

v7.0 Thinfinity® Remote Workspace

Thinfinity® Remote Workspace

Administrator's Guide

What is Thinfinity® Remote Workspace?

It's the first integrated solution to virtualize your applications, desktops, data, and access any host from a unified portal. Thinfinity® Remote Workspace delivers remote and virtual desktops to any device with an HTML5 Browser anywhere.

Technology details:

The application takes advantage of the HTML5 technology and interoperates with almost every platform and browser.

Thinfinity® Remote Workspace does not require Java, ActiveX, or any other setup on the end-user side and can be used from almost any device.

Furthermore, Thinfinity® Remote Workspace 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 Workspace's cross-browser, cross-platform capability, Windows, Mac OS X, Linux, Android, and iOS users can remote login into Windows desktops and work with single applications through their favorite browser. The application supports Edge, Firefox, Chrome, Safari, and other HTML5 capable web browsers.

About This Document

In this help file you will find information about Thinfinity® Remote Workspace. This document is intended for administrators to set up and configure Thinfinity® Remote Workspace.

Check the [Getting Started](#) section and follow the instructions to quickly install and configure Thinfinity® Remote Workspace.

Look into the [Advanced Settings](#) section to learn how you can better take advantage of the many features Thinfinity® Remote Workspace 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 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> ↗

Introduction

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

Why Thinfinity® Remote Workspace®?

- 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.
- 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.
- In a Local Area Network (LAN), Thinfinity® Remote Workspace 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 Workspace 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 Workspace 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 Workspace'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 Google Chrome, Mozilla Firefox, Safari, Opera, Microsoft Edge and other HTML5 capable web browsers.

What's new in Thinfinity® Remote Workspace

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

New in Thinfinity® Remote Workspace:

- [Multi-Monitor](#)
- [VDI Manager](#)
- [Resource Reservation](#)
- [H264 support for GPU applications and video rendering](#)
- [Authentication against a Remote Active Directory \(RemoteAD\)](#)
- [Bidirectional audio redirection](#)
- [Direct file transfer \(WebBridge\)](#)
- [Secondary broker \(Pool of resources\)](#)
- [USB redirection](#)
- [Advanced Web Features \(Tree View, Listing Options, Search Bar\)](#)
- [Native iPad Application](#)
- [Thinfinitiy® RemoteAD API](#)
- [Thinfinitiy® REST API](#)
- [Web VPN Profiles](#)
- [Web Folder Profiles](#)

And all the features from previous versions of Thinfinity® Remote Workspace:

- Added support for VNC/RFB connections. [Read more](#)
- Added support for Telnet/SSH connections. [Read more](#)
- Integrated protection measures for DOS attacks
- Multiple port listening for both HTTP and HTTPS redirection
- Support for Microsoft® RemoteFX™, enabling a 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 Workspace 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 Workspace authentication with the RADIUS system. [Read more](#)
- Populate Microsoft RD Web Access remote apps and desktops. [Read more](#)
- Customize the Thinfinity® Remote Workspace 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](#)
- Added support for native TOTP. [Read more](#)
- Support for OpenID Connect protocol
- Support for DUO 2FA. [Read more](#)
- Support for ForgeRock OAuth
- User-based Access Profiles. [Read more](#)
- User-based Credentials Management. [Read more](#)

Architecture

Thinfinity® Remote Workspace is composed of:

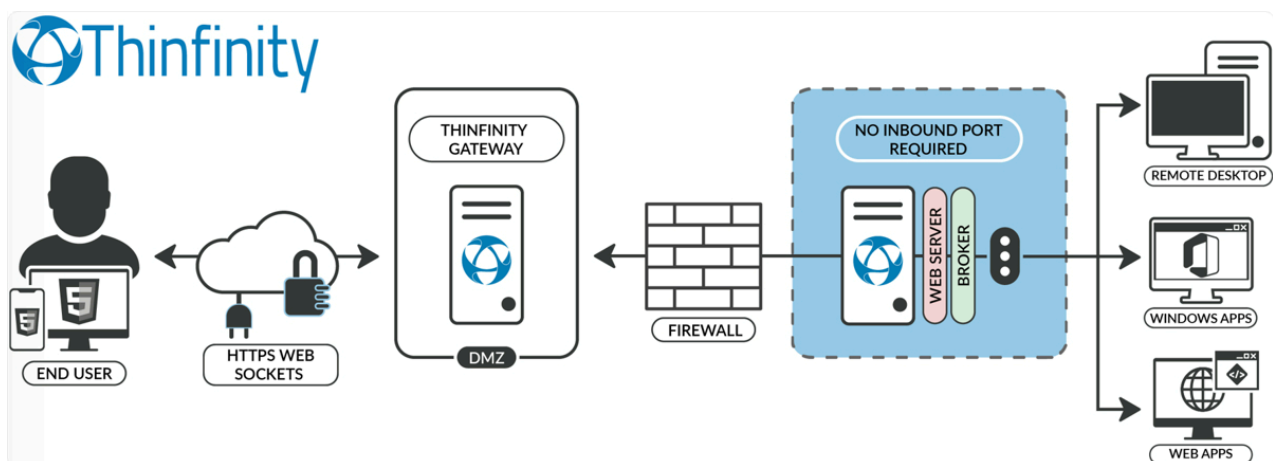
- A Server Machine running Thinfinity® Remote Workspace
- Thinfinity® Remote Workspace Web Client (*which loads on an HTML5 browser*)

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

When the end-user accesses the Thinfinity® Remote Workspace main page and enters the appropriate connection parameters, the Thinfinity® Remote Workspace Web Client communicates with the server, using WebSocket to start the connection to the remote-end.

If the connection fails to start using WebSocket, then Ajax will be used instead. This connection protocol is deprecated and will not be supported in future versions.

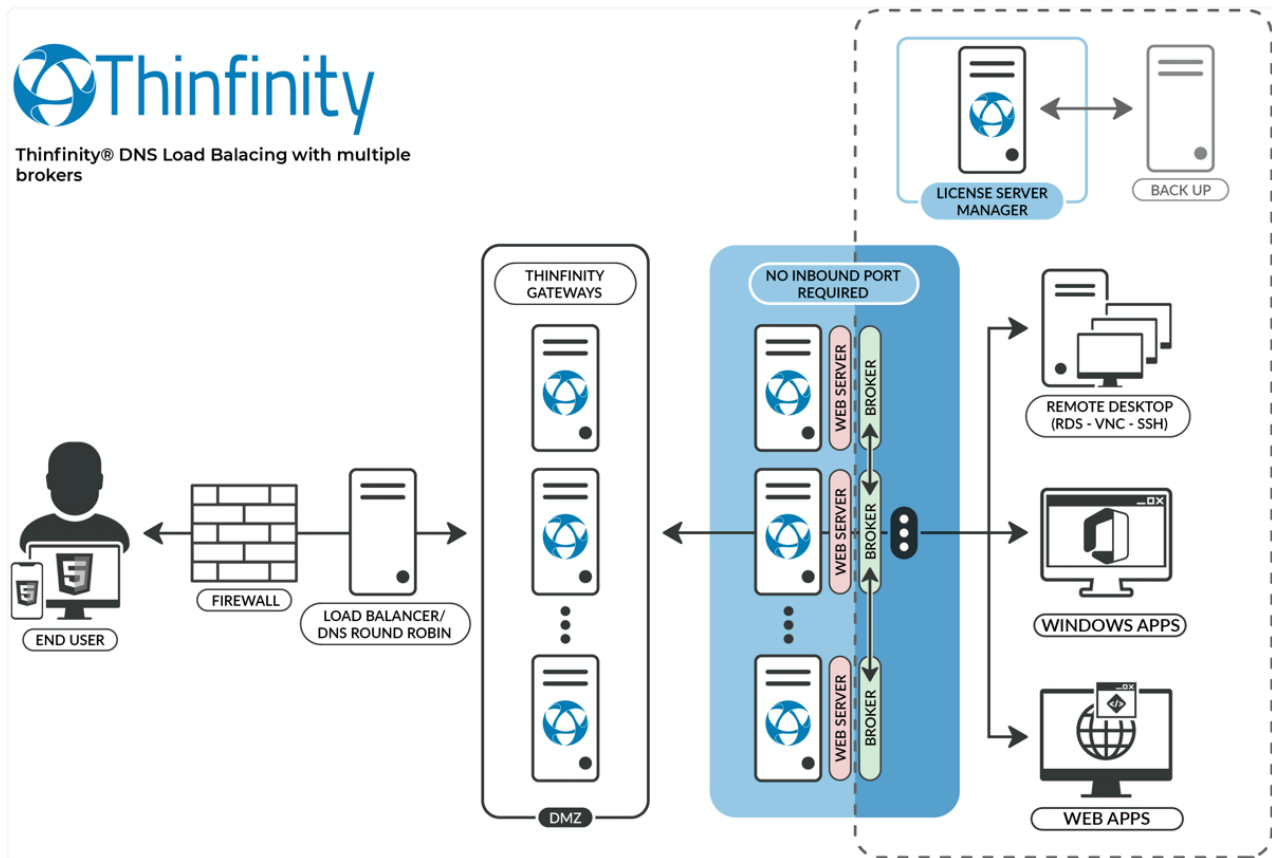
Once the connection is established, the server will receive RDP commands, optimize them for the web, and send the resulting data stream to the Thinfinity® Remote Workspace Web Client.



Load Balancing Architectures for Thinfinity® Remote Workspace:

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

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



[Read more about load balancing](#)

Requirements:

Using Thinfinity® Remote Workspace, 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
- Mozilla Firefox 17+
- Google Chrome 22+
- Safari 6.0.1+

- iOS 5.1.1+
- Android 2.3, 4.0+
- Microsoft Edge 38+

Server Machine

- Windows 11 Pro or Enterprise
- Windows 10 Pro or Enterprise
- Windows Server 2012 and 2012 R2
- Windows Server 2016
- Windows Server 2019

Security

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

Secure connections

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

Authentication levels

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

Getting Started Section

Getting Started

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

- [Installing Thinfinity® Remote Workspace](#)
- [Customizing Thinfinity® Remote Workspace](#)
- [After Customization](#)
- [Supported RDP shortcut keys](#)

Find a more exhaustive reference of the available options here:

- [Advanced Settings](#)
- [Managing the SSL Certificate](#)
- [Mobile devices](#)
- [Integrating Thinfinity® Remote Workspace](#)
- [User's Guide](#)

Installing Thinfinity® Remote Workspace

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

- Download the installer from this link:

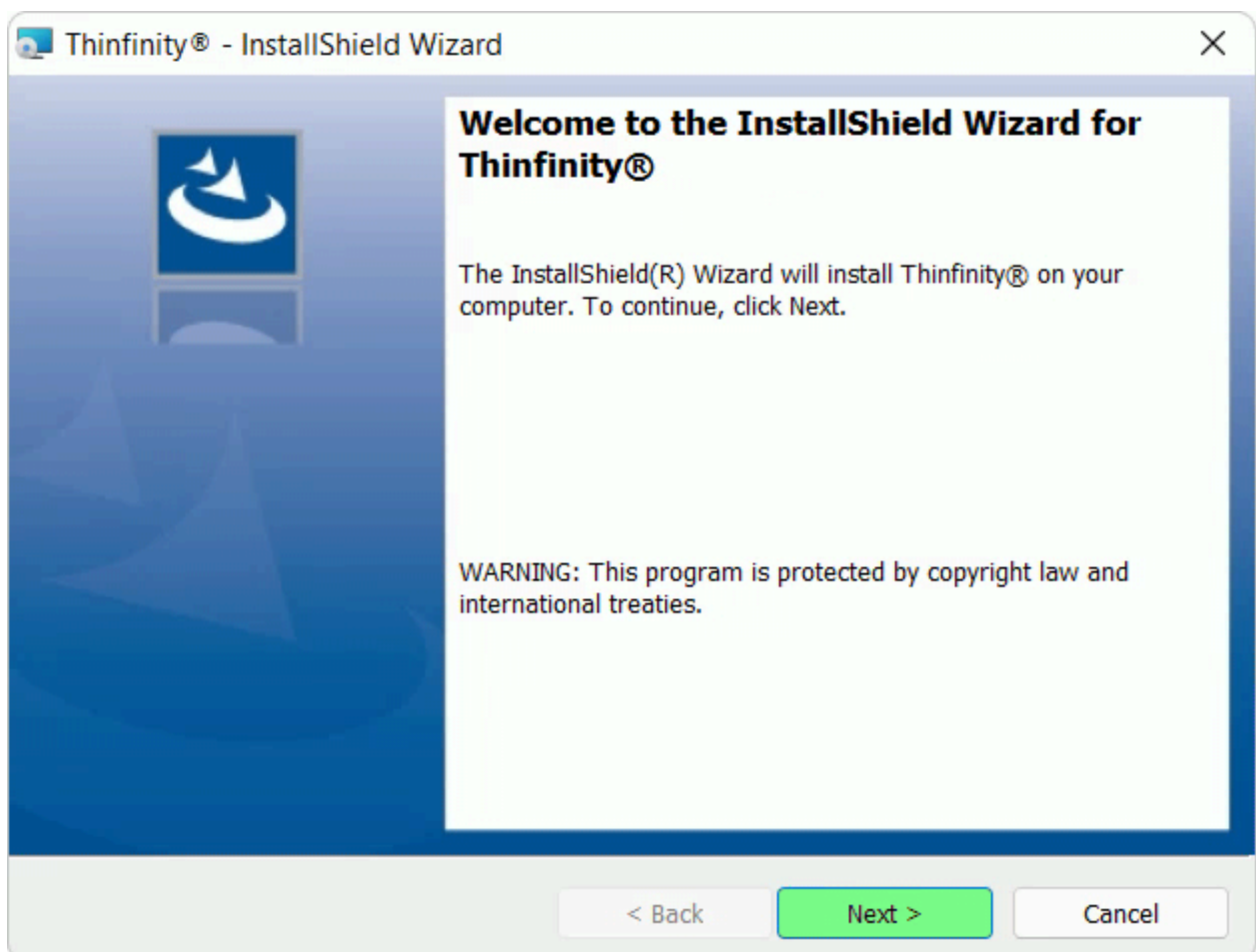


Download

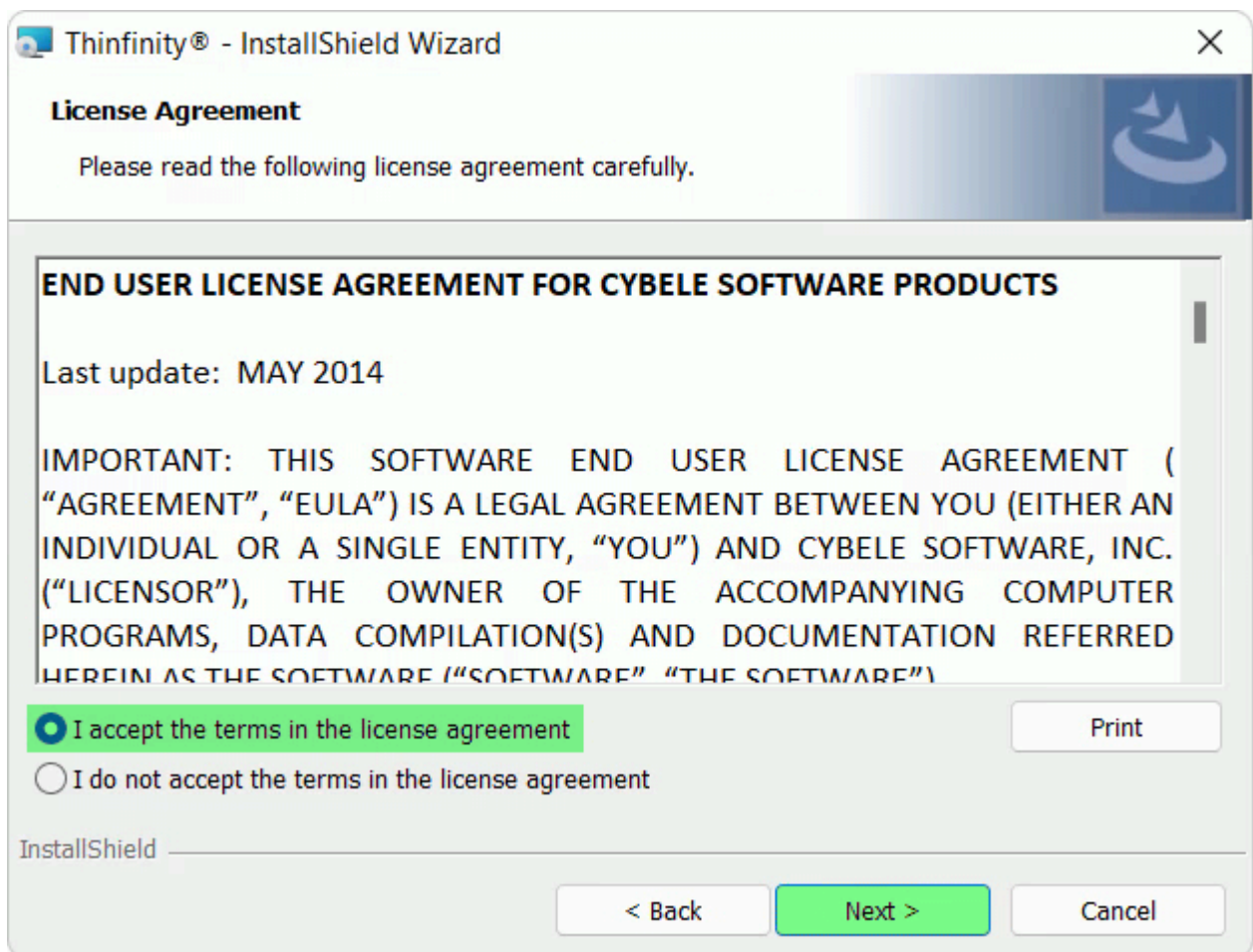
Cybele Software, Inc.



