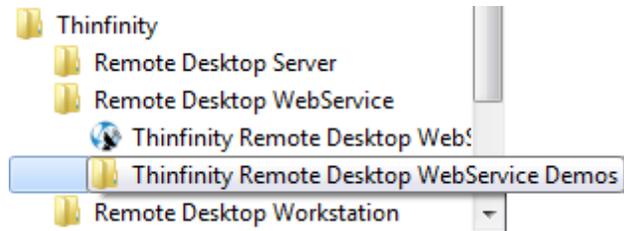
- I. Set up a service on Windows, so the Web Service will be started every time Windows is turned on.

⚙️ Telephony	Provides Tel...		Manual
⚙️ Themes	Provides us...	Started	Automatic
⚙️ Thinfinity Remote Desktop Server	Allows secu...	Started	Automatic
⚙️ Thinfinity Remote Desktop WebService Admin Tool	Allows rem...	Started	Automatic

* 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 "*WebService Admin tool*"

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



Read more:

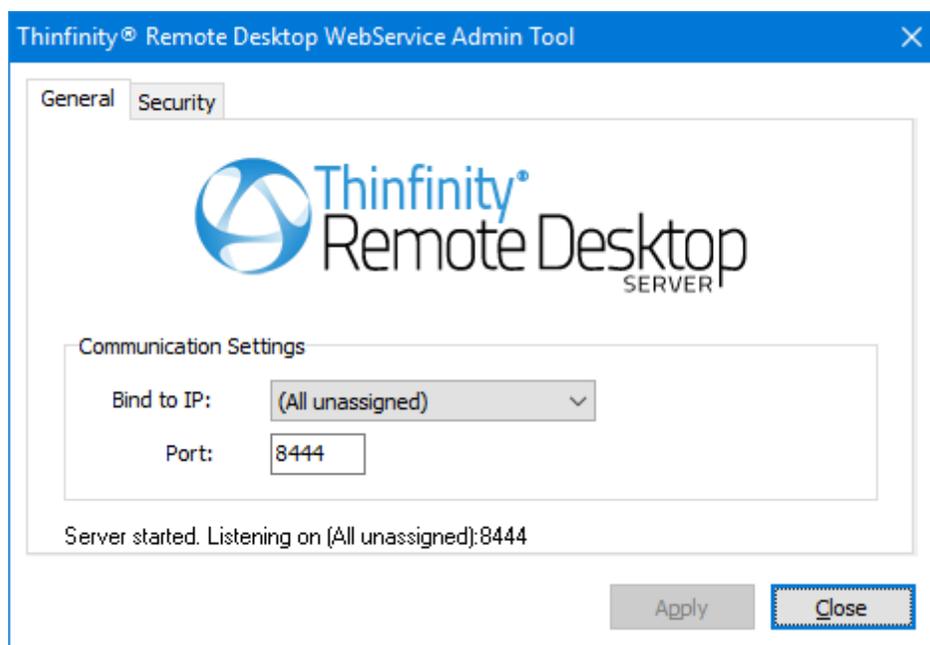
- [Setting up the communication settings](#)
- [Profiles Web Service](#)
- [Analytics Web Service](#)

11.5.3 Setting up the Communication Settings

Open the "WebService Admin Tool" from the Windows start menu.

General tab:

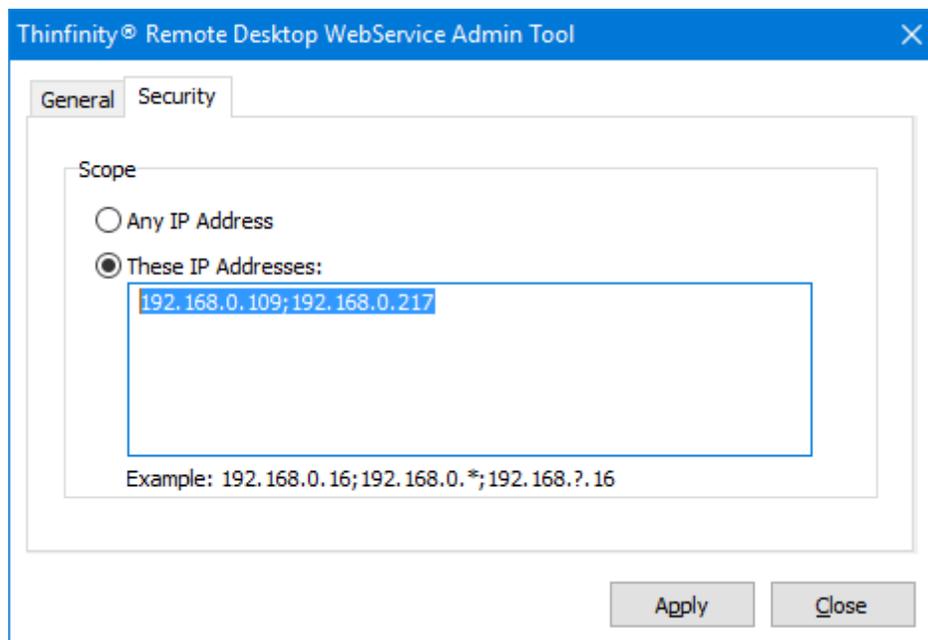
1. Go to the "General" tab.
2. On the "Bind to IP" field inform the IP address you want the Web Service to be listening on. If you need all the server IP's to listen to the service, select the "All unassigned" option.
3. Inform also what "Port" you want the service to be listening on in the "Port" field.



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.



1. Substitute 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.

Read more:

- [Profiles Web Service](#)
- [Analytics Web Service](#)

11.5.4 Profiles Web Service

The Access Profiles Web Service integration allows external applications to:

1. Retrieve any information from the profiles configured in Thinfinity® Remote Desktop 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.

Read more:

- [Methods](#)
- [Types](#)
- [The demo applications](#)
- [Analytics Web Service](#)

11.5.4.1 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 Thinfinity® Remote Desktop Server	If there are no profiles yet, returns a WSProfileArray with 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 with a computer.	string: computer IP	WSProfileArray: profiles associated with the informed computer.	If there are no profiles associated with the computer, returns a WSProfileArray with length = 0.
FindByUserName	Returns all profiles assigned to the user.	string: username	WSProfileArray: user granted profiles.	If there is are no profiles associated with the user, returns a WSProfileArray with 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.	WSPProfile: 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 WSPProfile ID, returns a value \neq 0.
NewPublicKey	Generates a new public key for an existing profile.	string: profile ID	WSPProfile: profile carrying the new Public Key.	If there is no profile matching the WSPProfile 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.			

Read more:

- [Types](#)
- [The Demo Applications](#)

11.5.4.2 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	Value range
WSProfile	Complex	The <code>WSProfile</code> type represents one profile. It has all the attributes that describe a profile.	
<code>WSProfileArray</code>	Complex	The <code>WSProfileArray</code> is an array of WSProfile . It is used mostly as a parameter for methods that retrieve more than one profile from the server.	
<code>TRdpCredentials</code>	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"
<code>TRdpScreenBPP</code>	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"
<code>TRdpScreenResolution</code>	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 Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server works with.	"sqPoor" "sqGood" "sqOptimal" "sqExcellent"

Read more:

- [The Demo Applications](#)

11.5.4.2.1 The WSPProfile type

The complex WSPProfile type represents a profile and carries all its information. In order to retrieve, create, delete and update the Thinfinity® Remote Desktop Server profiles, you will have to manipulate this WSPProfile 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	TRdpCredential s	Configures the credential mode Thinfinity® Remote Desktop Server 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	TRdpScreen Resolution	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 off-screen surfaces in video memory. Also, the desktop will present many visual effects.	yes
PrinterEnabled	boolean	Uncheck this option to disable Thinfinity® Remote Desktop Server PDF printer.	yes
PrinterSetAsDefault	boolean	Mark this option to make Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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, Thinfinity® Remote Desktop Server will automatically download any file saved/copied in 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 Thinfinity® Remote Desktop Server 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

11.5.4.3 The Demo Applications

We have packed with the Thinfinity® Remote Desktop Server installation two example applications that use Thinfinity® Remote Desktop Server Web Service to manipulate Access Profiles.

If you have already [installed Thinfinity® Remote Desktop Server WebService](#), you can access the demos from the Windows Start menu: All Programs/Thinfinity Remote Desktop Server/Thinfinity Remote Desktop Server Demos.

Both applications 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 Webservice 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 become 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 Thinfinity® Remote Desktop Server application, until you call the `Commit` method on the Web Service.

Read more:

- [Analytics Web Service](#)

11.5.5 Analytics Web Service

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

Read more:

- [Methods](#)
- [Types](#)
- [The demo application](#)

11.5.5.1 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 nam	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	WSDBRecordA rray	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	WSDBRecordAr rray	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: WSQueryRang e ; Successful: Boolean Failed: Boolean	WSDBRecordAr rray	If the search does not match any record, the result will be a WSDBRecordArray with length = 0.

Read more:

- [Types](#)
- [The demo application](#)

11.5.5.2 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	Value range
WSQueryType	Simple	The WSQueryType represents the available query types to be performed on the Web Service. The possible options are "qtSessions", "qtConnections" and "qtBrowsers".	"qtSessions" "qtConnections" "qtBrowsers"
WSQueryInfo	Complex	This type is used to send a filter criteria to the server when 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 when 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 WSDBBrowserRecord).	
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 WSDBBrowserRecord type describes how a Browser record is structured.	

Read more:

- [WSQueryInfo](#)
- [WSQueryRange](#)
- [WSDBLoginRecord](#)
- [WSDBSessionRecord](#)

- [WSDBConnectionRecord](#)
- [WSDBBrowserRecord](#)
- [The demo application](#)

11.5.5.2.1 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

Read more:

- [WSQueryRange](#)
- [WSDBLoginRecord](#)
- [WSDBSessionRecord](#)
- [WSDBConnectionRecord](#)
- [WSDBBrowserRecord](#)

11.5.5.2.2 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

Read more:

- [WSDBLoginRecord](#)
- [WSDBSessionRecord](#)
- [WSDBConnectionRecord](#)
- [WSDBBrowserRecord](#)

11.5.5.2.3 WSDBLoginRecord

The WSPProfile complex type represents a profile and carries all its information. In order to retrieve, create, delete and update the Thinfinity® Remote Desktop Server profiles, you will have to manipulate this WSPProfile data structure.

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

Read more:

- [WSDBSessionRecord](#)
- [WSDBConnectionRecord](#)
- [WSDBBrowserRecord](#)

11.5.5.2.4 WSDBSessionRecord

The WSDBSessionRecord type describes how a Session record is structured.