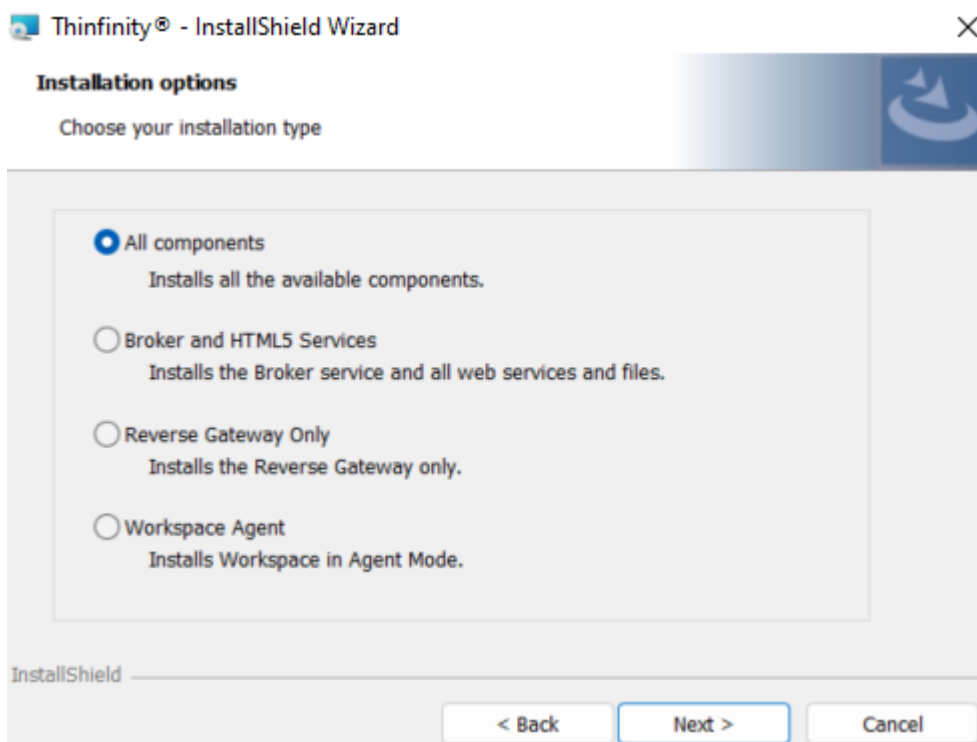
- After executing the installer on the target machine, click on 'Next':



- Check the '*I accept the terms in the license agreement*' and then click on 'Next':



- You will be presented with three installation options, choose one and hit 'Next'. For this article, the 'All components' option is selected:



All Components

Choose this option for a standalone installation. Both a Thinfinity® 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.

Broker and HTML5 Services

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

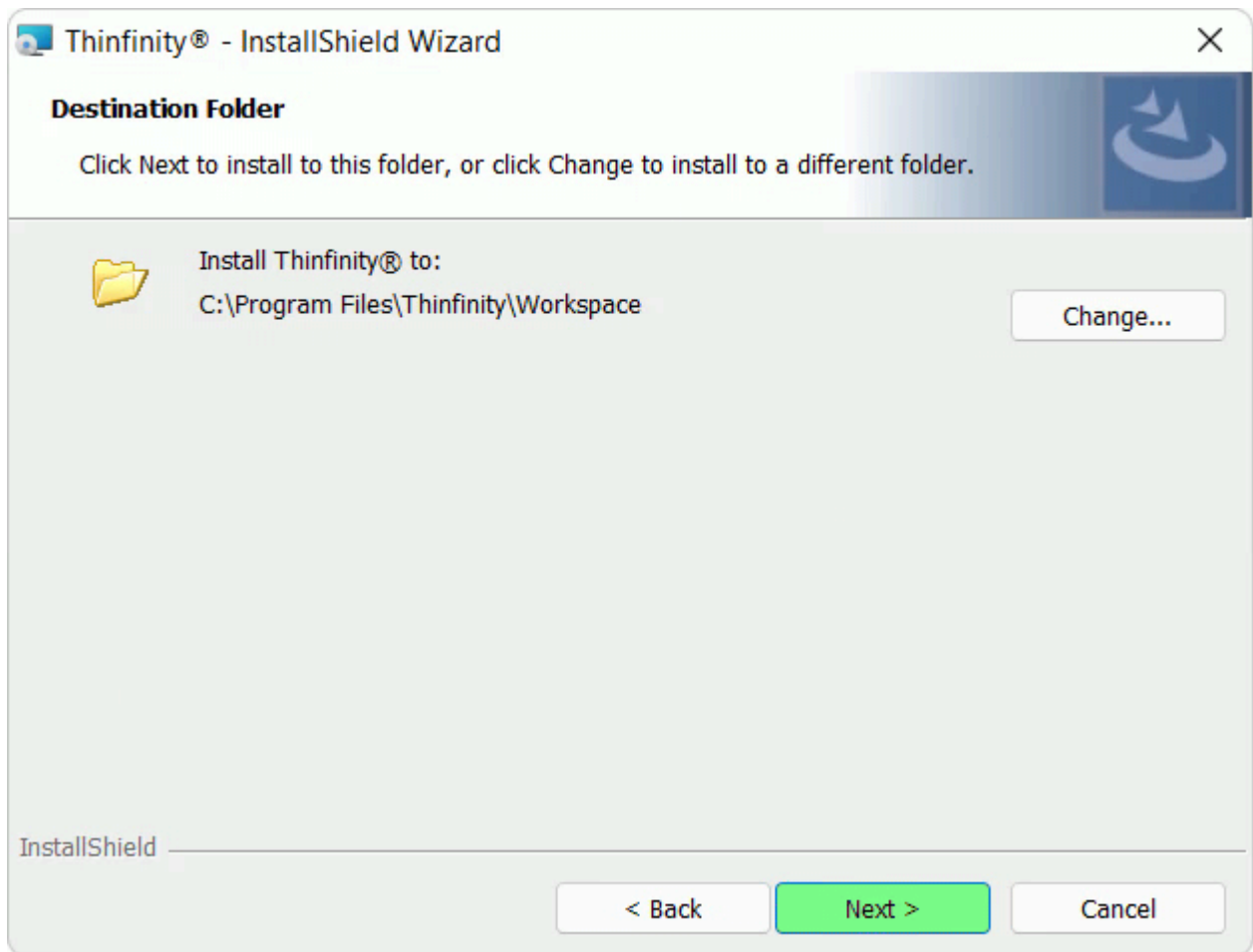
Reverse Gateway Only

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® Services installations.

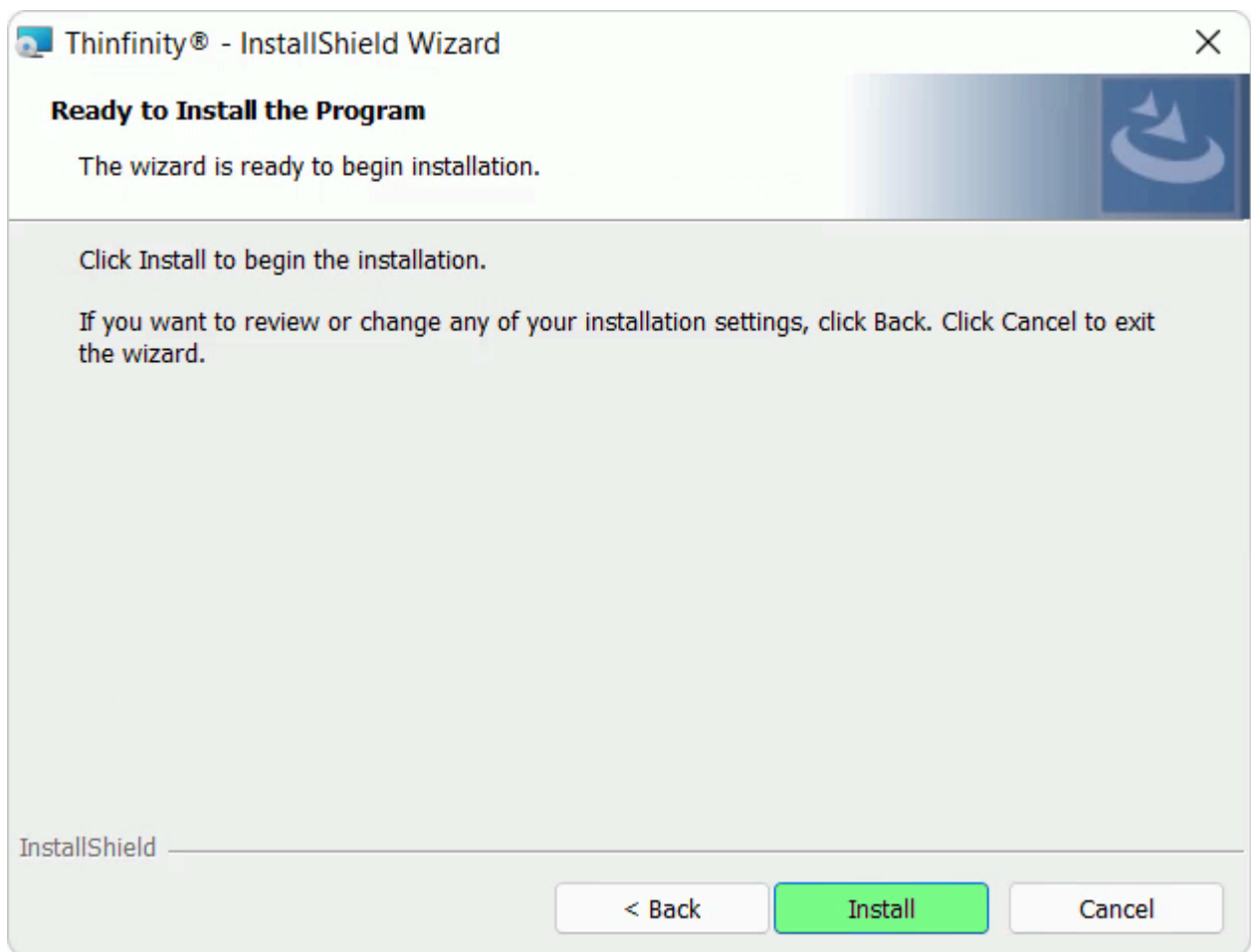
Workspace Agent

This option allows you to create an RDP connection that doesn't require opening any inbound ports.

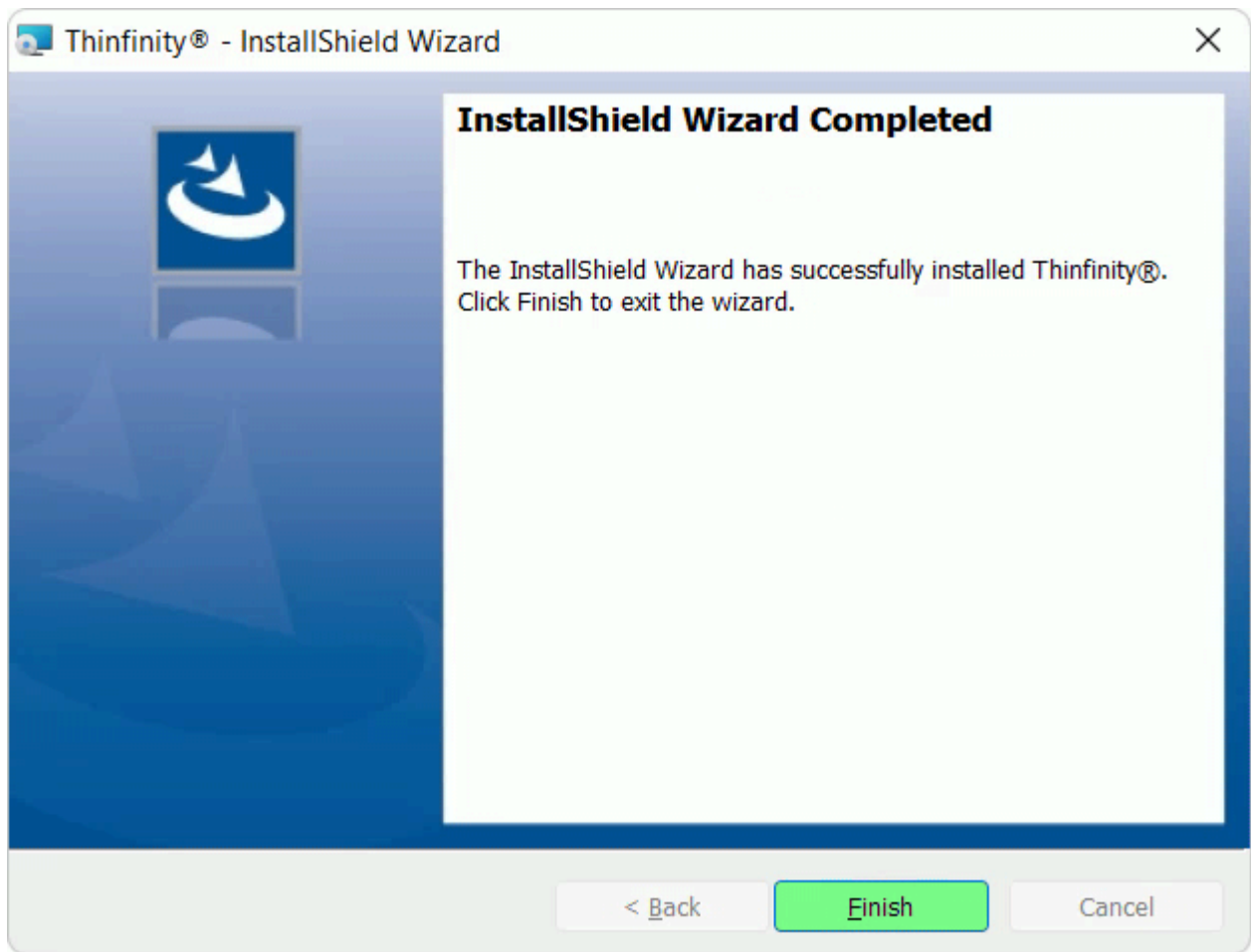
- You can change the installation path for Remote Workspace by pressing '*Change*' or you can leave it by default. Click '*Next*' afterwards:



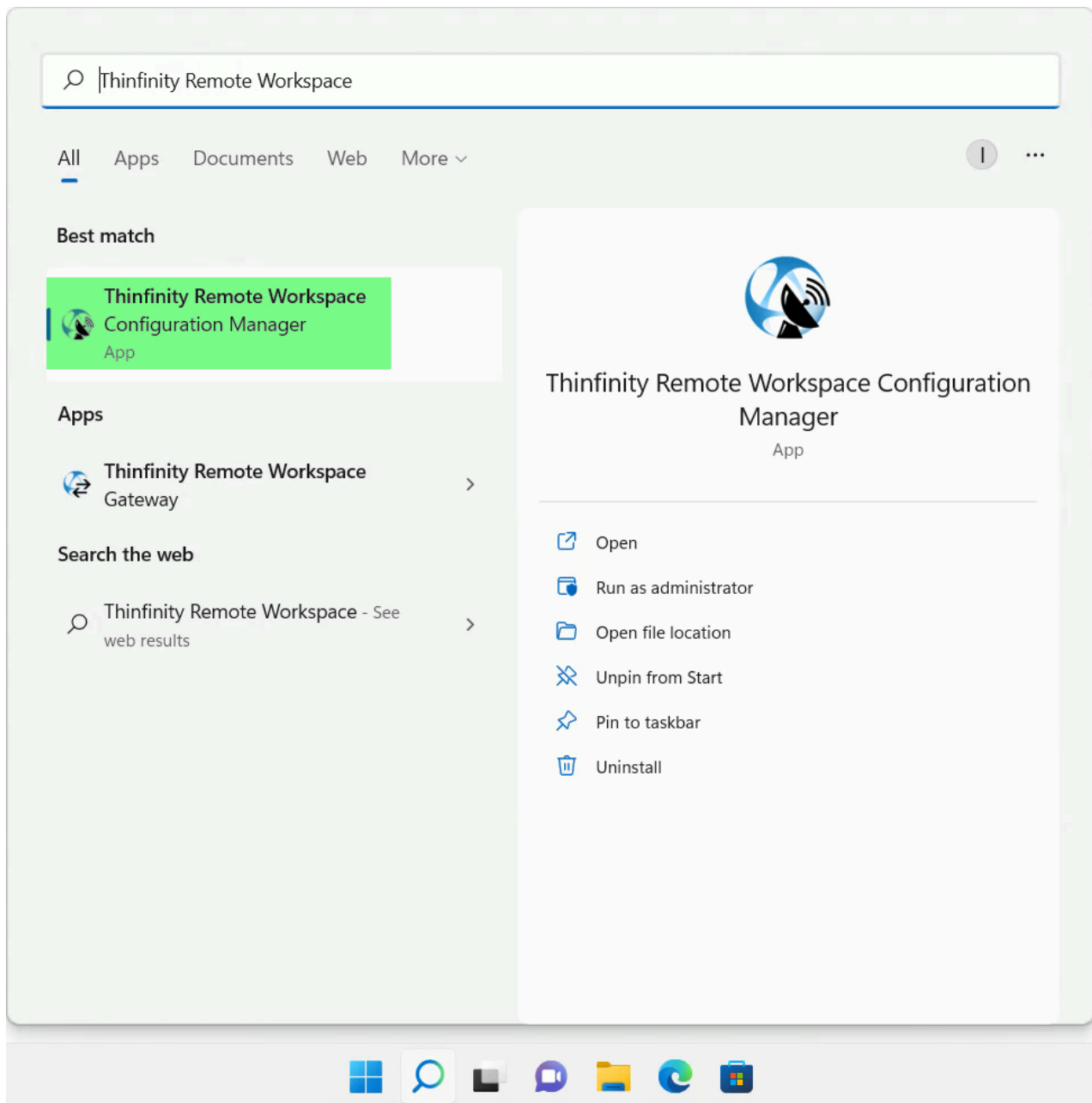
- Once all of this is done, click on '*Install*':