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

Read more:

- [WSDBConnectionRecord](#)
- [WSDBBrowserRecord](#)

11.5.5.2.5 WSDBConnectionRecord

The WSDBConnectionRecord type describes how a Connection record is structured.

Attribute name	Type	Description
<code>userField</code>	string	User that established the connection.
<code>sourceIPField</code>	string	IP Address from which the connection was established.
<code>hostField</code>	string	Host Name to which the connection was established.
<code>connStartField</code>	string	Date and time when the Connection was Started.
<code>connEndField</code>	string	Date and time when the Connection was Ended.

Read more:

- [WSDBBrowserRecord](#)

11.5.5.2.6 WSDBBrowserRecord

The WSDBSessionBrowser type describes how a Browser record is structured.

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

Read more:

- [The demo application](#)

11.6 One-Time-URL

Thinfinity® Remote Desktop 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 Thinfinity® Remote Desktop 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 Thinfinity® Remote Desktop Server on a Single-Sign-On Scheme along with external applications.

How it works:

1. First you need to ask Thinfinity® Remote Desktop Server to generate the URL for you. Call Thinfinity® Remote Desktop Server server following this URL format:

```
http(s)://ThinfinityRDP: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
<code>apikey</code>	The ApiKey is a secret value, known only by Thinfinity® Remote Desktop Server and the corporate application. Find out more about it on the ApiKey topic .
<code>apiuser</code>	Use this parameter to identify the user within Thinfinity® Remote Desktop Server. The value should be the user or email registered in your website. The users are seen in the Analytics Web Service .
<code>model</code>	Send the profile key of the profile you want to connect to. The profile's settings will work as a template for the One-Time-URL.

	connection that will be established. You can modify these settings by adding more parameters to the One-time-URL.
<code>plen</code>	The plen parameter carries the password length.
<code>expires</code>	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 Thinfinity® Remote Desktop Server 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.

```
/otur1.html?key=w7NJNschBdJD9e6G6luWh0Ca1M$oFW7guqC6jE1IQah3AJm3&pass=B0WZB8FG
```

Concatenate the Thinfinity® Remote Desktop Server address to the generated URL, following this format below:

```
http(s)://ThinfinityRDP:Port/otur1.html?  
key=w7NJNschBdJD9e6G6luWh0Ca1M$oFW7guqC6jE1IQah3AJm3&pass=B0WZB8FG
```

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.

Read more:

- [Configuring the Connection](#)
- [Enabling Features](#)

11.6.1 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
<code>model</code>	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
<code>overrideDefaults</code>	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 Thinfinity® Remote Desktop Server setting individually.

Find below the list of the parameters you can configure manually:

Parameter	What it means	Type/format	Default
<code>computer</code>	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	

<code>username¹</code>	The username to authenticate against the remote machine. If this parameter is not sent, Thinfinity® Remote Desktop Server will prompt the user for this information.	string username	
<code>password¹</code>	The password to authenticate against the remote machine. If this parameter is not sent, Thinfinity® Remote Desktop Server will prompt the user for this information.	string password	
<code>startprg</code>	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
<code>command</code>	Full remote application path that should start upon connection establishment.	string app path	
<code>directory</code>	Initial context directory to be used by the application set on command parameter described above.	string dir path	
<code>cmdargs</code>	Arguments to start the application specified on the "command" property.	string app args	
<code>bpp</code>	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
<code>resolution</code>	"fittobrowser", "fittoscreen", "fixed". When "fixed", the 'width' and 'height' parameters will be considered.	string toolbar size	"fittobrowser"
<code>width</code>	Remote desktop screen width. It will only be considered when the resolution parameter is set to "fixed".	integer pixels	Desktop width
<code>height</code>	Remote desktop screen height. It will only be considered when the resolution parameter is set to "fixed"	integer pixels	Desktop height
<code>imagequality</code>	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
<code>desktopbackground</code>	Set to true to show the original remote desktop background.	boolean true,false	false
<code>visualstyles</code>	Set to true to change the start menu and other windows features style.	boolean true,false	false

<code>menuwindowanimation</code>	Set to true to show an animation on the Start menu.	boolean true,false	false
<code>fontsmoothing</code>	Set to true to make text easier to read, especially magnified text.	boolean true,false	false
<code>showwindowcontent</code>	Set to true to show window's contents while dragging them.	boolean true,false	false
<code>desktopcomposition</code>	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
<code>unicodekeyboard</code>	Allows for using full unicode keyboard charsets. Set to false to connect to xRDP servers.	boolean true,false	true
<code>keyboardlayout</code>	Allows to specify the keyboard layout when unicode keyboard is disabled.	string Keyboard identifier (hexadecimal)	"00000409 (US)
<code>console</code>	Forces the connection to connect to the remote console session.	boolean true,false	false
<code>wcompression</code>	Set to true to enable the compression for the exchanged WebSocket data and have the application performance improved.	boolean true,false	true
<code>disablenla</code>	Set the option disableNLA if you use a CredSSP other than Microsoft.	boolean true,false	false
<code>desttype</code>	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	
<code>destinfo</code>	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	
<code>diskenabled</code>	Set to true to have an intermediate disk available on the connection.	boolean true,false	true
<code>diskname</code>	Identify the intermediate disk among the other remote desktop disks.	string name	"ThinDisk"

<code>diskautodownload</code>	Set to true to automatically download any file saved/copied in 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
...
```

Read more:

- [Enabling Features](#)

11.6.2 Enabling Features

You can also send some parameters on the queryString to enable Thinfinity® Remote Desktop Server features.

Find below the parameters you can send in order to enable and configure Thinfinity® Remote Desktop Server features for the One-Time-URL connection:

Clipboard:

Parameter	What it means	Type/format	Default
<code>clipboard</code>	Set to false to disable the remote desktop clipboard. The clipboard works only with text.	boolean true,false	true

Printer:

Parameter	What it means	Type/format	Default
<code>printerenabled</code>	Set to true to enable Thinfinity® Remote Desktop Server PDF printer.	boolean true,false	false
<code>printersetasdefault</code>	Thinfinity® Remote Desktop Server printer as the remote default printer.	boolean true,false	true
<code>printername</code>	Specify the printer name that you want to be shown on the remote machine's printer list.	string name	
<code>printerdriver</code>	Mark this option to set Thinfinity® Remote Desktop Server printer as the remote machine default printer.	string driver	

Sound:

Parameter	What it means	Type/format	Default
<code>soundenabled</code>	Set to true to enable remote sound.	boolean true,false	false
<code>soundquality</code>	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)

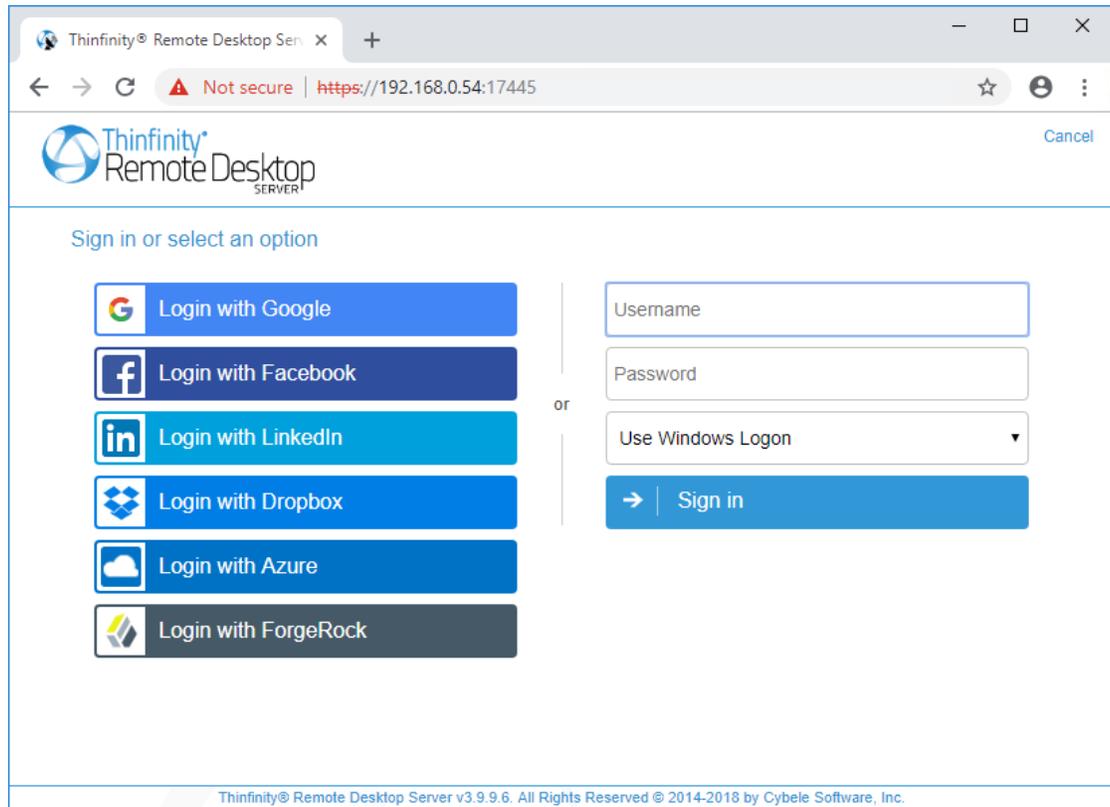
12 User guide

This section is a quick User Guide, focused on the everyday use of Thinfinity® Remote Desktop Server.

1. [Logging In](#)
2. [Connecting](#)
 - 2.1 [Connecting with Profiles](#)
 - 2.2 [Connecting with Open parameters](#)
3. [Toolbar](#)
4. [Features](#)
 - 4.1 [File Transfer](#)
 - 4.2 [Remote Sound](#)
 - 4.3 [Mapped Drives](#)
 - 4.4 [Analytics](#)
5. [Disconnecting](#)

12.1 Logging In

1. Open your preferred web browser.
2. Type into the address bar [http\(s\)://ThinfinityRDPip:ThinfinityRDPport/](http(s)://ThinfinityRDPip:ThinfinityRDPport/).



3. Enter your credentials (username and password) provided by the system administrator. **The system administrator should also let you know if you are using a Security method other than the default (Windows Logon).**

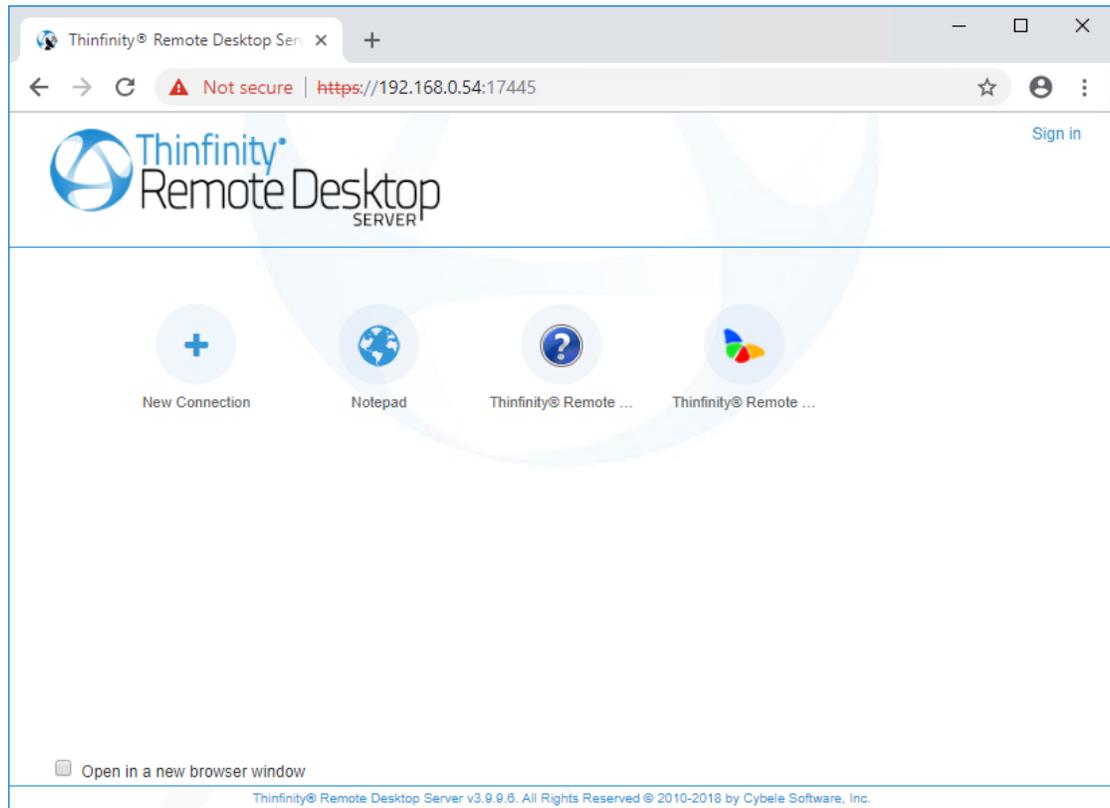
4. Press the "Sign In" button.

Read more:

- [Connecting](#)
- [Toolbar](#)
- [Features](#)
- [Accessing from Mobile Devices](#)
- [Disconnecting](#)

12.2 Connecting

Once you reach the Thinfinity Remote Desktop Server, you will be presented by either the "New Connection" button, or the specific Access Profiles designated by your system administrator :



If you only have the " New Connection" option, read the [Connection through open parameters](#) topic, to continue with the reading.

General Display Resources Program Experience Advanced 

Computer:

Username:

Password:

Read more:

- [Toolbar](#)
- [Features](#)
- [Accessing from Mobile Devices](#)
- [Disconnecting](#)

12.2.1 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.

The screenshot shows a configuration interface with a horizontal tab bar at the top containing 'General', 'Display', 'Resources', 'Program', 'Experience', and 'Advanced'. The 'General' tab is active. Below the tabs are three input fields: 'Computer:' with the value '192.168.0.52', 'Username:' with the value 'MyAdminUser', and 'Password:' which is empty. At the bottom right, there are two blue buttons: 'CONNECT' with a right-pointing arrow and 'BACK' with a left-pointing arrow.

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 plus (+) sign and you will see the settings tabs:

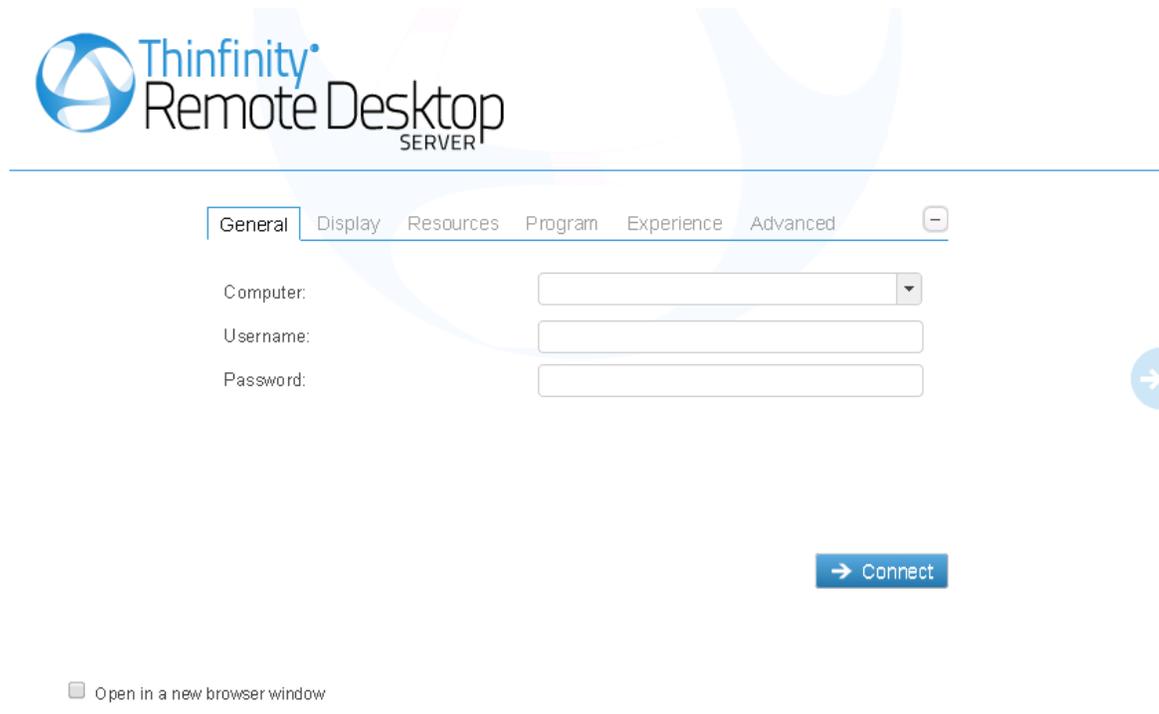
[The General tab](#)
[The Display tab](#)
[The Resources tab](#)
[The Program tab](#)
[The Experience tab](#)
[The Advanced tab](#)

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 .

12.2.1.1 General



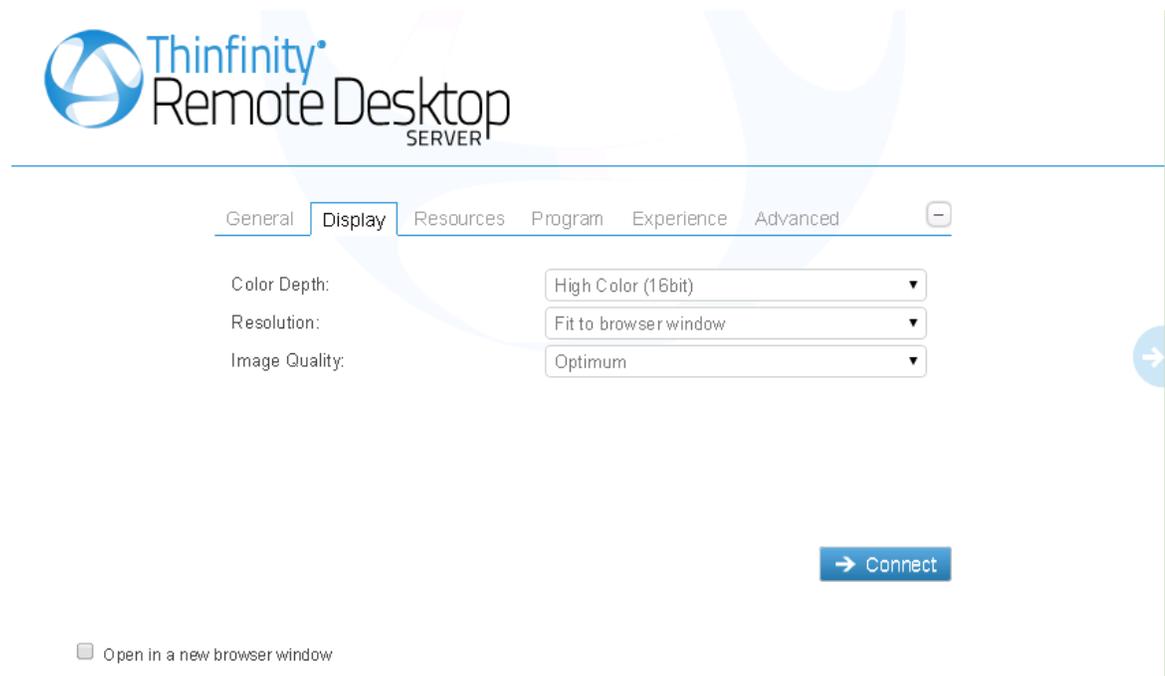
The screenshot shows the Thinfinity Remote Desktop Server web interface. At the top left is the logo for Thinfinity Remote Desktop SERVER. Below the logo is a horizontal menu with tabs: General (selected), Display, Resources, Program, Experience, and Advanced. Under the General tab, there are three input fields: Computer (a dropdown menu), Username (a text box), and Password (a text box). To the right of these fields is a blue button with a right-pointing arrow and the text "Connect". Below the input fields is a checkbox labeled "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](#).