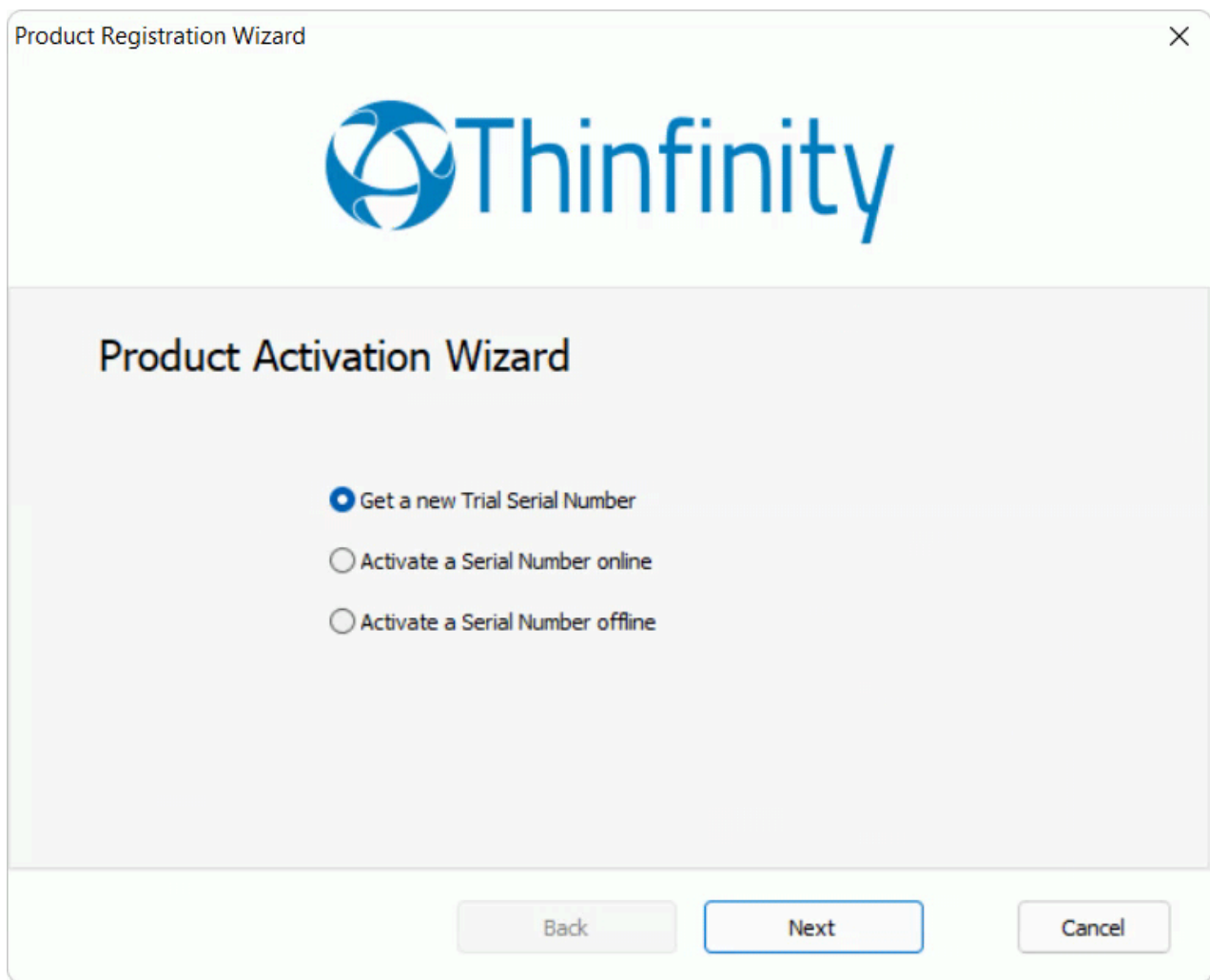
- After the installation process is done, click on '*Finish*':



- Look for the '*Thinfinitiy® Remote Workspace Configuration Manager*' on the Start Menu:



- You'll now be prompted to register Thinfinity® Remote Workspace:



You can find more information on how to register Thinfinity® Remote Workspace on the following links:



Get a new Trial Serial Number
Thinfinity® Remote Workspace



Activate a Serial Number Online
Thinfinity® Remote Workspace



Activate a Serial Number Offline
Thinfinity® Remote Workspace



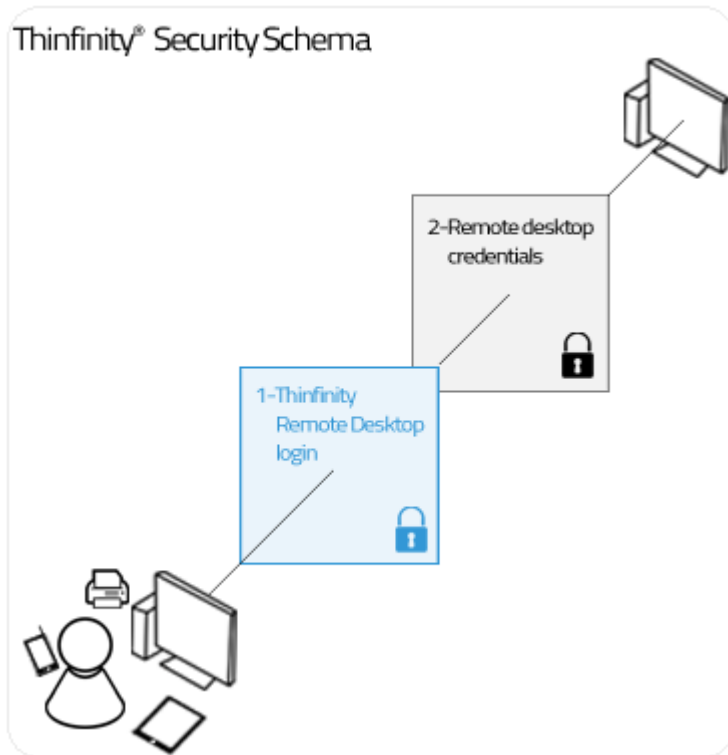
Customizing Thinfinity® Remote Workspace

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

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

Setting the Access Security Level

The application administrator can set two user access security levels:



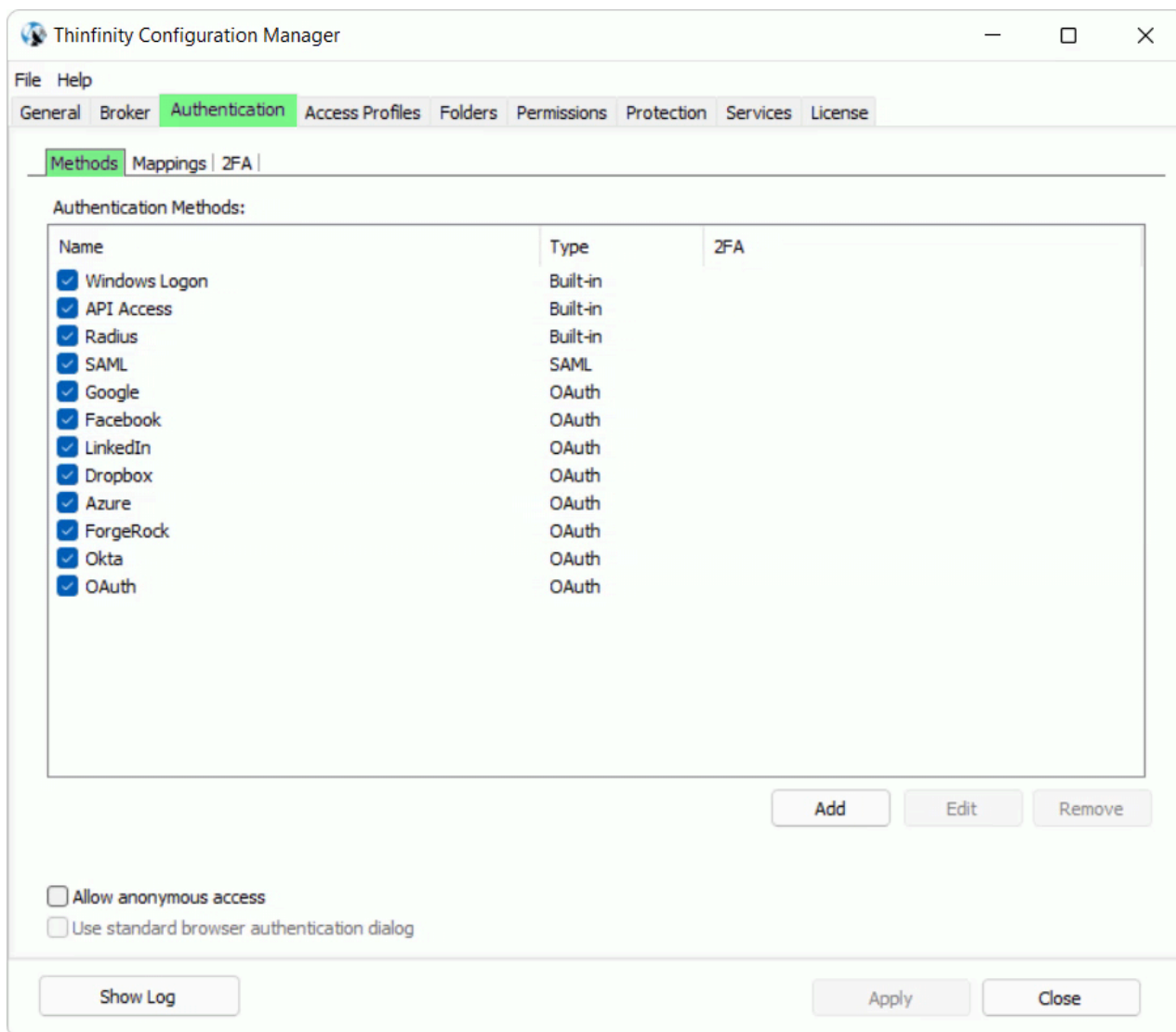
Application Login:

The first level provides access to users into the Thinfinity® Remote Workspace application.

- Thinfinity® Remote Workspace Credentials:

Once logged into the application, the users will have to provide the remote desktop credentials.

You can find this on the '*Methods*' tab under the '*Authentication*' section of the Thinfinity® Remote Workspace Configuration Manager:



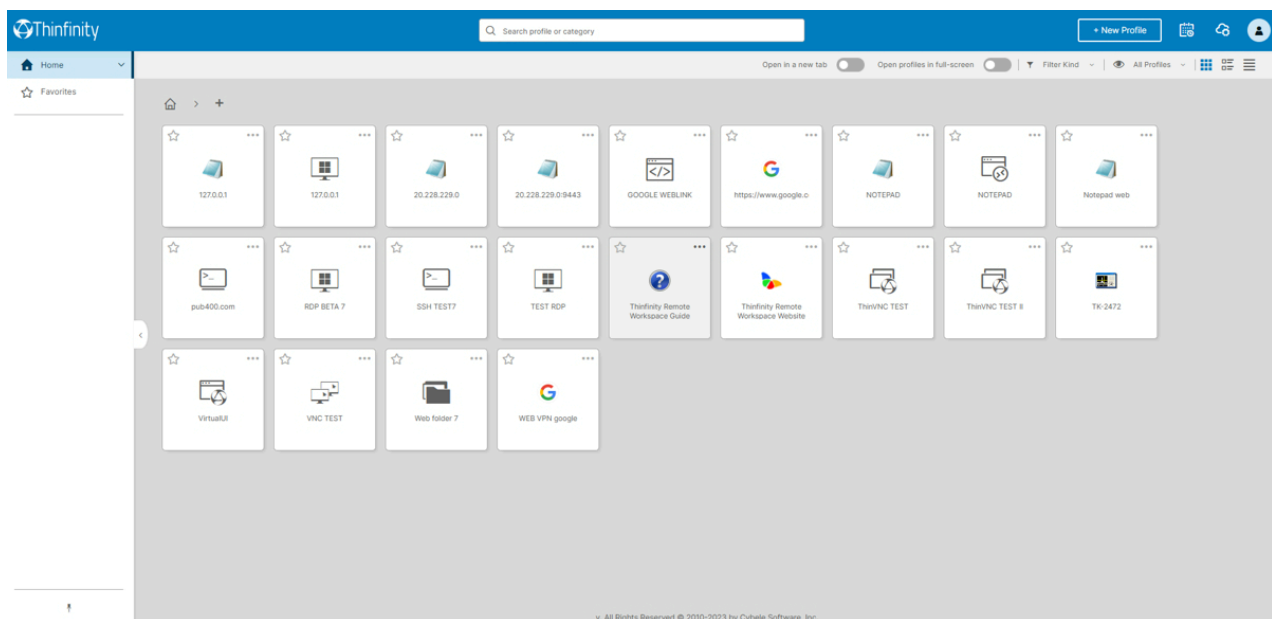
Testing Internal Access

Although Thinfinity® Remote Workspace requires no installation on 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 Workspace, 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 Workspace main web interface:



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

Configuring Internet Access

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

Test the access

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

[https://External-IP:Port ↗](https://External-IP:Port)

or

[https://Your-Domain:port ↗](https://Your-Domain:port)

Configuring the router:

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

Port Forwarding:

- Access the router by typing into a web browser the IP address for the Default Gateway
- Authenticate with the router credentials
- 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 Workspace is running on, or a different one
- Forward the internet port to the machine internal IP address where you have installed Thinfinity® Remote Workspace and the port where it's running
- Save the changes

If you need help configuring the router, contact us at [support@cybelesoft.com ↗](mailto:support@cybelesoft.com)

Mapping Remote Drives

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

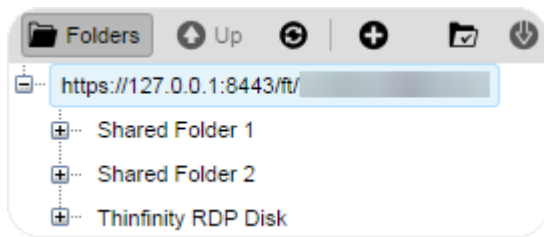
You can map remote drives using two different features:

- [Intermediate Disks](#)
- [Shared Folders](#)

Intermediate Disks

An intermediate disk is a directory created by Thinfinity® Remote Workspace to keep files that users will exchange between the remote computer and the browser. This option is only available in RDP Profiles.