12.2.1.2 Display

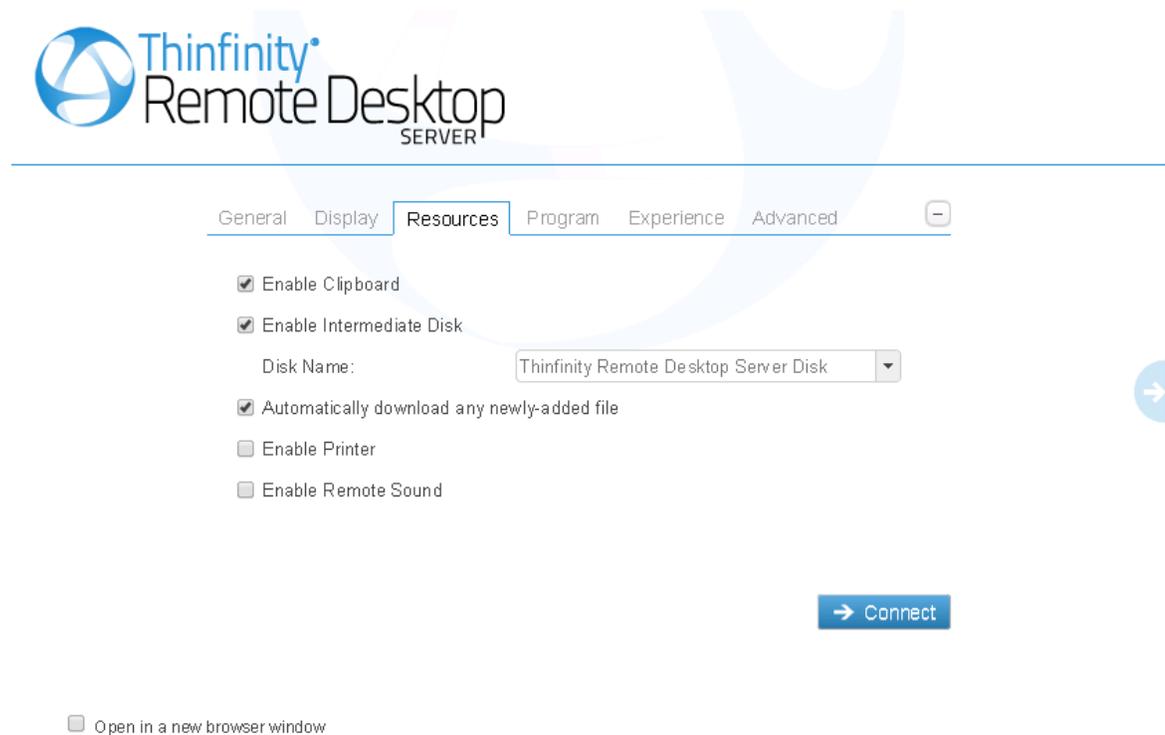


The web interface "Display" tab presents you with these following options:

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	<p>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:</p> <p>Highest - Works only with PNG images and has no compression (0% compression)</p> <p>Optimal - Combines PNG and JPEG images (20% compression).</p> <p>Good - Works only with JPEG images (40% compression)</p> <p>Faster - Works only with JPEG images (50%</p>

	compression).
--	---------------

12.2.1.3 Resources



The screenshot shows the Thinfinity Remote Desktop SERVER web interface. The 'Resources' tab is selected, showing several configuration options:

- Enable Clipboard
- Enable Intermediate Disk
 - Disk Name:
- Automatically download any newly-added file
- Enable Printer
- Enable Remote Sound

At the bottom right, there is a blue 'Connect' button with a right-pointing arrow. At the bottom left, there is an unchecked checkbox labeled '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.

The screenshot shows the Thinfinity Remote Desktop Server Administrator's Guide interface. The 'Resources' tab is selected, displaying the following settings:

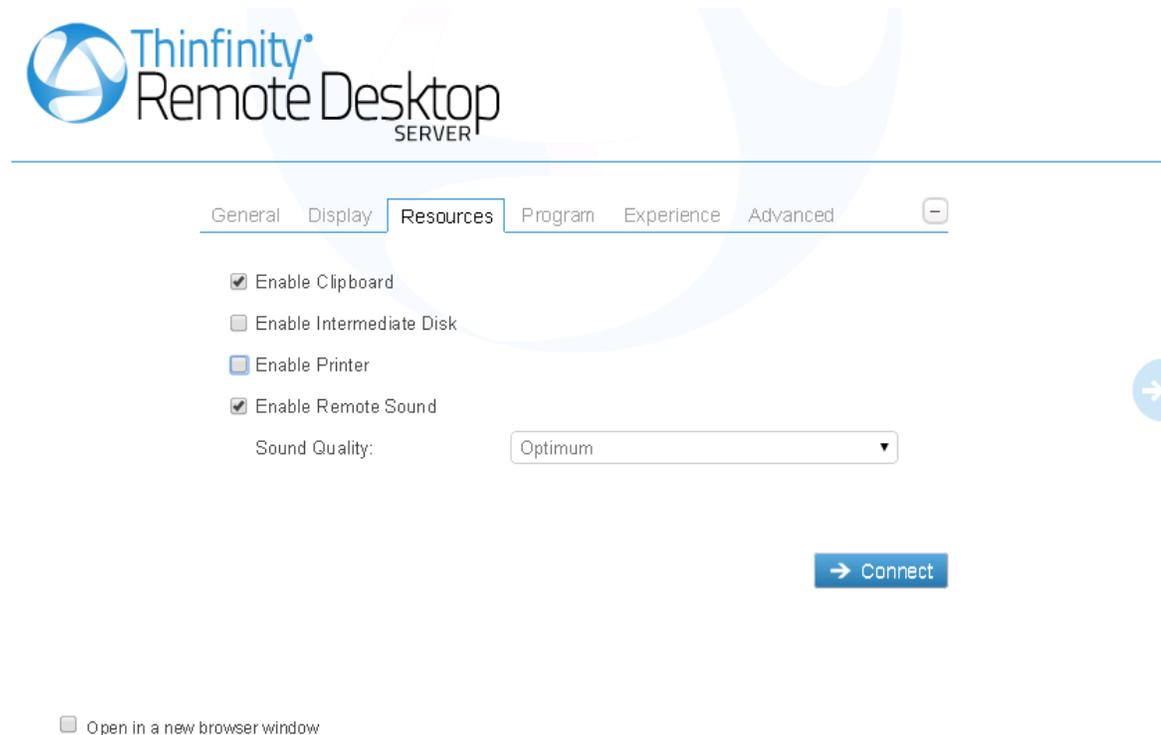
- Enable Clipboard
- Enable Intermediate Disk
- Enable Printer
 - Set As Default Printer
 - Printer Name:
 - PostScript Printer Driver:
- Enable Remote Sound

At the bottom right, there is a blue button labeled 'Connect' with a right-pointing arrow. At the bottom left, there is a checkbox labeled '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.

<p>Enable a Remote Printer</p>	<p>Uncheck this option to disable Thinfinity® Remote Desktop Server PDF printer.</p>
<p>Printer name</p>	<p>Specify the printer name that you want to be shown on the remote machine's printer list.</p>
<p>PostScript printer driver</p>	<p>This is the driver to be used by Thinfinity® Remote Desktop Server 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.</p>

Set as default printer	Mark this option to make Thinfinity® Remote Desktop Server printer the remote machine default printer.
--	--

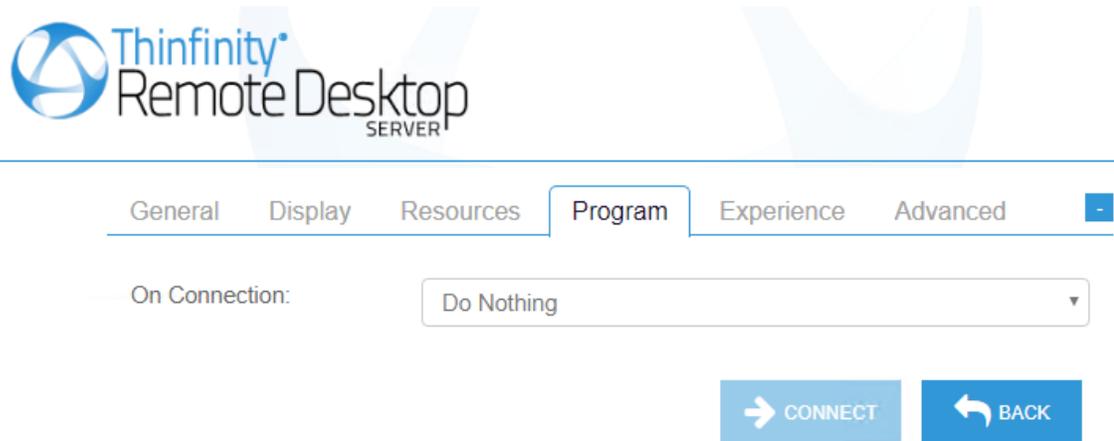


When you mark the "Enable Remote Sound" option, the interface will be seen as the image above. Learn below how each sound option works.

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 Thinfinity® Remote Desktop Server will use to reproduce the remote sound. The highest quality, the most resources will be required.

12.2.1.4 Program

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



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.



General Display Resources **Program** Experience Advanced ⊖

On Connection..

Start a Program ▾

Program path and file name:

Arguments:

Start in the following folder:

Available only within Windows Server versions.

→ Connect

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 Thinfinity® Remote Desktop Server, by selecting the "Execute as RemoteApp" on the Program tab.



General Display Resources **Program** Experience Advanced ⊖

On Connection...

Execute as RemoteApp ▾

Program path and file name:

Arguments:

Start in the following folder:

Available only within Windows Server versions.