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

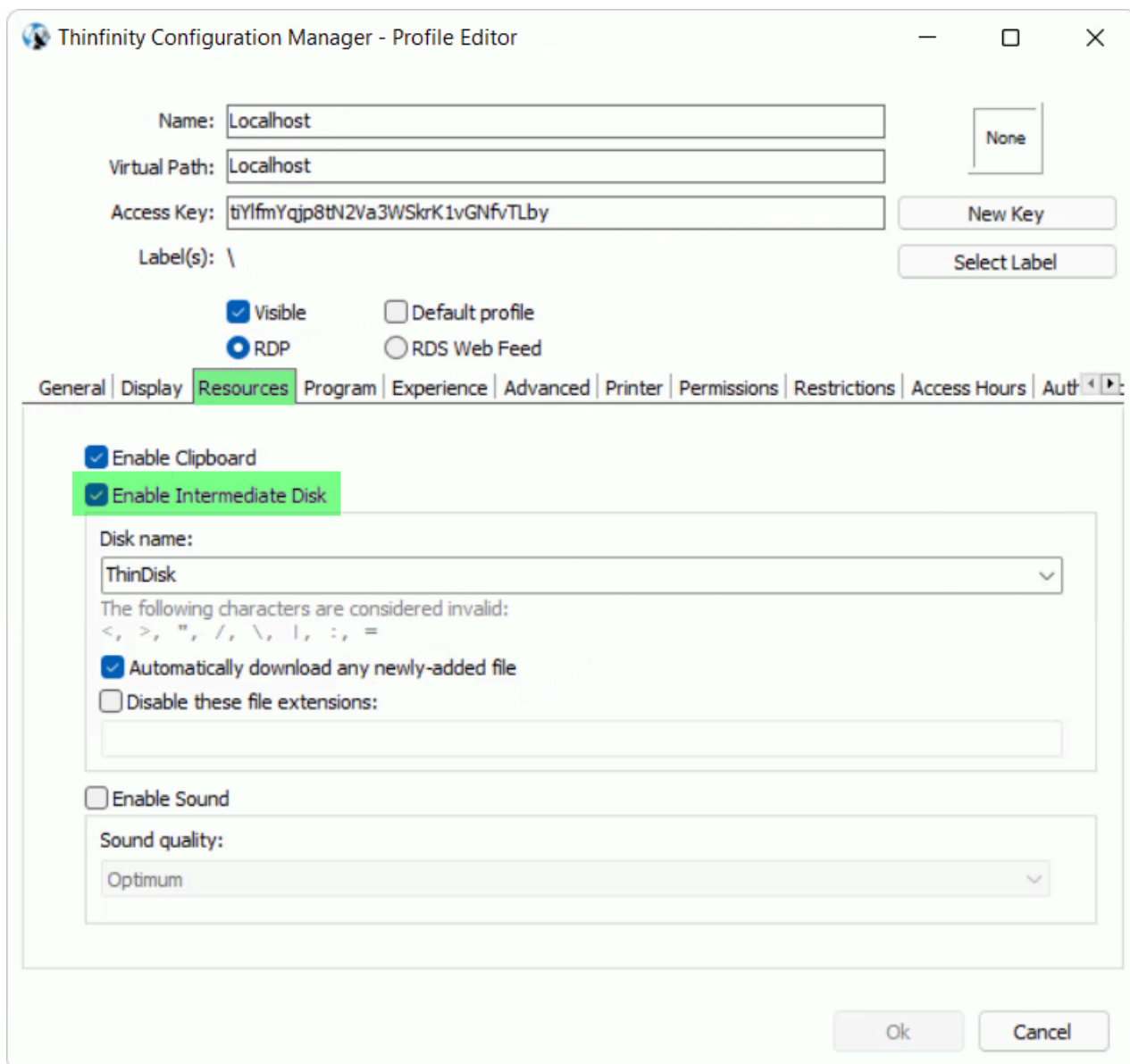


- On the remote connection on Windows Explorer, as a mapped drive.
- On the [File Transfer](#) Manager as a remote directory to exchange files with.

Configuring an Intermediate disk is very easy:

If you are using Access Profiles:

- On Thinfinity® Configuration Manager, go to the '*Access Profiles*' tab.
- Edit the RDP profile where you want to enable the intermediate disk.
- Open the '*Resources*' tab.
- Check the option '*Enable Intermediate Disk*', give a name to the disk and save the changes:



Thinfinity Configuration Manager - Profile Editor

Name: Localhost

Virtual Path: Localhost

Access Key: tiYlfmYqip8tN2Va3WSkrK1vGNfvTLby

Label(s): \

None

New Key

Select Label

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General | Display | **Resources** | Program | Experience | Advanced | Printer | Permissions | Restrictions | Access Hours | Auth

☒ Enable Clipboard

☒ Enable Intermediate Disk

Disk name:

ThinDisk

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

☒ Automatically download any newly-added file

☐ Disable these file extensions:

☐ Enable Sound


Sound quality:

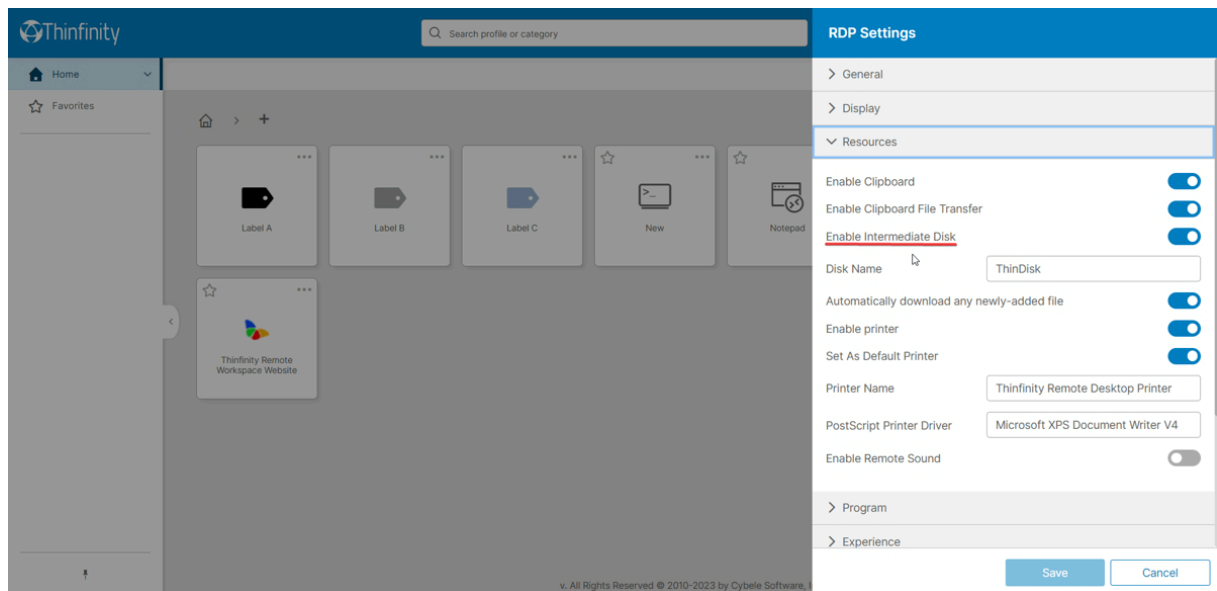
Optimum

Ok Cancel

- When you connect using this profile, look for this drive on the remote machine on Windows Explorer.

If you are using other authentication methods:

- On the Web Interface, click on the Edit button  (pen on the top-right corner of the Profile button).
- Go to the 'Resources' tab.
- Check the option 'Enable Intermediate Disk' and give a name to the disk:

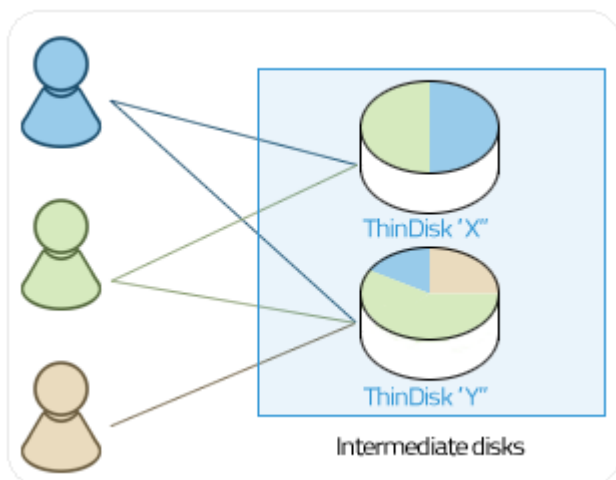


- Connect and look for the drive that was created, on the remote machine on Windows Explorer.

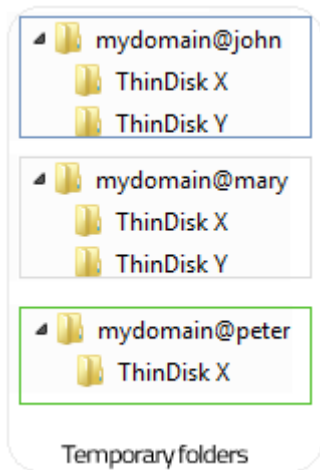
Intermediate physical files location:

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



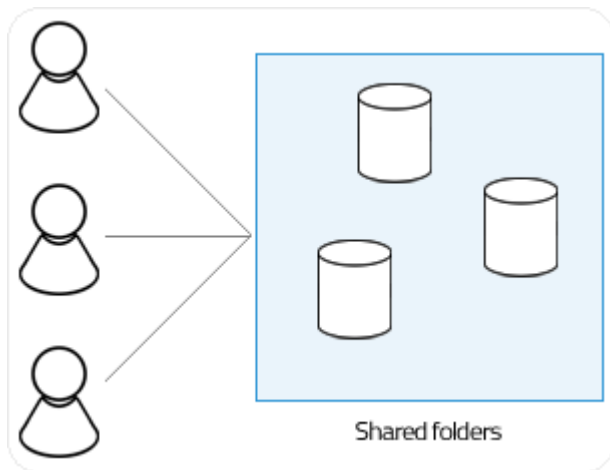
A user will have access to an intermediate disk, if he/she has access to any profile associated with this disk.

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

Shared Folders

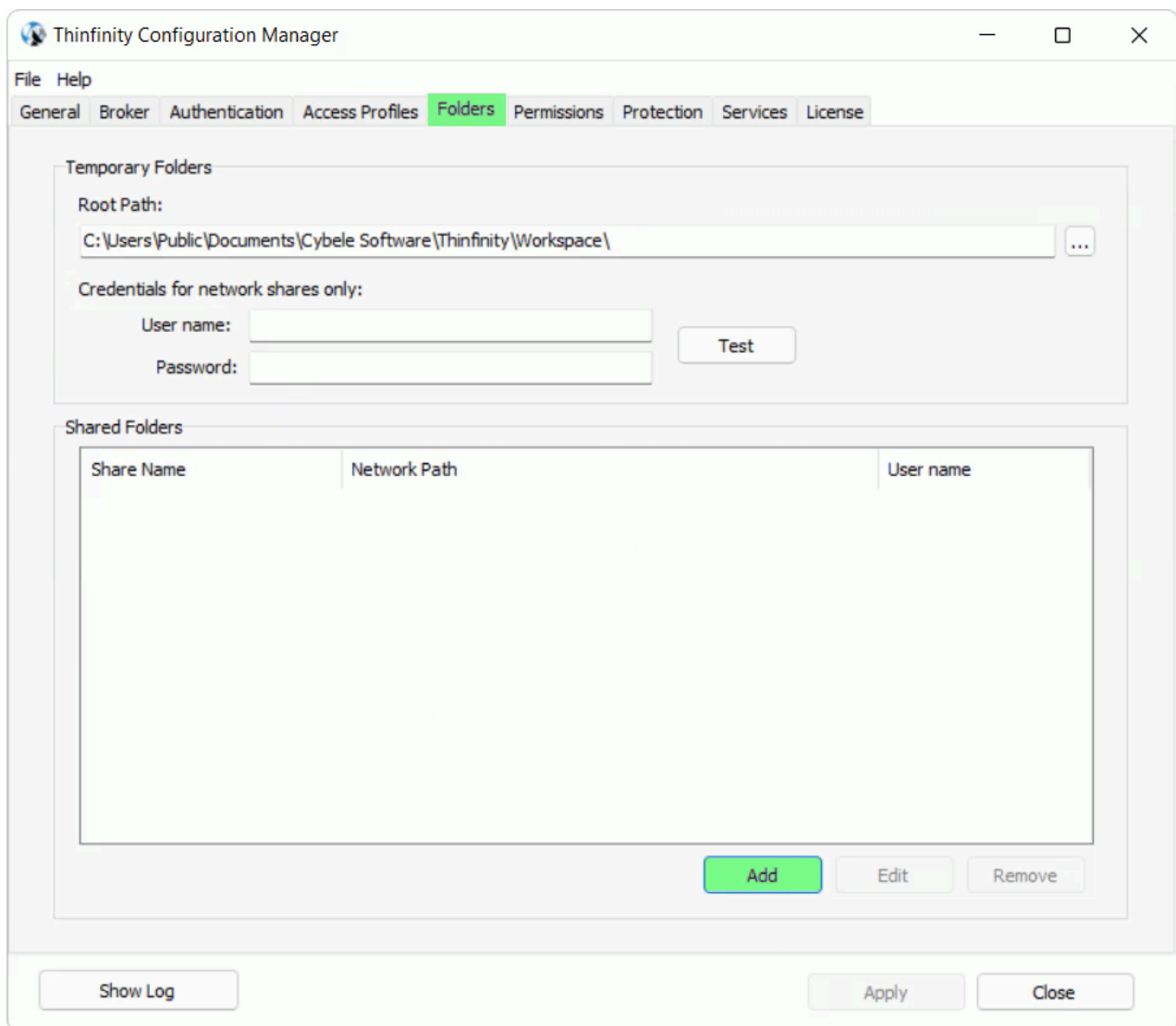
The shared folders are existing local network directories that you can map as a drive on Thinfinity® Remote Workspace remote connections.

Once set, they will be accessible from every connection and by all Thinfinity® Remote Workspace users.

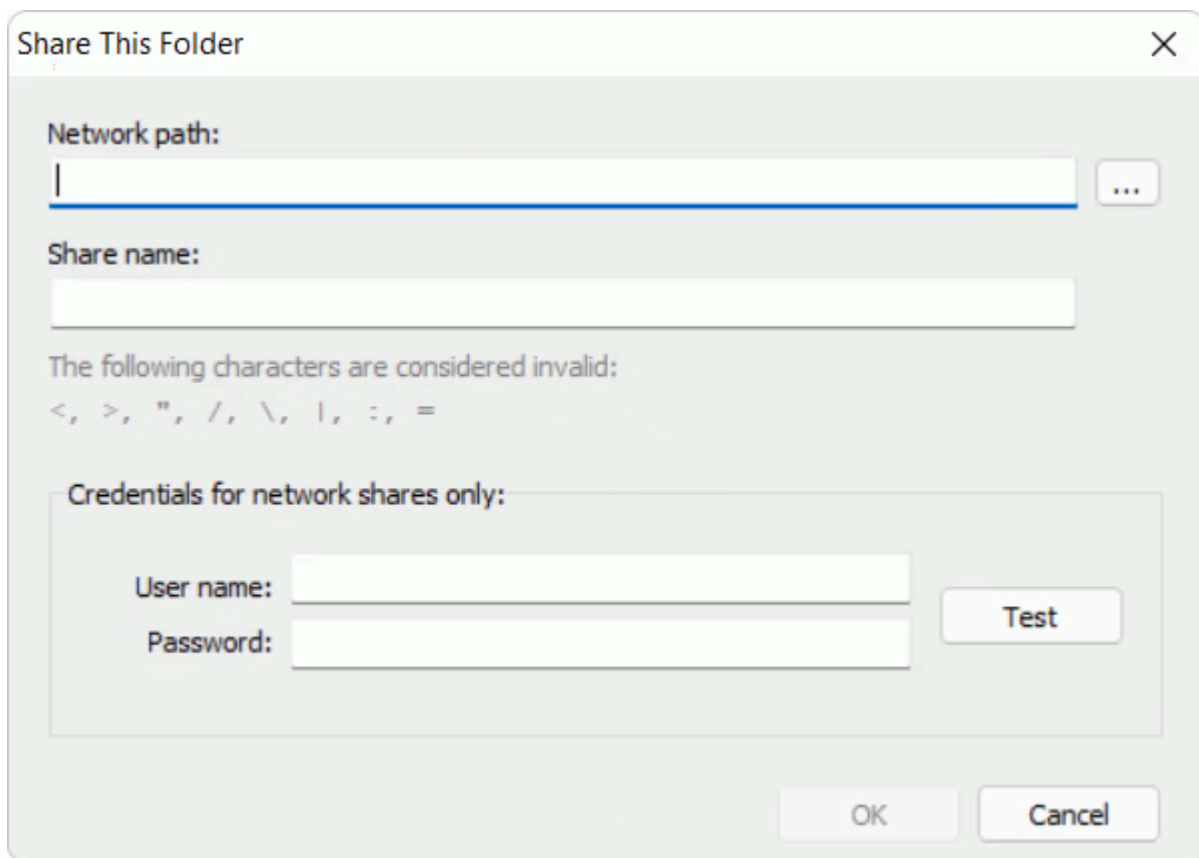


Follow these steps to configure a new Shared Folder:

- On Thinfinity® Configuration Manager open the '*Folders*' tab.
- Click on the '*Add*' button

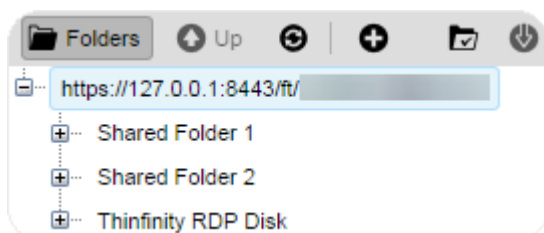


- Inform the '*Network path*' to be shared.
- On '*Share name*' enter a name to be shown on the remote mapped disks:



The 'Share This Folder' dialog box is shown. It has a title bar with a close button (X). The 'Network path:' field is empty, with a browse button (three dots) to its right. The 'Share name:' field is also empty. Below these fields, a message states: 'The following characters are considered invalid: <, >, ", /, \, |, :, ='. At the bottom of the dialog, there is a section titled 'Credentials for network shares only:' which contains 'User name:' and 'Password:' text boxes, a 'Test' button, and 'OK' and 'Cancel' buttons at the very bottom.