Show Windows Login and Logout Screen

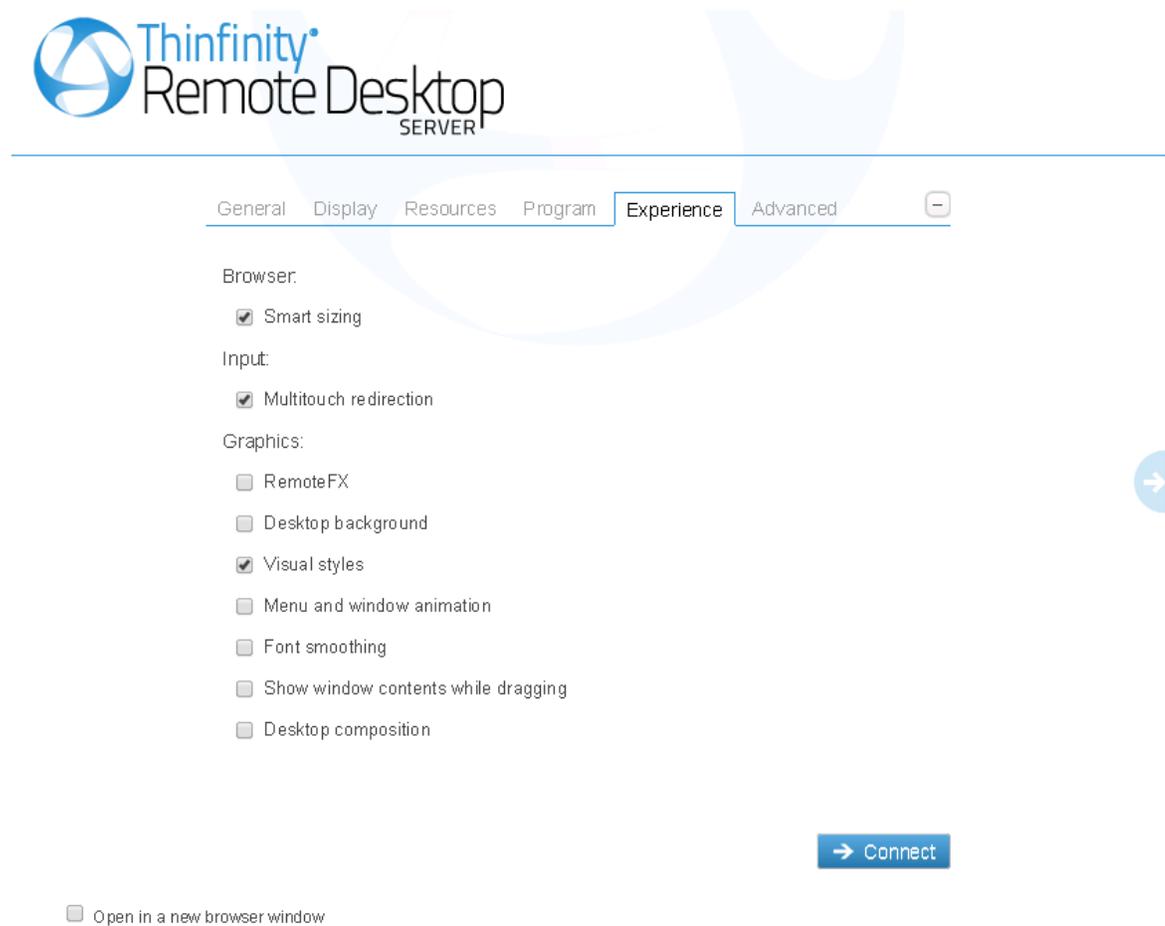
[→ Connect](#)

Open in a new browser window

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"

12.2.1.5 Experience



The screenshot shows the Thinfinity Remote Desktop SERVER web interface. At the top, there is a navigation bar with tabs: General, Display, Resources, Program, Experience (selected), and Advanced. Below the navigation bar, the interface is divided into sections: Browser, Input, and Graphics. Each section contains a list of settings with checkboxes. The 'Experience' tab is active, and the 'Connect' button is visible at the bottom right.

Thinfinity Remote Desktop SERVER

General Display Resources Program **Experience** Advanced

Browser:

- Smart sizing

Input:

- Multitouch redirection

Graphics:

- RemoteFX
- Desktop background
- Visual styles
- Menu and window animation
- Font smoothing
- Show window contents while dragging
- Desktop composition

[→ Connect](#)

Open in a new browser window

The web interface "Experience" tab presents you with these following options:

Smart Sizing	Check this option to scale the connection image. The maximum size of the connection will be the original desktop size.
Multitouch redirection	Check this option to enable Multitouch Redirection. Read more about Multitouch Redirection .
RemoteFX	Check this option to enable RemoteFX. Read More about Remote FX . This option affects other settings.
Desktop Background	Check this option to show the desktop background.

Visual Styles	Check this option to show Windows Visual Styles: the appearance of common controls, colors, borders, 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.

12.2.1.6 Advanced



General Display Resources Program Experience **Advanced**

- Unicode keyboard
- Keyboard Layout:
- Connect to console session
- Disable NLA Login
- Websocket compression
- Record remote desktop session
- Touch to relative mouse movements
- Touch to hold delay (Milliseconds)
- Minimum drag distance (Pixels)

→ Connect

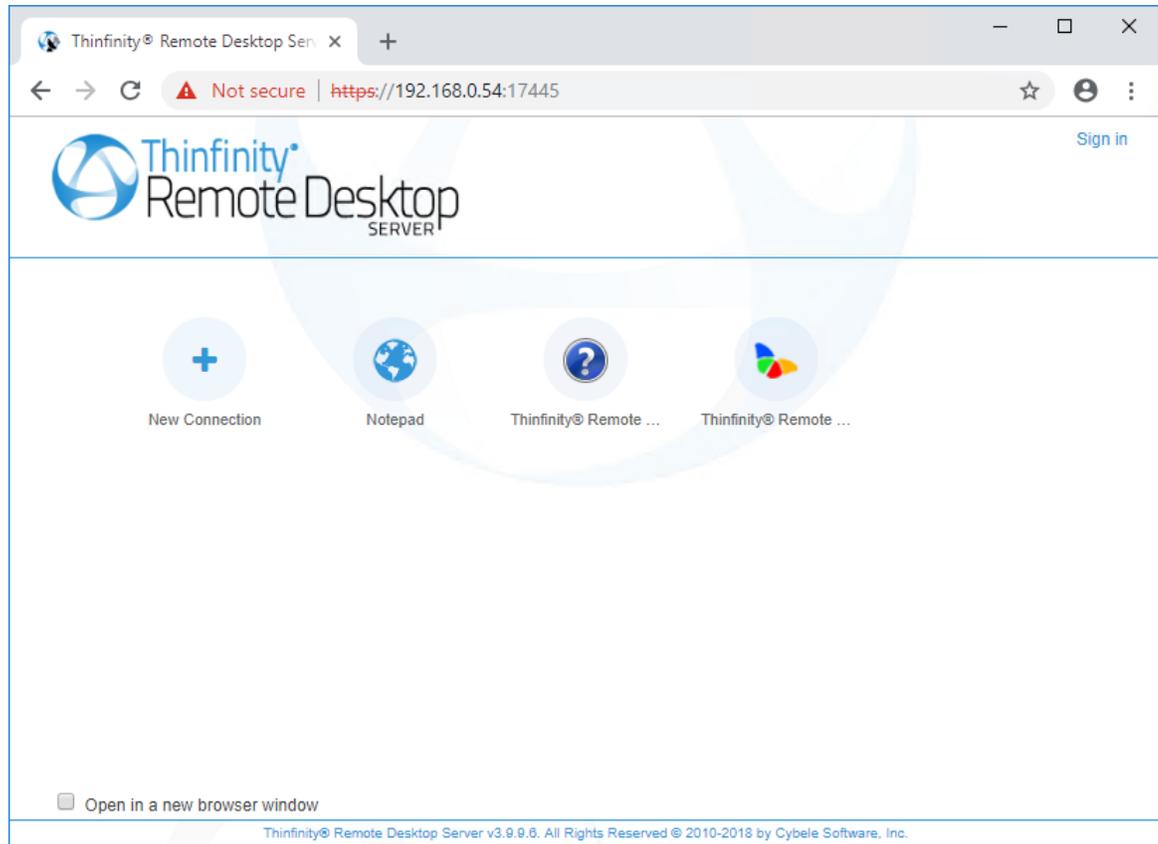
Open in a new browser window

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 behavior encountered in touch screen mobile devices, in which the screen cursor moves relatively to the touch. Uncheck this option to have a mouse behavior similar to the real desktop mouse in which the cursor will be always positioned under the touch.

12.2.2 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.

12.3 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](#).

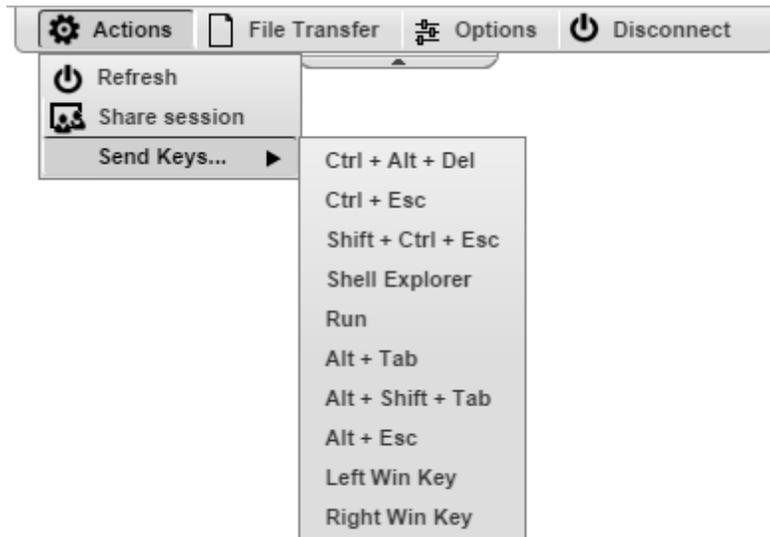


Read more:

- [Actions menu](#)
- [File Transfer menu](#)
- [Options menu](#)
- [Disconnect menu](#)
- [Features](#)
- [Accessing from Mobile Devices](#)
- [Disconnecting](#)

12.3.1 Actions

Click on the "Actions" button and its menu will open:



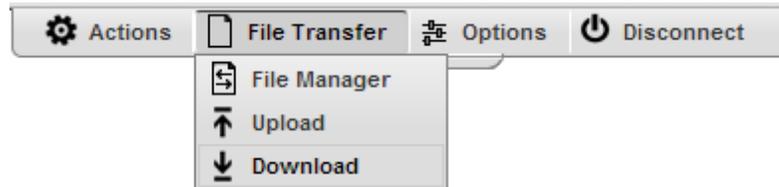
Refresh	The Refresh button performs a reconnection with the server, using the same parameters as the current connection, except for the screen size values, that will be updated to the current screen size (only if scale is on).
Share session	The Share session feature, allows you to share the current desktop 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.
View params & layout	Displays a list of parameters related to your connection.

Read more:

- [File Transfer menu](#)
- [Options menu](#)
- [Disconnect menu](#)

12.3.2 File Transfer

Click on the "File Transfer" button and its menu will open:



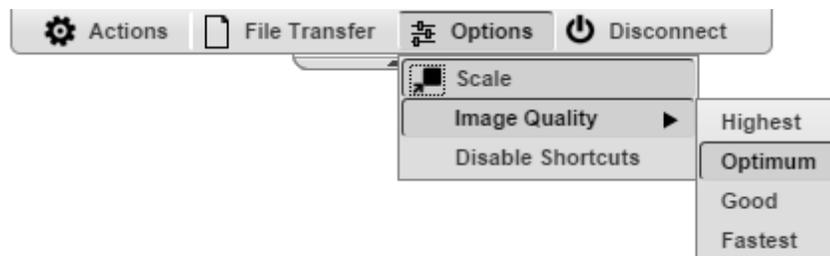
Upload	This option allows you to upload a file located on the local computer into the remote desktop.
Download	This option enables you to download any file located inside the Intermediate disk .
File Transfer	This option will open the File Transfer Manager . If the button is not available ask the system administrator to set you the permissions for it.