- Press 'OK'.
- From now on, users will find this directory as a mapped drive in every Thinfinity® Remote Workspace 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.

After Customization

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

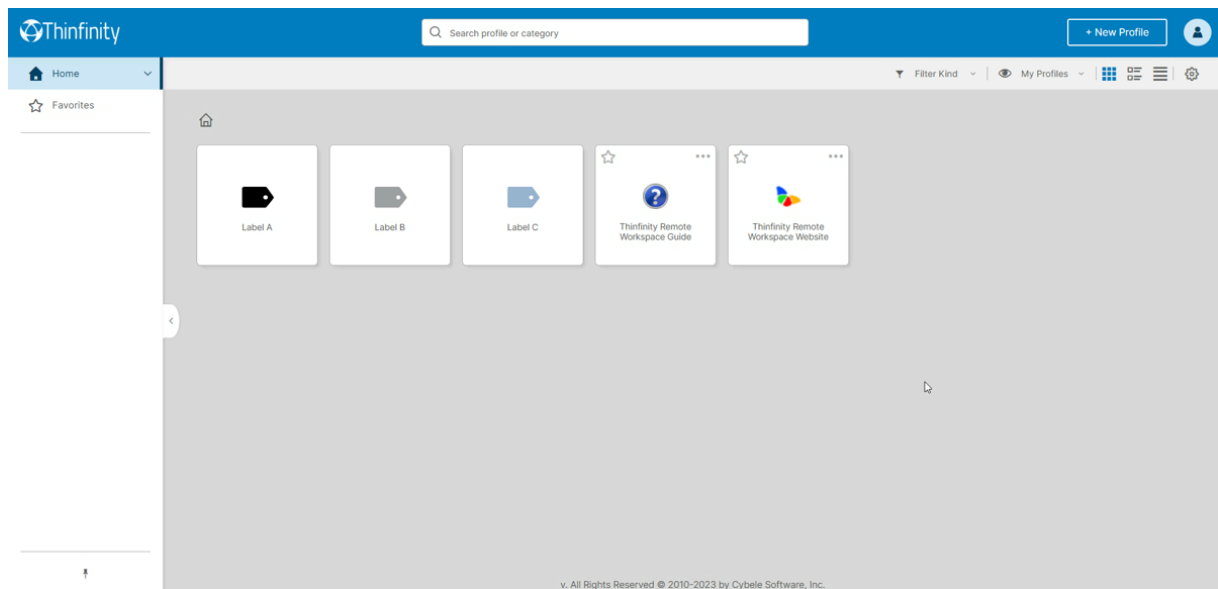
Read more:

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

Connecting to a Desktop

In order to connect to a remote desktop using Thinfinity® Remote Workspace, open a browser and type the Thinfinity® Remote Workspace URL, which is composed by <https://ServerIP:Port> ↗

- 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.
- You will be presented with the following screen:



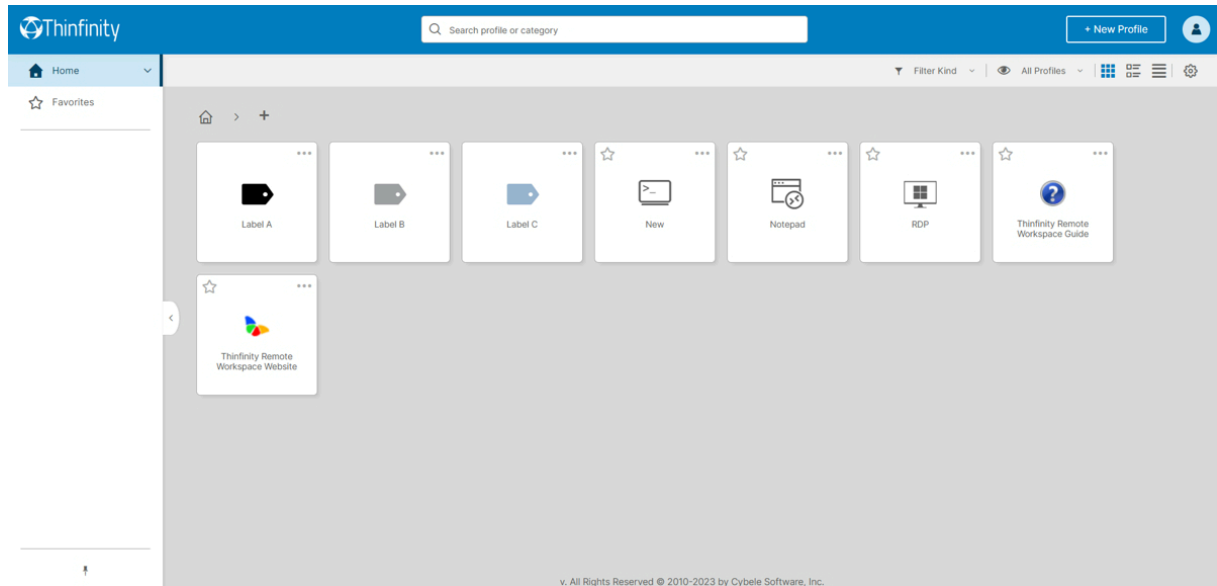
The '+' option represents the '*Any Computer*' profile: it enables the user to select the type of connection, the remote computer's IP address and credentials, and configure the connection.

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 side of the screen. Use it to switch between the '*Any Computer*' profile and the other(s).

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

Connecting to an Access Profile:

- Click on the profile you want to connect to.
- 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:



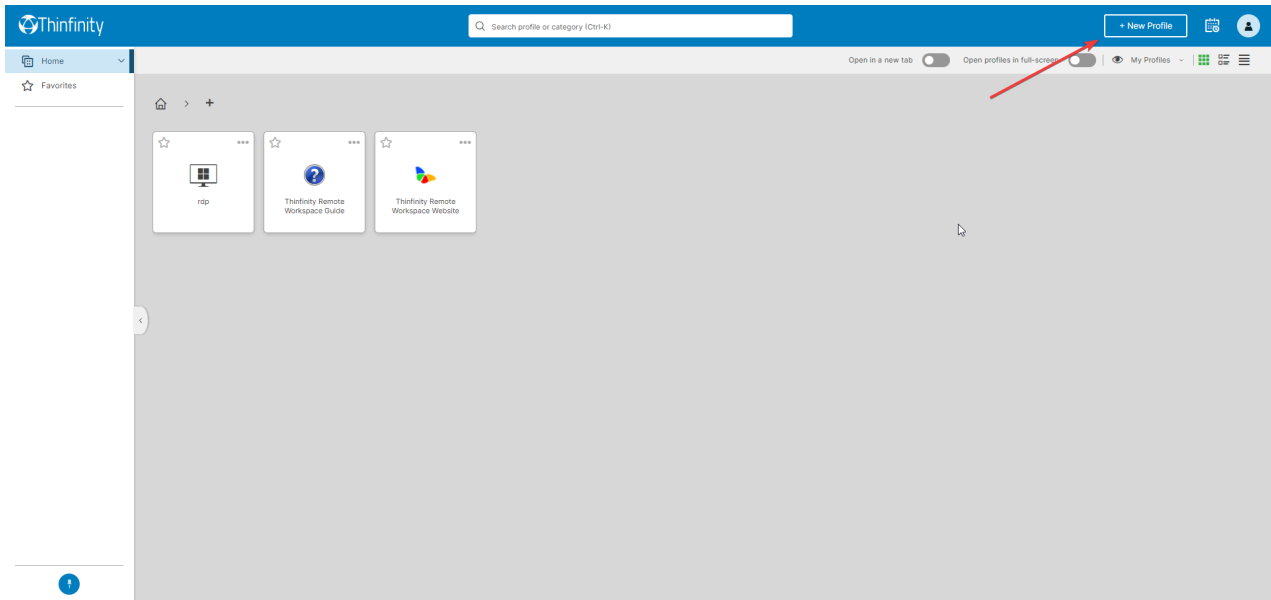
Connecting to 'Any Computer'

- 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.
- Enter the internal IP address/host name for the computer you want to access and press '*Connect*'.
- 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. You can also change the RDP options by pressing the plus [+] sign in order to show the settings tabbed interface.

Read more about each option on the [Web Interface Settings](#) section.

Connecting to an application

- First, you need to open the *landing page of Workspace* - *http(s)://ThinfinityURL:Port*
- Then click on the "New Profile" icon of the landing page

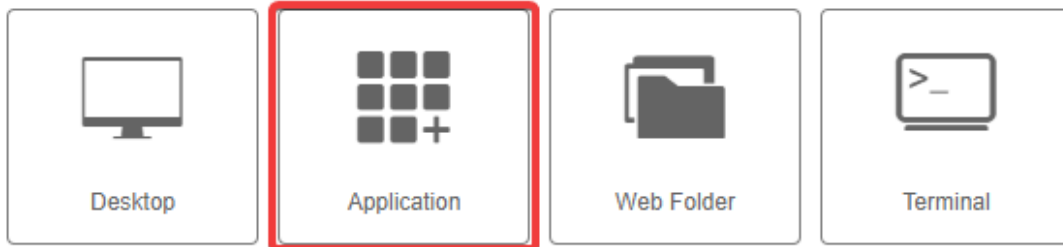


- Then select the "Application" type of connection, and click on next



Welcome! Let's create a new connection.

This wizard will help you create a new access profile. Please choose the type of connection you want to create.

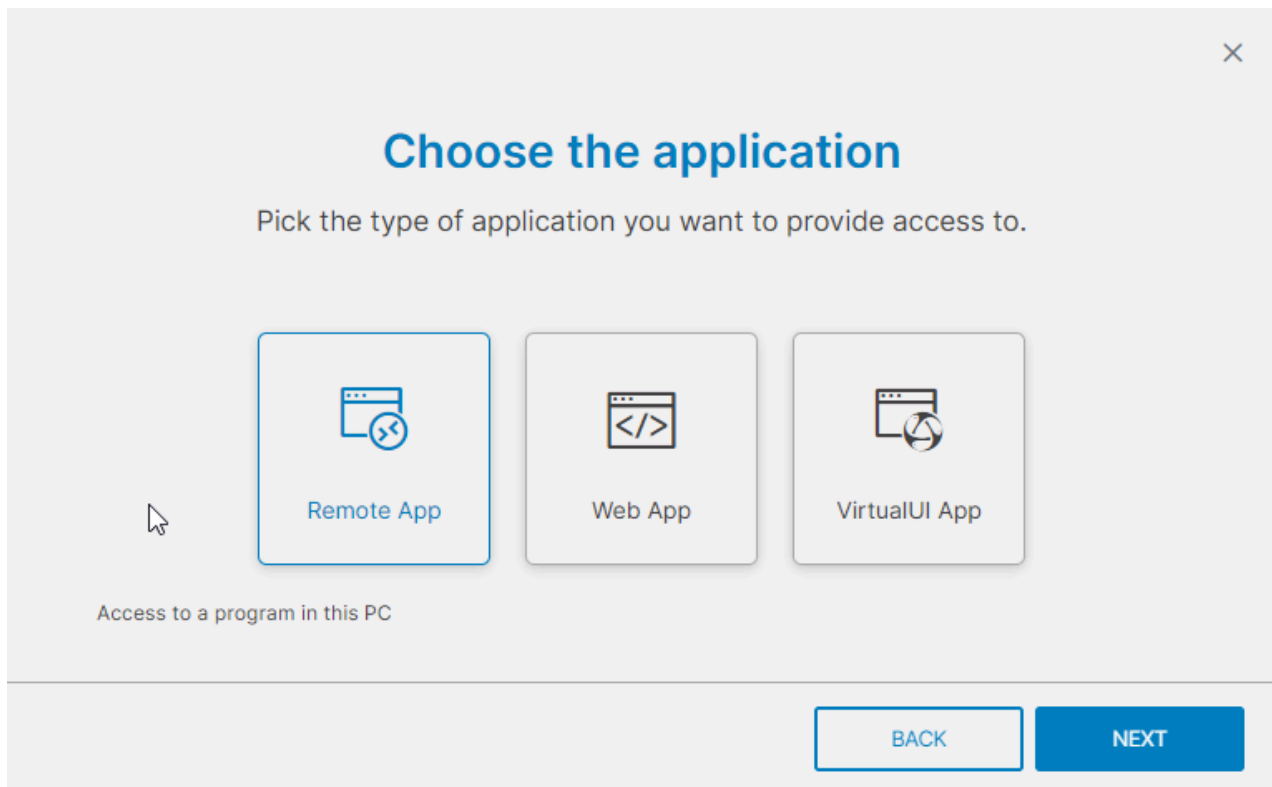


Make this profile available to other users

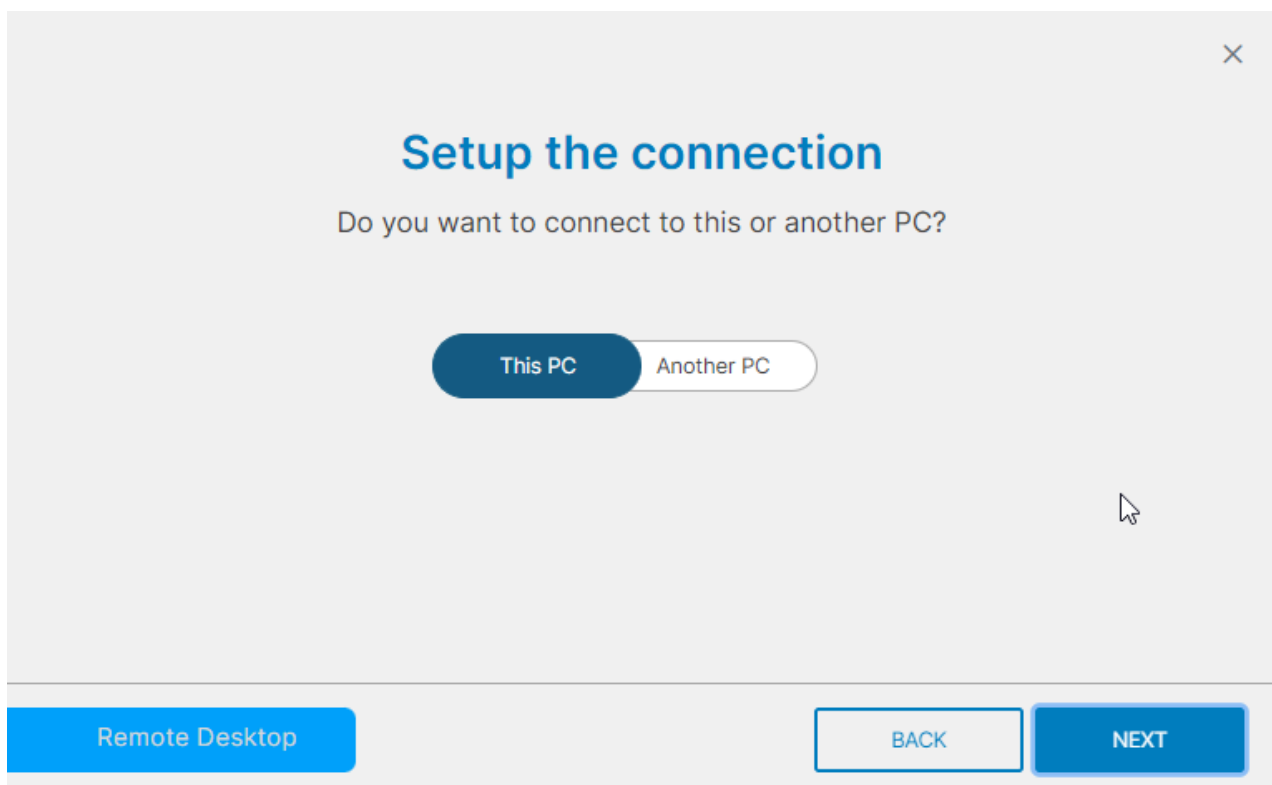


Next

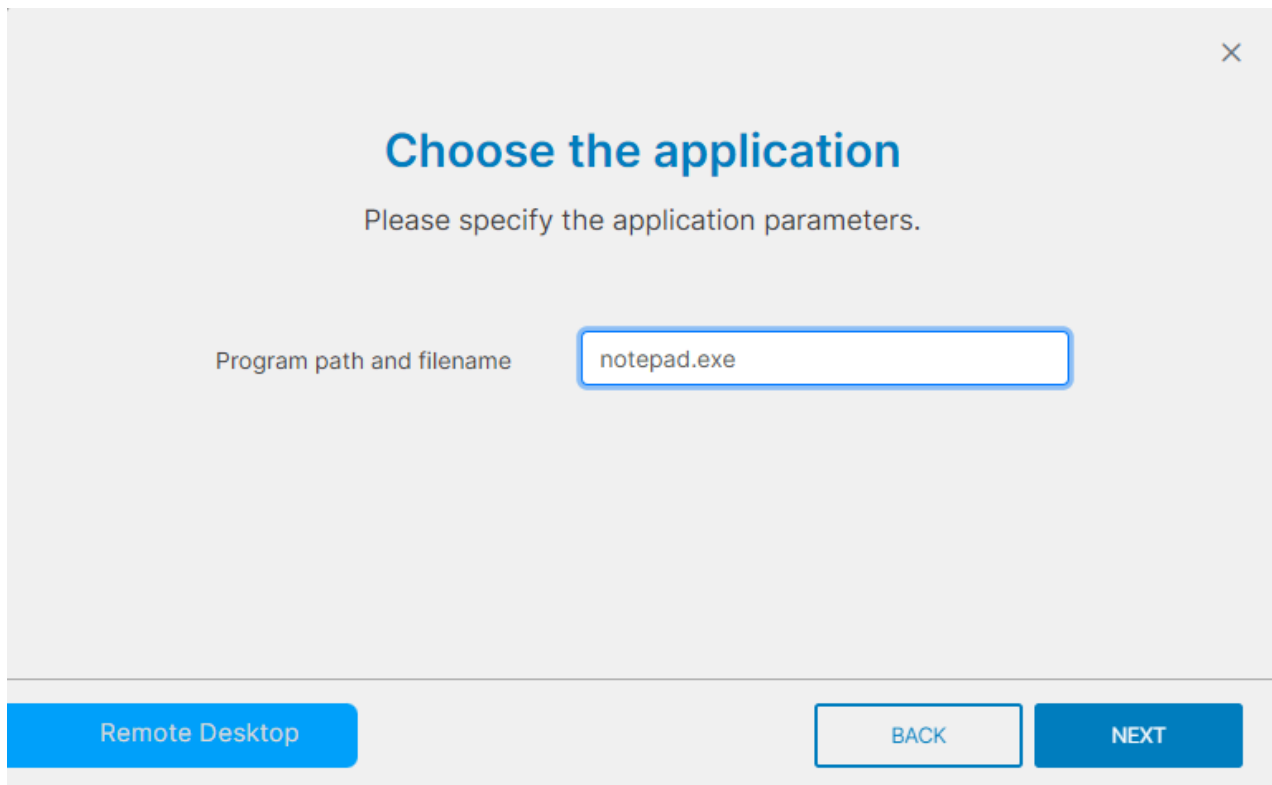
- Select "RemoteApp"