Read more:

- [Options menu](#)
- [Disconnect menu](#)

12.3.3 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

	<p>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:</p> <p>Highest - Works only with PNG images and has no compression (0% compression)</p> <p>Optimum - Combines PNG and JPEG images (20% compression).</p> <p>Good - Works only with JPEG images (40% compression)</p> <p>Fastest - Works only with JPEG images (50% compression).</p>
Disable shortcuts	<p>When you mark this option, Thinfinity® Remote Desktop Server will stop interpreting keyboard shortcuts. All the shortcut combinations will be redirected to the remote desktop exactly as they where typed in.</p>

Read more:

- [Disconnect menu](#)

12.3.4 Disconnect

The disconnect button will close the connection with the remote desktop.

**Read more:**

- [Features](#)

12.4 Features

These are some of the most important Thinfinity Remote Desktop Server features:

- [File Transfer](#)
- [Remote Printer](#)
- [Remote Sound](#)
- [Share Session](#)
- [Mapped Drives](#)
- [Analytics](#)

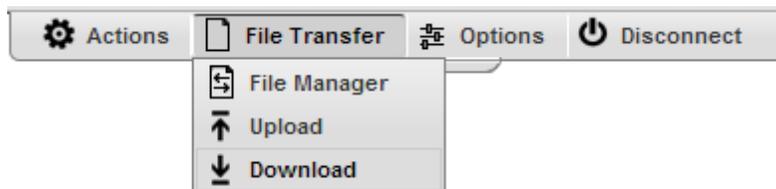
12.4.1 File Transfer

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.

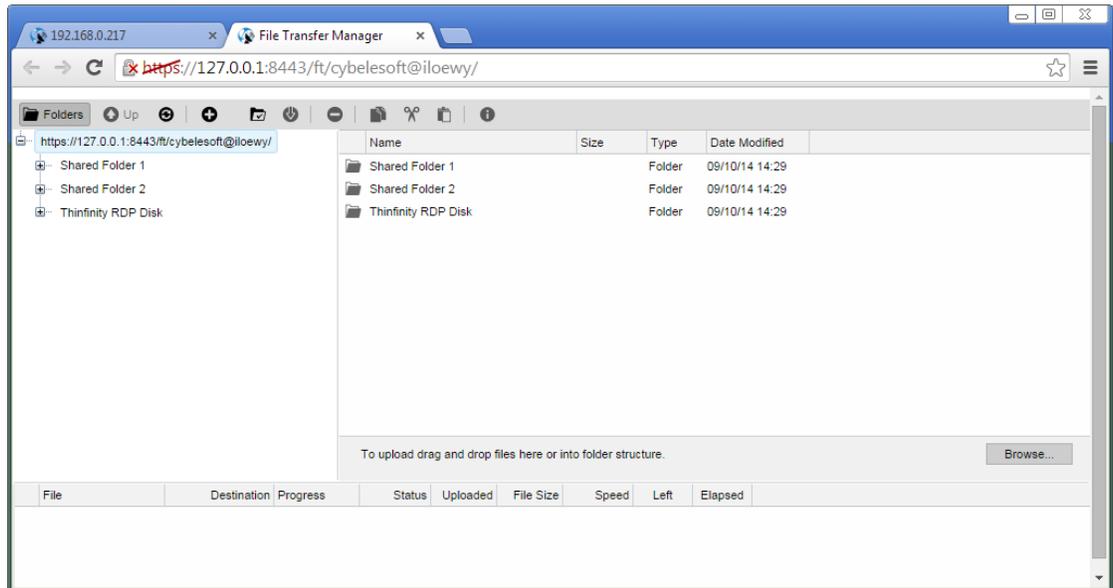


Upload	Click on this option to upload a file located on the local computer into the remote desktop. A window will be opened so that you can select the file to be uploaded.
Download	This option enables you to download any file located inside the Intermediate disk . Select the file on the presented list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



See also, the option to [Automatically download any newly-added file](#).

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



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.

Read more:

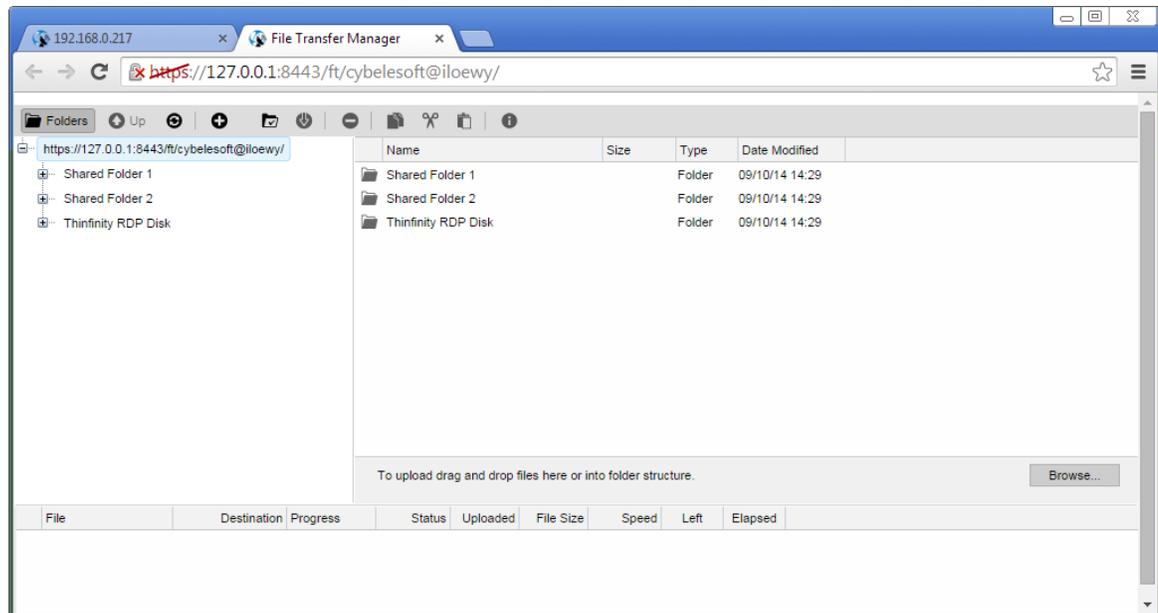
- [Navigating on the File Transfer Screen](#)
- [File Options](#)
- [Remote Folder Area Options](#)
- [Downloading and Uploading Files](#)

12.4.1.1 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.

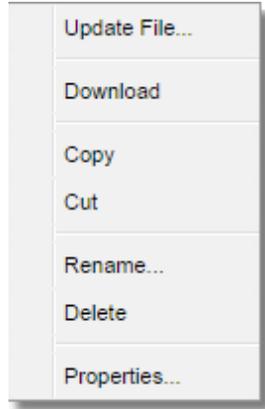


Read more:

- [File Options](#)
- [Remote Folder Area Options](#)
- [Downloading and Uploading Files](#)

12.4.1.2 File Options

Right click on a remote file to access these options:



Find the behaviour for each one of these options below:

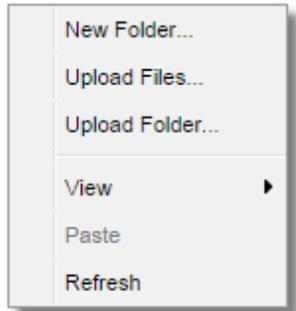
Update File	Choose this option to replace the selected remote file with a local file.
Open/Download	Choose this option to open or download the selected file.
Custom Properties	Choose this option to see the remote file's properties.
Copy	Choose this option to copy the file into the remote clipboard. You 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.

Read more:

- [Remote Folder Area Options](#)
- [Downloading and Uploading Files](#)

12.4.1.3 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.

Read more:

- [Downloading and Uploading Files](#)

12.4.1.4 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](#).

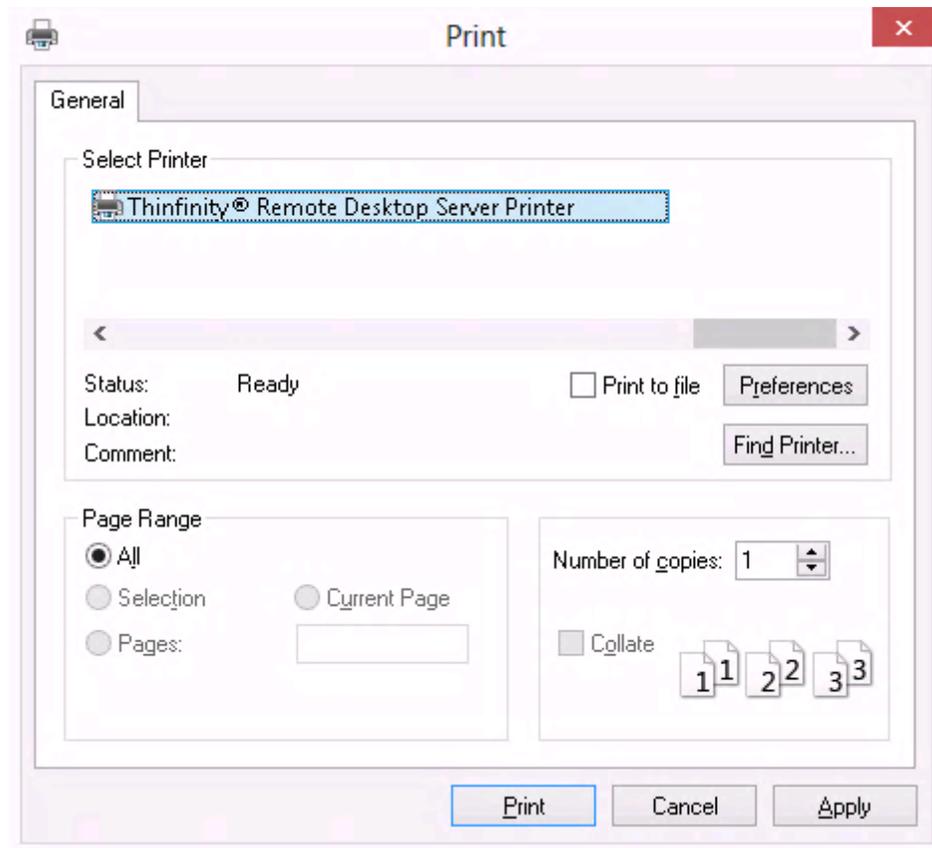
2. Uploading local files:

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.