- Now choose between making the connection to the current pc where you're working, or to another terminal

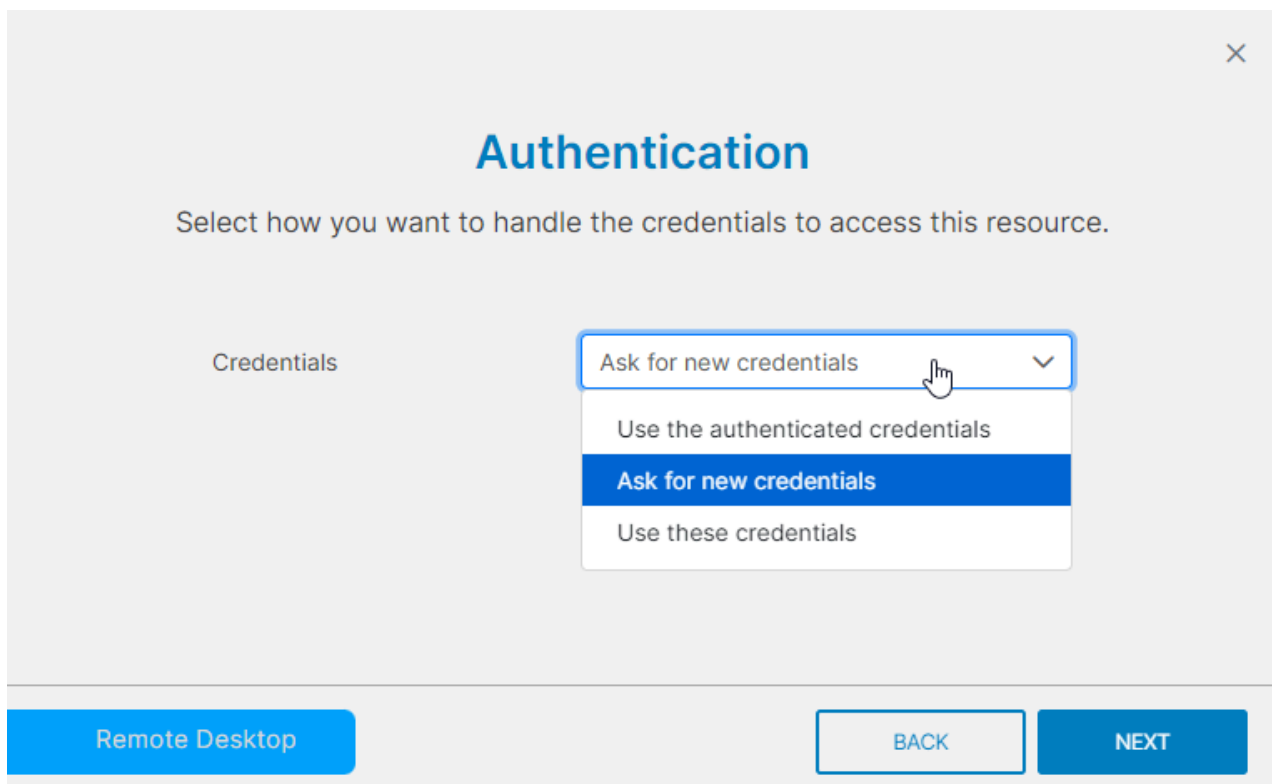


- After that we need to set the virtual path of the application you want to connect



A screenshot of a dialog box titled "Choose the application" with a close button (X) in the top right corner. Below the title is the instruction "Please specify the application parameters." There is a label "Program path and filename" followed by a text input field containing "notepad.exe". At the bottom, there is a blue button labeled "Remote Desktop" on the left, and two buttons labeled "BACK" and "NEXT" on the right.

- Now choose the authentication method



A screenshot of a dialog box titled "Authentication" with a close button (X) in the top right corner. Below the title is the instruction "Select how you want to handle the credentials to access this resource." There is a label "Credentials" followed by a dropdown menu. The dropdown menu is open, showing four options: "Ask for new credentials" (with a checkmark and a hand cursor), "Use the authenticated credentials", "Ask for new credentials" (highlighted in blue), and "Use these credentials". At the bottom, there is a blue button labeled "Remote Desktop" on the left, and two buttons labeled "BACK" and "NEXT" on the right.

- And at last, the name and the icon of the application you're going to use

×

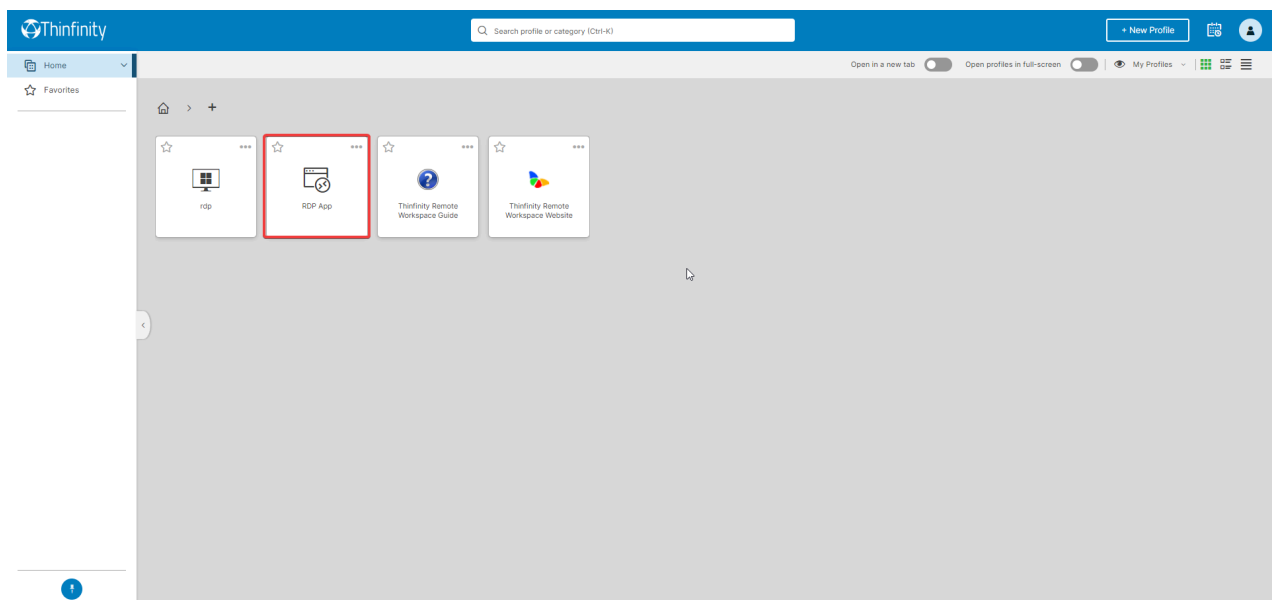
Profile Name

Enter a new name for this profile. This will be used as a friendly name for this connection.

Name

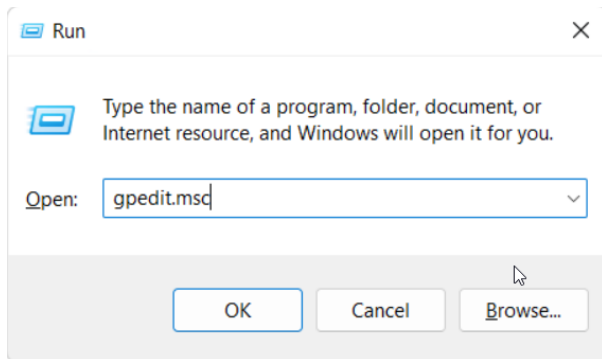
Remote DesktopBACKDONE

- You can now run the application by starting the newly created connection

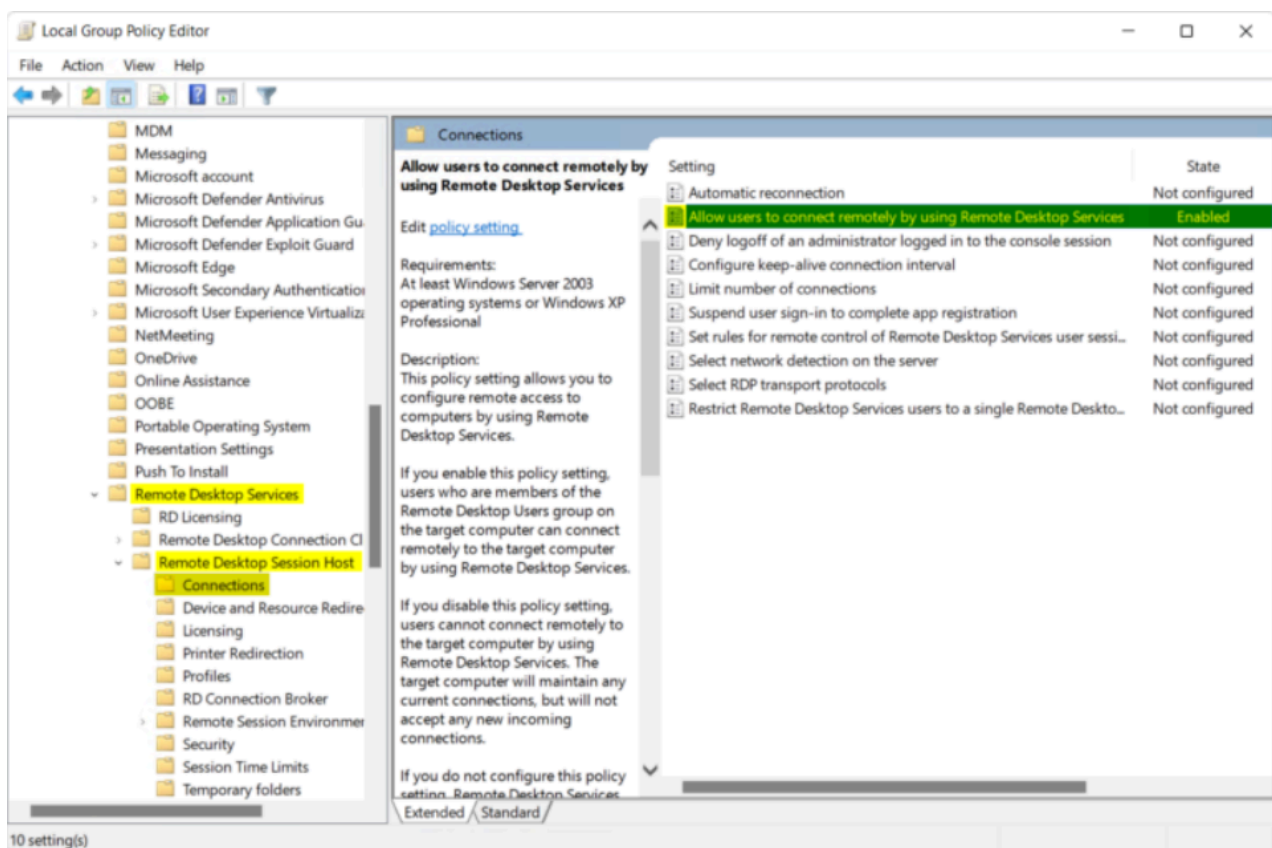


- If you start multiple RemoteApps, you'll find a dock menu at the bottom of the browser screen, this allows you to toggle between different applications of the same connection.
- You can also resize the App's windows and be able to see more than one at the same time.

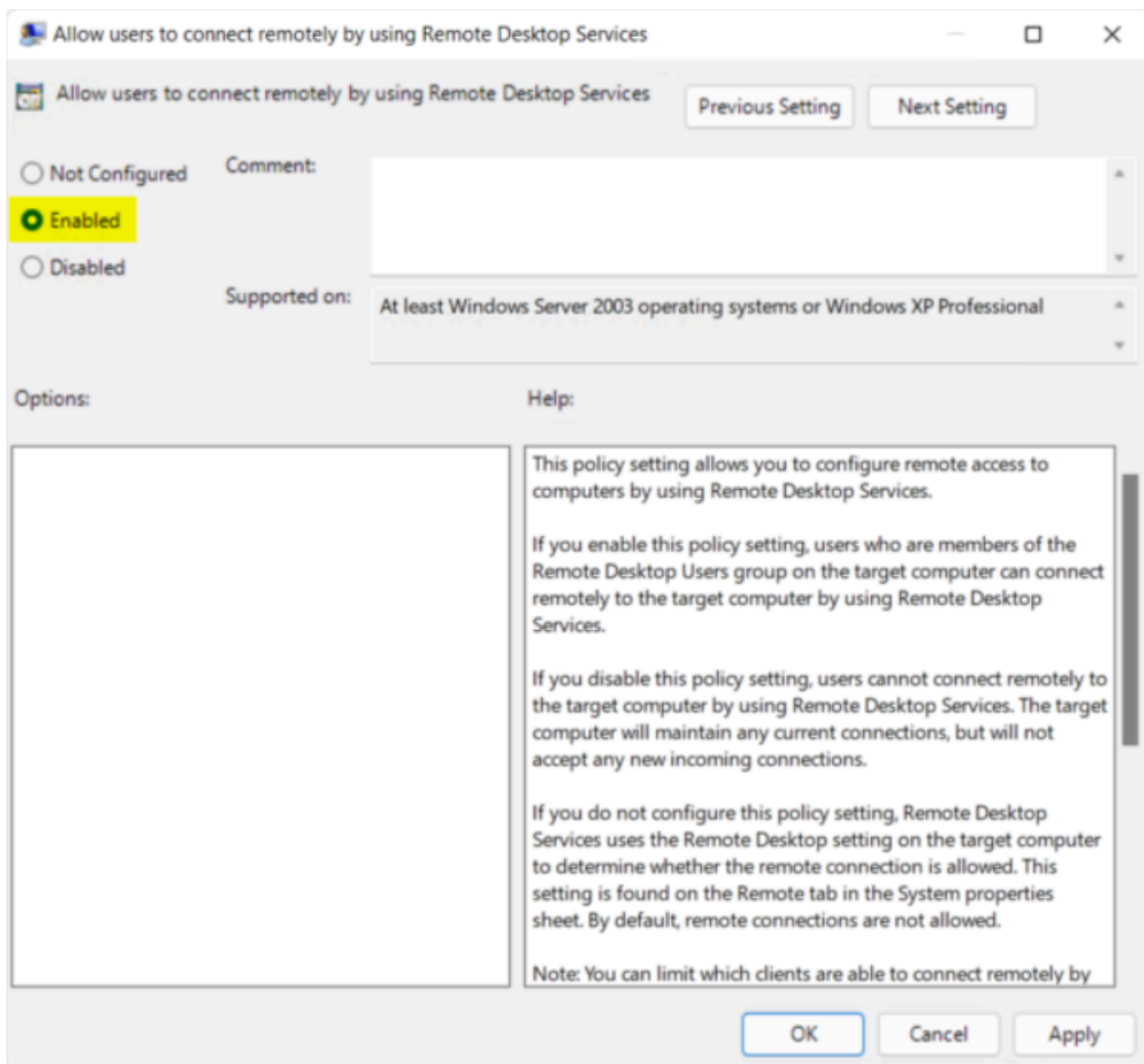
- You can also pin this menu to be always on top or unpin it to automatically hide it.
- If you get an access denied error, you would need to enable a group policy to allow unlisted programs to be started. To this end, open the '*Group Policy Editor*' by going to '*Start > Run > gpedit.msc*':



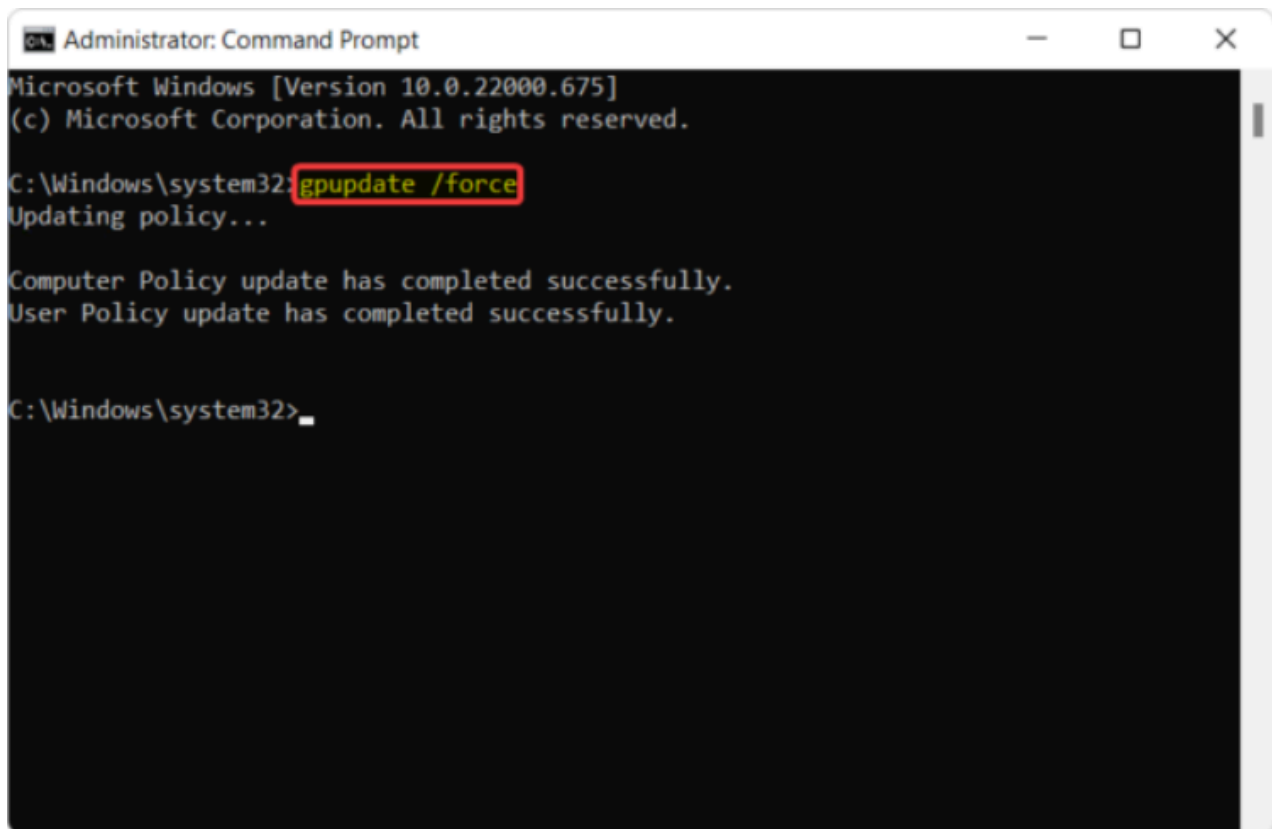
- On the '*Group Policy Editor*' navigate to:
- '*Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections > Allow users to connect remotely by using Remote Desktop Services*'



- Double click on this policy and then click on the check-box next to '*Enabled*':



- Afterwards, you'll have to update the group policies. In order to do this, call '*gpupdate /force*' from a '*Command Prompt*' window elevated as an Administrator:



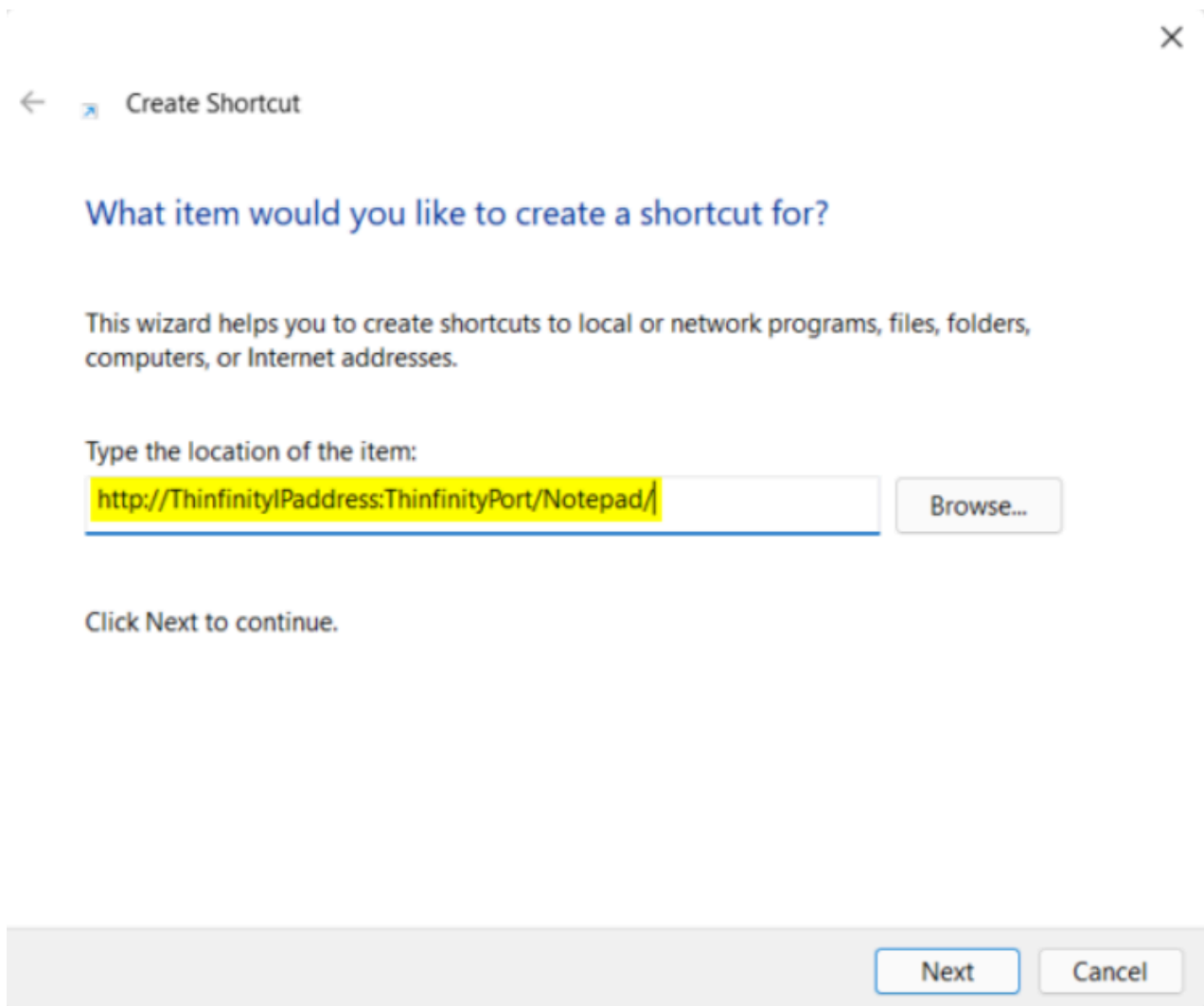
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>gpupdate /force
Updating policy...