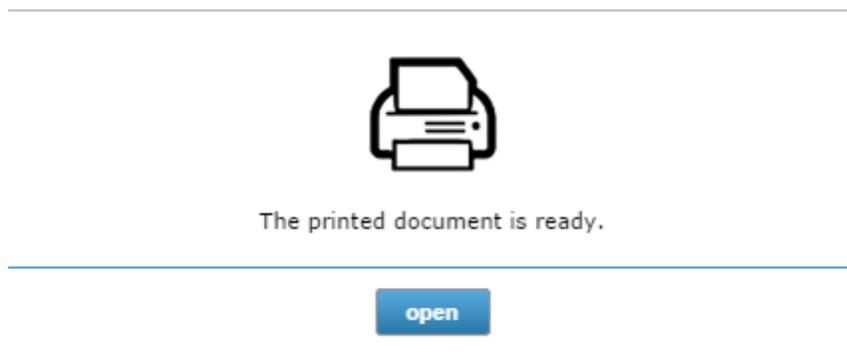
12.4.2 Remote Printer

The Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server Printer will be shown among the list of available printers.

1. Open a remote document and try to print it.



2. Select Thinfinity® Remote Desktop Server printer and press "Print".
3. A message will be presented to let you know that the document is ready to be printed.



- 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.

Read more:

- [Remote Sound](#)
- [Share Session](#)
- [Mapped Drives](#)
- [Analytics](#)

12.4.3 Remote Sound

With Thinfinity® Remote Desktop Server 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.

Read more:

- [Share Session](#)
- [Mapped Drives](#)
- [Analytics](#)

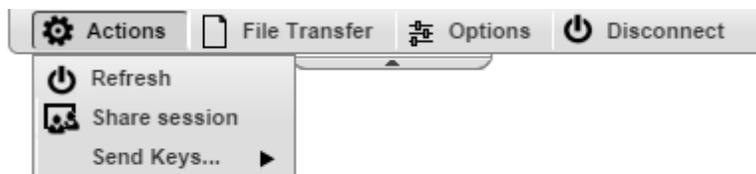
12.4.4 Share Session

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:

Password:

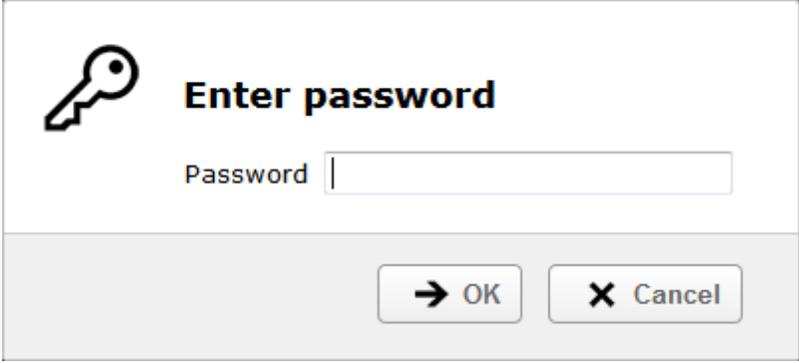
OK

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

A dialog box titled "Enter password" with a key icon on the left. It contains a text input field labeled "Password" and two buttons at the bottom: "→ OK" and "× Cancel".

 **Enter password**

Password

3. You should now be able to see and interact with the previously shared connection.

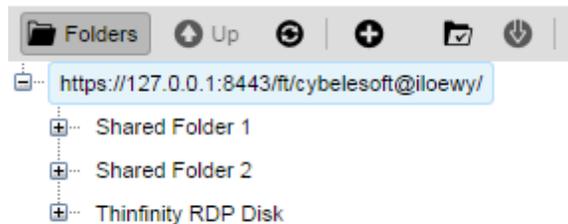
Read more:

- [Mapped Drives](#)
- [Analytics](#)

12.4.5 Mapped Drives

In order to exchange files with the remote machine, Thinfinity® Remote Desktop Server 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.



Thinfinty® Remote Desktop Server maps two kinds of directories:

Intermediate disks

The intermediate disks are directories created by Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server as an "anonymous user".

Shared Folders

The Shared Folders are network directories accessible by all Thinfinity® Remote Desktop Server 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.

Read more:

- [Analytics](#)

12.4.6 Analytics

The analytics feature allows assigned users to view historical data regarding Logins, Sessions and Connections established within Thinfinity® Remote Desktop Server 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 Thinfinity® Remote Desktop Server 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 open on a new window and find inside the "Log & Statistics" window the following tabs/options:

[Logins](#)

[Sessions](#)

[Connections](#)

[Browsers](#)

[Filter](#)

In order to use this feature, you need to install MS SQL Server. Read on to learn how to [use MS SQL Server as Backend](#).

12.4.6.1 Logins

The Logins View mode shows all the logins performed through the application within a determined period of time (default filter: Last hour).

Log & Statistics

Logins Sessions Connections Browsers Refresh

Date and Time	User	Source IP	Successful
2014-10-08 18:54:14	cybelesoft\jloewy	127.0.0.1	True
2014-10-09 14:08:27	cybelesoft\jloewy	127.0.0.1	True

Filters

View active users only

Users (comma separated):

Host name or IP address:

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

Read more:

- [Sessions](#)
- [Connections](#)
- [Browsers](#)
- [Filter](#)
- [Use MS SQL Server as Backend](#)

12.4.6.2 Sessions

The Session View mode shows all the sessions created through the application within a determined period of time (default filter: Last hour).

 **Log & Statistics**

Logins Sessions Connections Browsers Refresh

	User	Source IP	Start	End	Connections
-	cybelesoft\iloewy	127.0.0.1	2014-10-08 19:20:25	2014-10-08 19:20:33	1
	Host		Type	Start	End
		192.168.0.8:3389	rdp	2014-10-08 19:20:27	2014-10-08 19:20:33
+	cybelesoft\iloewy	127.0.0.1	2014-10-08 19:20:03	2014-10-08 19:20:14	1
+	cybelesoft\iloewy	127.0.0.1	2014-10-08 19:13:32	2014-10-08 19:17:53	1

Filters

View active users only

Users (comma separated):

Host name or IP address:

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 that the session was started from.
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.

Read more:

- [Connections](#)
- [Browsers](#)
- [Filter](#)
- [Use MS SQL Server as Backend](#)

12.4.6.3 Connections

The Connection View mode shows all the connections established in a determined period of time (default filter: Last hour).

The screenshot shows the 'Log & Statistics' interface. At the top, there are tabs for 'Logins', 'Sessions', 'Connections', and 'Browsers', with 'Connections' selected. A 'Refresh' button is located to the right of the tabs. Below the tabs is a table with the following data:

User	Source IP	Type	Host	Start	End
cybesoft\jloewy	127.0.0.1	rdp	192.168.0.8:3389	2014-10-08 19:20:27	2014-10-08 19:20:33
cybesoft\jloewy	127.0.0.1	rdp	192.168.0.8:3389	2014-10-08 19:20:08	2014-10-08 19:20:14
cybesoft\jloewy	127.0.0.1	rdp	192.168.0.8:3389	2014-10-08 19:13:37	2014-10-08 19:17:53

To the right of the table is a 'Filters' panel. It includes a checkbox for 'View active users only', a text input for 'Users (comma separated)', a text input for 'Host name or IP address', and a dropdown menu for 'Pick a date range from the list...' with 'Last 7 days' selected. An 'apply' button is at the bottom of the filters panel.

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

Read more:

- [Browsers](#)
- [Filter](#)
- [Use MS SQL Server as Backend](#)

12.4.6.4 Browsers

The Browsers View mode shows all the kinds of browsers used to access Thinfinity® Remote Desktop Server.

The screenshot shows the 'Log & Statistics' interface with the 'Browsers' tab selected. The table below shows the data displayed in the interface:

User Agent	Sessions
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.124 Safari/537.36	3

The filters panel on the right includes the following options:

- View active users only
- Users (comma separated):
- Host name or IP address:
- Pick a date range from the list...: Last 7 days
-

This is the information shown on the Browsers table:

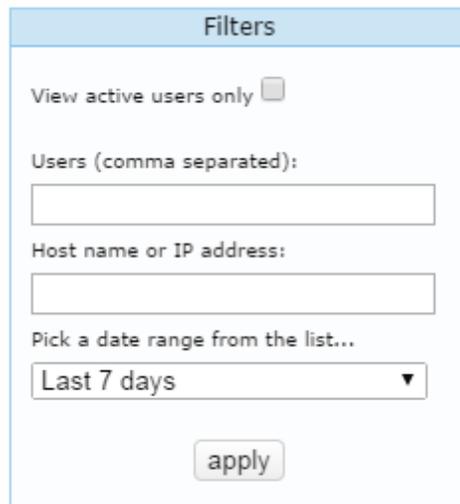
User Agent	Browser User Agent.
Sessions	Counter of Sessions established within the Same Browser User Agent kind.

Read more:

- [Filter](#)
- [Use MS SQL Server as Backend](#)

12.4.6.5 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.

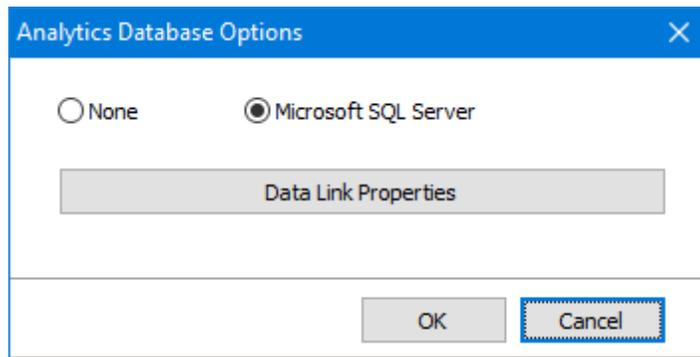
Read more:

- [Use MS SQL Server as Backend](#)

12.4.6.6 Configuring MS SQL Server

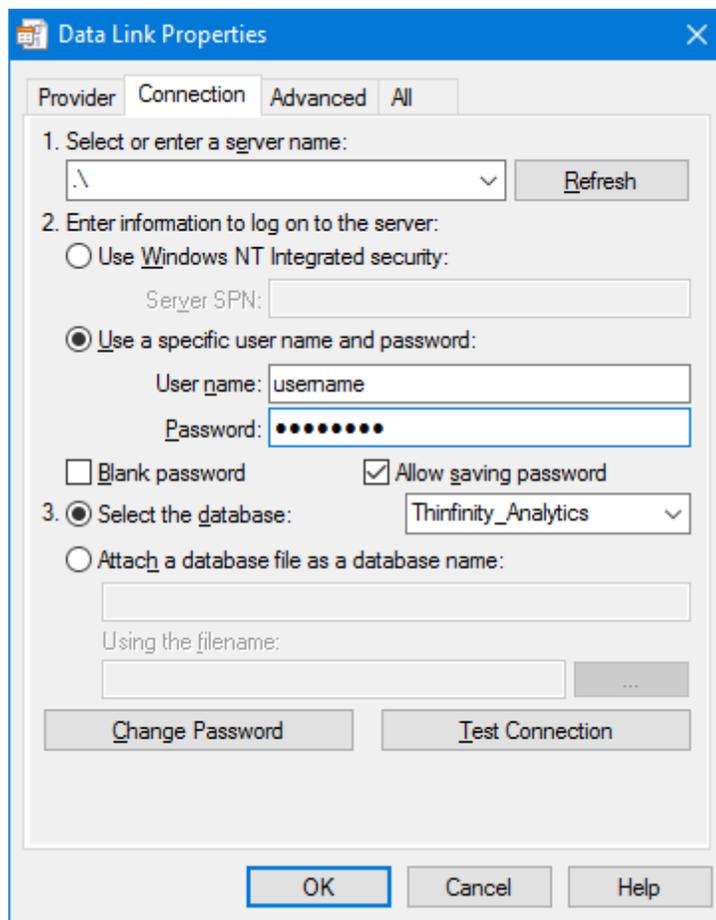
These are the requisites for Thinfinity® Remote Desktop Server Analytics to use MS SQL Server:

1. An MS SQL Server 2005 (or higher) installation that is accessible from the machine running Thinfinity® Remote Desktop Server.
2. Create a blank database with permissions to Create/Modify tables and Read/Insert/Update data.
3. Go to the '[Permissions](#)' tab in the Thinfinity® Remote Desktop Server Manager, and press the 'Configure Analytics' button:

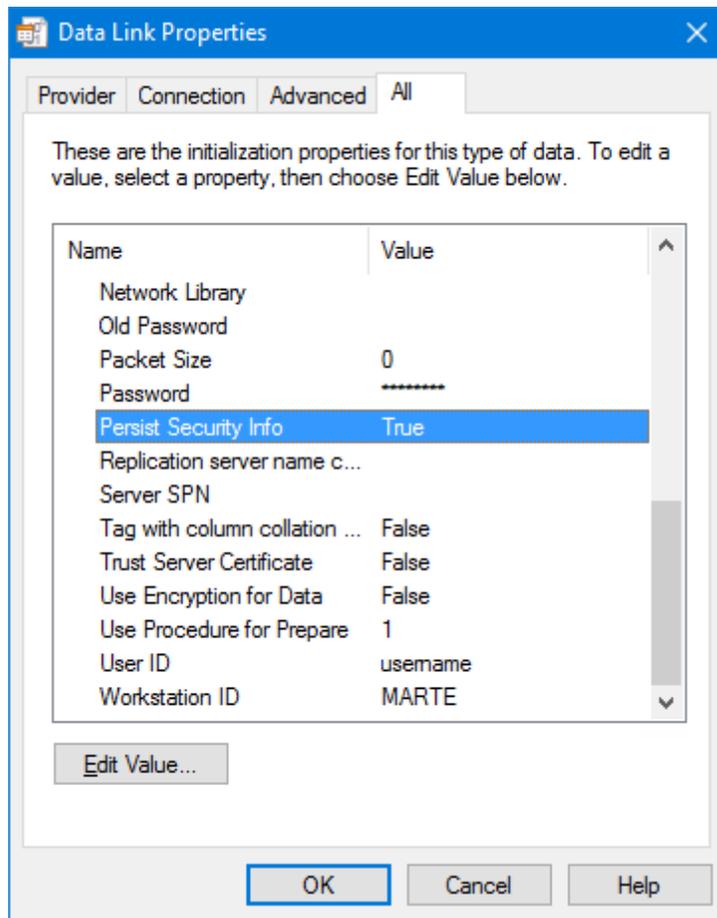


Choose 'Microsoft SQL Server'.

4. Access the Microsoft SQL Server Data Link Properties and configure the connection:



- 4.1 Enter the server name and complete the information to log in to the server.
 - 4.2 Uncheck the 'Blank password' field and check the 'Allow saving password' field.
 - 4.3 Select the database created in step 2.
5. Go to the 'All' tab:



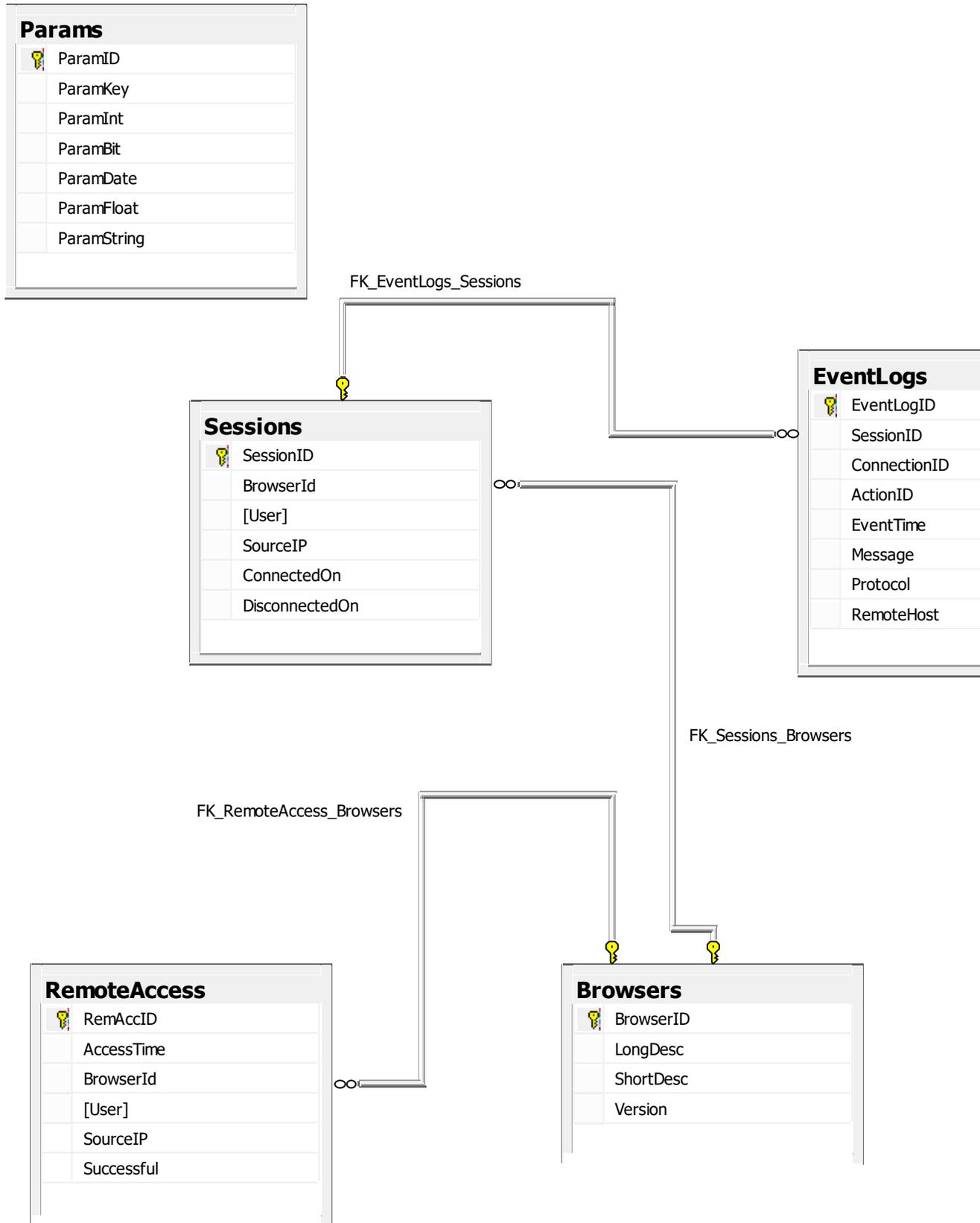
- 5.1 Set the 'Persist Security Info' property to 'True'.
- 5.2 Type the password in the 'Password' field.

Read more:

- [Analytics tables references](#)

12.4.6.6.1 Analytics Tables Reference

Analytics tables



Note: The Analytics tables are automatically created when using the product or through the migration utility.

Main Tables

RemoteAccess Table: Registers the information relevant to the Thinfinity® Remote Desktop Server user access.

Field	Description
RemAcclID	Auto increment field. Unique ID
AccessTime	The moment when the user accessed Thinfinity® Remote Desktop Server.
BrowserID	Reference to the browser the user accessed with, shown in the Browser table.
[User]	Username.
SourceIP	IP address that the user logged in from.
SuccessFul	1 = successful login, 0 = Error

Thinfinity® Remote Desktop Server session information

The Thinfinity® Remote Desktop Server session information is stored in two tables with a master/detail relationship.

Sessions Table: Each time a user access a remote server through Thinfinity® Remote Desktop Server an entry in the Sessions table is generated. This entry is updated with the disconnection date when the session ends (by closing the tab or browser).

Field	Description
SessionID	Auto increment field. Unique session ID.
BrowserID	Reference to Browsers table indicating which browser did the user start the session with.
[User]	Thinfinity® Remote Desktop Server logged in username.
ConnectedOn	Date/time of session start.
DisconnectedOn	Date/time of session end. If this field has a 'Null' value it means the session is still open.

EventLogs Table: In this table an entry is generated for each event related to the session referenced by the SessionID field.

Field	Description
EventLogID	Auto increment field. Unique ID.
SessionID	Reference to Sessions.SessionID. Shows the session the event belongs to.
ConnectionID	Always 0 for Thinfinity® Remote Desktop Server.
ActionID	Reference to Actions.ActionID. Shows the action of the event.
EventTime	Date/time of the event.
Message	Event message.
Protocol	Protocol. Such as: UDP, etc.
RemoteHost	Remote host, when available.

Auxiliary Tables

Actions: Fixed list container for actions referenced by the ActionID column in the EventLogs table.

Field	Description
ActionID	Action ID.
Description	Action description.

Browsers: Has a unique list of browsers detected by the product. Any reference in User Agent generates a new entry in the Browsers list. This table is references both by the RemoteAccess table and the Sessions table.

Field	Description
BrowserID	Auto increment field. Unique ID.
LongDesc	User Agent.

ShortDesc	Short description – CHROME, FIREFOX, etc.
Version	Not used for the moment.

12.5 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.