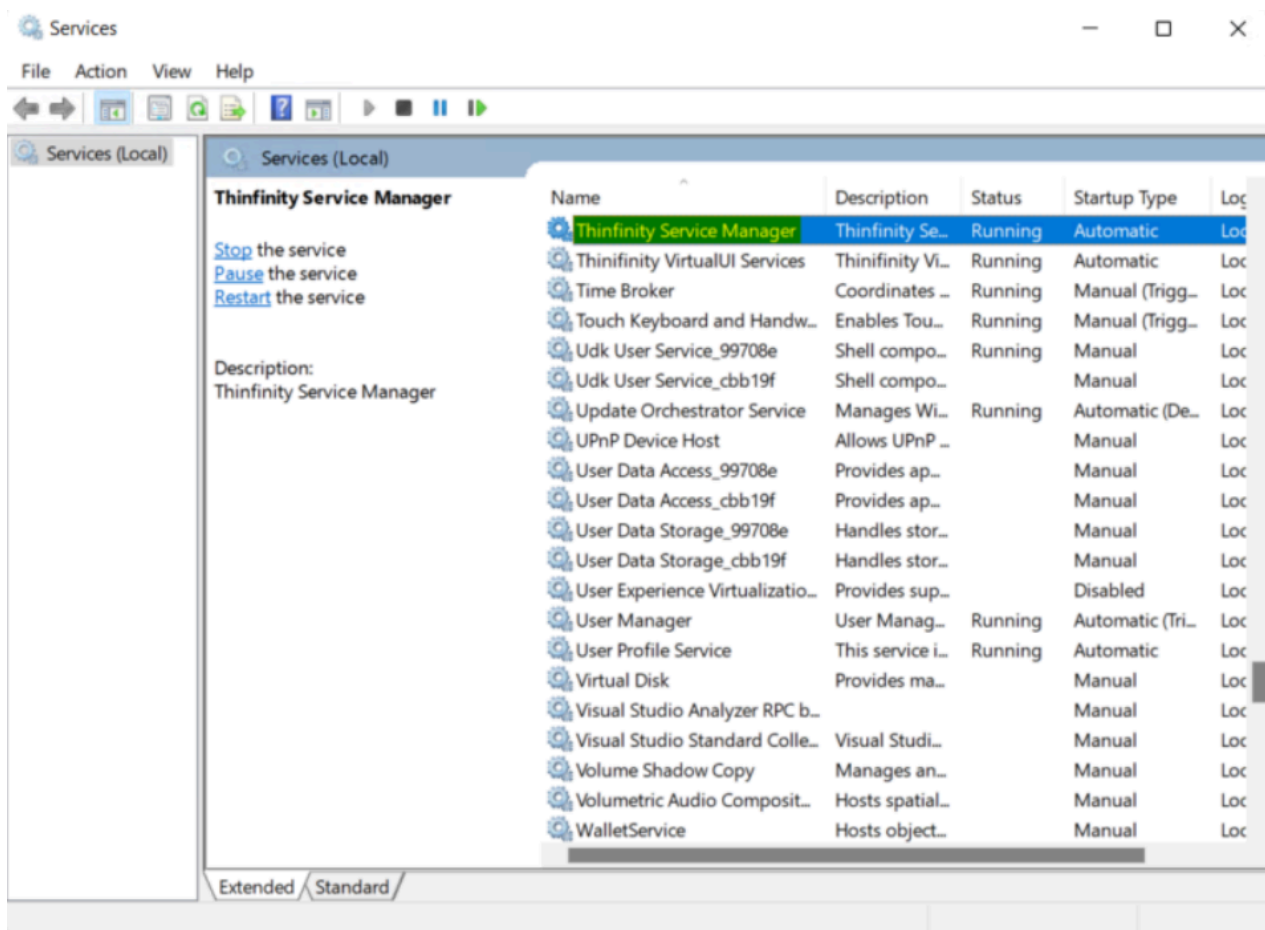
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Windows\system32>
```

- If you want to give your users quick access to your applications, you can create a desktop shortcut to the URL of VirtualUI with the Virtual Path of the application. Here's an example:



- To ensure these changes are applied, you can go to '*Start > Run > services.msc*' and restart the '*Thinfinitiy Service Manager*':



- You can check our live demo and experience this feature yourself. You will be able to test this feature with the following Profiles:
 - Desktop
 - Notepad
 - Paint

Connecting to an Application (old)

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.

Configuring a profile to connect to an application

- Go to the [Profile Editor](#)'s 'Program' tab
- 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:

The screenshot shows the 'Thinfinitiy Configuration Manager - Profile Editor' window. The 'Program' tab is selected, and the 'On Connection' dropdown is set to 'Execute as RemoteApp'. The 'Program path and file name' field contains 'C:\Windows\System32\notepad.exe', the 'Arguments' field is empty, and the 'Start in the following folder' field contains 'C:\Windows\System32'. The 'Show Windows Login and Logout Screen' checkbox is checked. The 'Name' field is 'Notepad', the 'Virtual Path' is 'Notepad', and the 'Access Key' is 'bFg2z4PoPd5NRzVHhwB\$H5z-ev5L\$R'. The 'Label(s)' field is empty. The 'Visible' checkbox is checked, and the 'RDP' radio button is selected. The 'Default profile' and 'RDS Web Feed' checkboxes are unchecked. The 'New Key' and 'Select Label' buttons are visible on the right. The 'Ok' and 'Cancel' buttons are at the bottom right.

Thinfinitiy Configuration Manager - Profile Editor

Name: Notepad

Virtual Path: Notepad

Access Key: bFg2z4PoPd5NRzVHhwB\$H5z-ev5L\$R

Label(s): \

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General | Display | Resources | **Program** | Experience | Advanced | Printer | Permissions | Restrictions | Access Hours | Auth...

On Connection: Execute as RemoteApp

Program path and file name:
C:\Windows\System32\notepad.exe

Arguments:

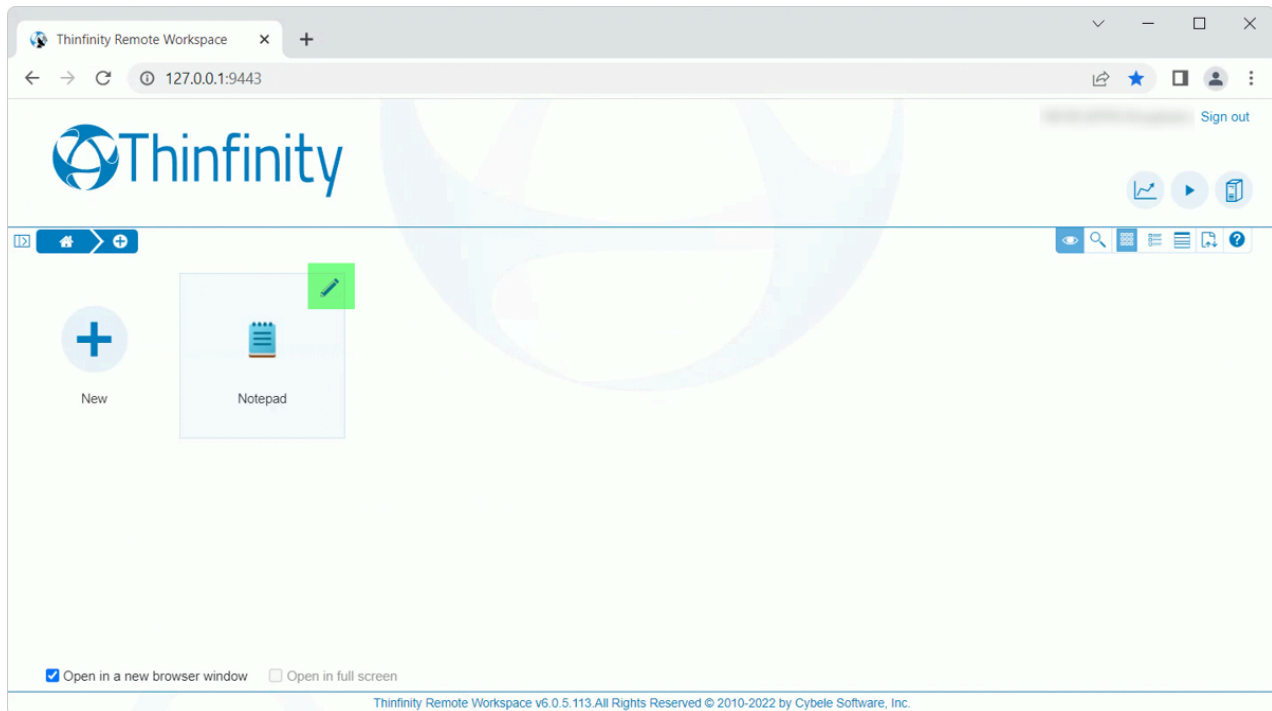
Start in the following folder:
C:\Windows\System32

☒ Show Windows Login and Logout Screen

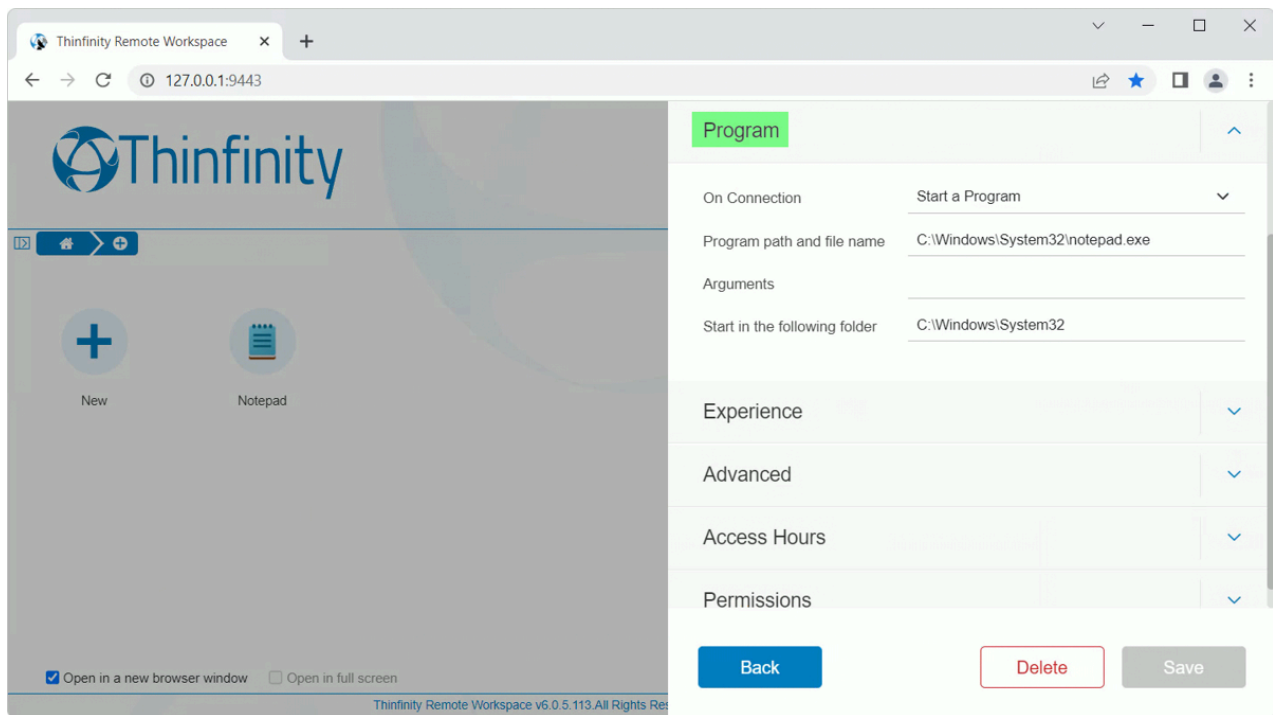
Ok Cancel

Connecting to an application using the '*Any Computer*' profile

- Log in to Thinfinity® Remote Workspace.
- Press the '*Edit*' button (a pen above the connection icon) to show the settings tabs:



- Go to the '*Program*' tab
- 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:



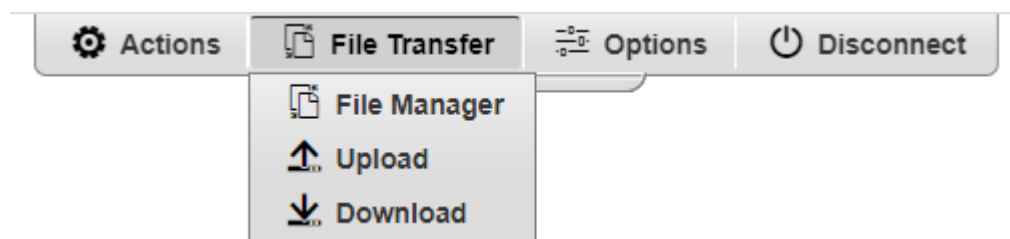
- Set up the other tabs options, if desired.
- Press '*Connect*'.

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:

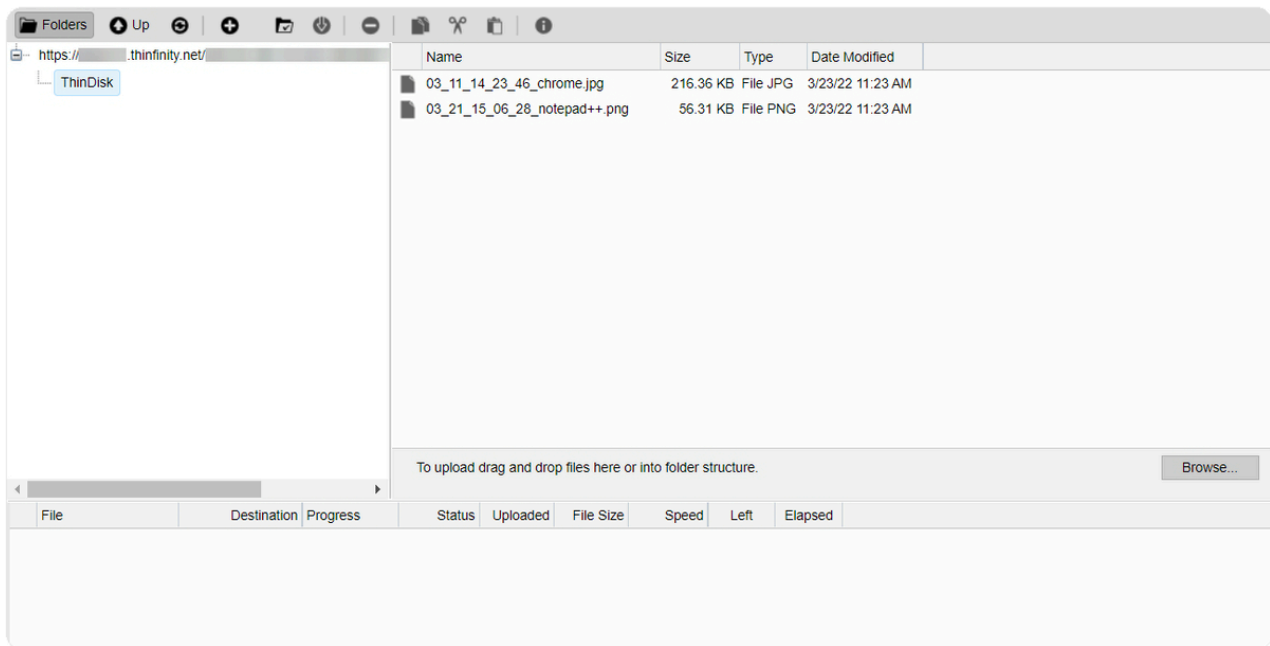
- Click on the connection middle top button, and the toolbar will be presented.

- 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.



OPTION	DESCRIPTION
Upload	Click 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 ' <i>Download</i> ' button.
File Transfer	This option will give you access to the File Transfer Manager.

- This is the screen where you can manage files and also transfer them:



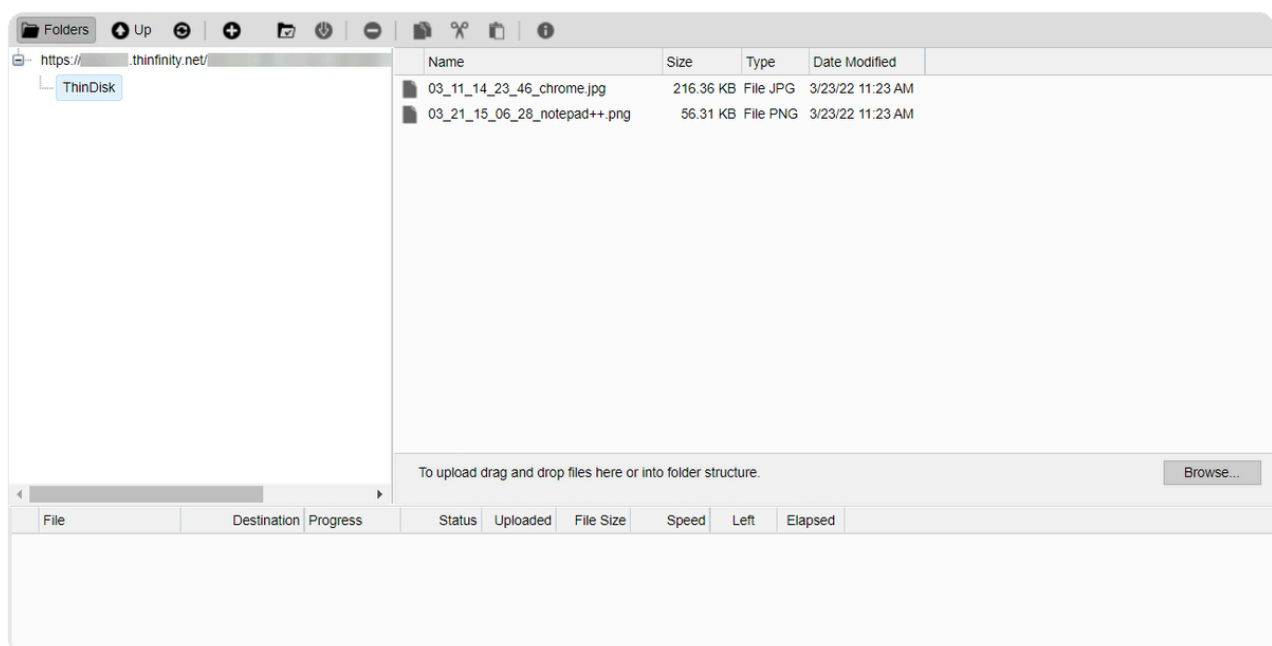
- Observe that the '[Shared Folders](#)' and the '[Intermediate Disk](#)' are the only remote directories available to exchange files with. If you need to [download or upload remote files](#) from the file manager, you should always move them first into these directories (they are going to be mapped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

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.

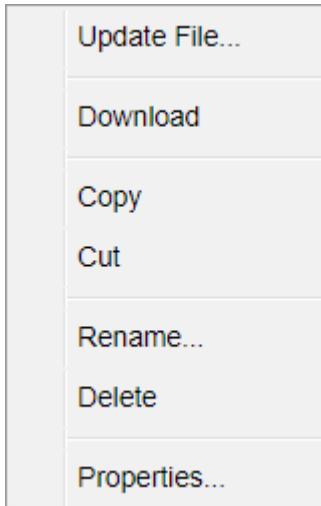
In order to upload files, drag them from your local PC and paste them into the remote view area, or press the '*Browse*' button.

The lower part of the screen shows the status of the files to be transferred.



File Options

Right click on a remote file to access these options:

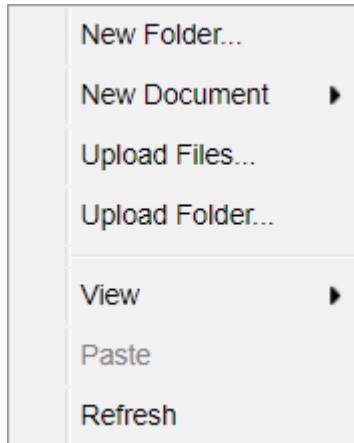


Find the behavior for each one of these options below:

OPTION	DESCRIPTION
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.

Remote Folder Area Options

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



Find the behavior for each one of these options below:

OPTION	DESCRIPTION
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.

Downloading and Uploading files

Downloading remote files:

- Connect to the remote machine.
- Open Windows Explorer on the remote machine and copy the remote files to be downloaded into a '[Shared Folder](#)' or an '[Intermediate Disk](#)'.
- Open the '*File Transfer*' Manager from the upper connection toolbar.
- Download the remote file to any local directory of your preference.

Uploading local files:

- Connect to the remote machine.
- Open the '*File Transfer*' Manager from the upper connection toolbar.
- Upload the file you want to transfer to the remote machine into a '[Shared Folder](#)' or an '[Intermediate Disk](#)'.
- Go back to the connection screen and open Windows Explorer on the remote machine.
- Copy the file from the '[Shared Folder](#)' or '[Intermediate Disk](#)' drive into the remote directory of your preference.

Supported RDP Shortcut Keys

The supported shortcut keys in Thinfinity® Remote Workspace 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)

Using Thinfinity® Remote Workspace for the first time

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

[Verify the communications settings](#)

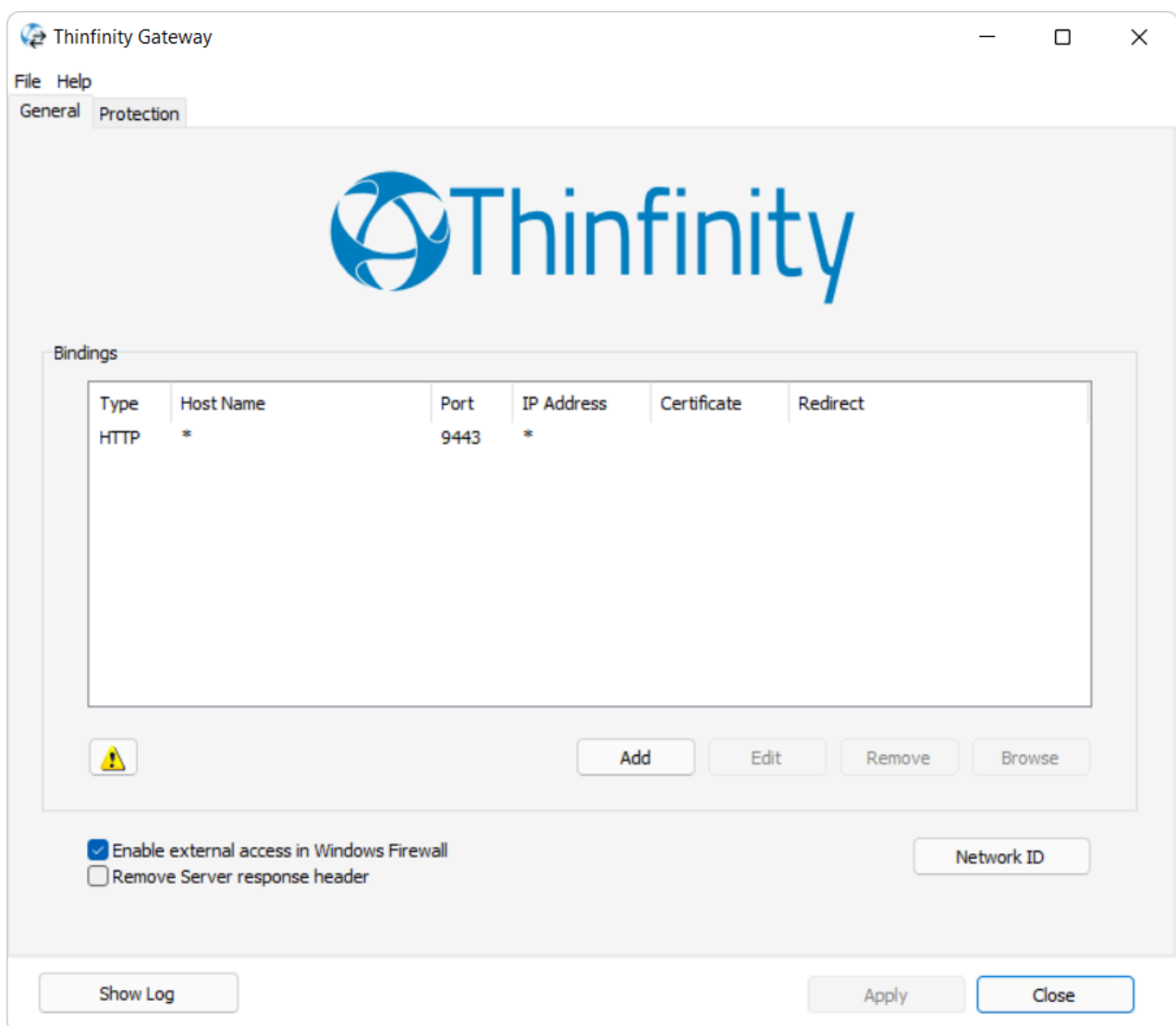
Once Thinfinity® Remote Workspace is installed and RDP is enabled on the remote machine, all you need is an HTML5 compatible browser: Google Chrome, Mozilla Firefox, Safari, Opera, Microsoft Edge.

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

Verifying the Communication Settings

Thinfinity® Gateway listens by default on port 9443. If you see the message '*Could not bind socket. Address and port are already in use*' in the Thinfinity® Remote Workspace Gateway Log (by clicking on the '*Show Log*' button), it means that you will have to use another port since this one is already in use by another application.

- Identify a port number that is not yet in use in the computer where Thinfinity® Remote Workspace Gateway is installed:



- Click on the binding you wish to change the port number and click on '*Edit*':

Binding

✕

Protocol: HTTP

Bind to IP: (All unassigned)

Port: 9443

Host name:

SSL

Certificate:

View

New

☐ Redirect incoming requests to this URL

URL:

Example: https://www.mycompany.com/

Status code: Found (302)

OK

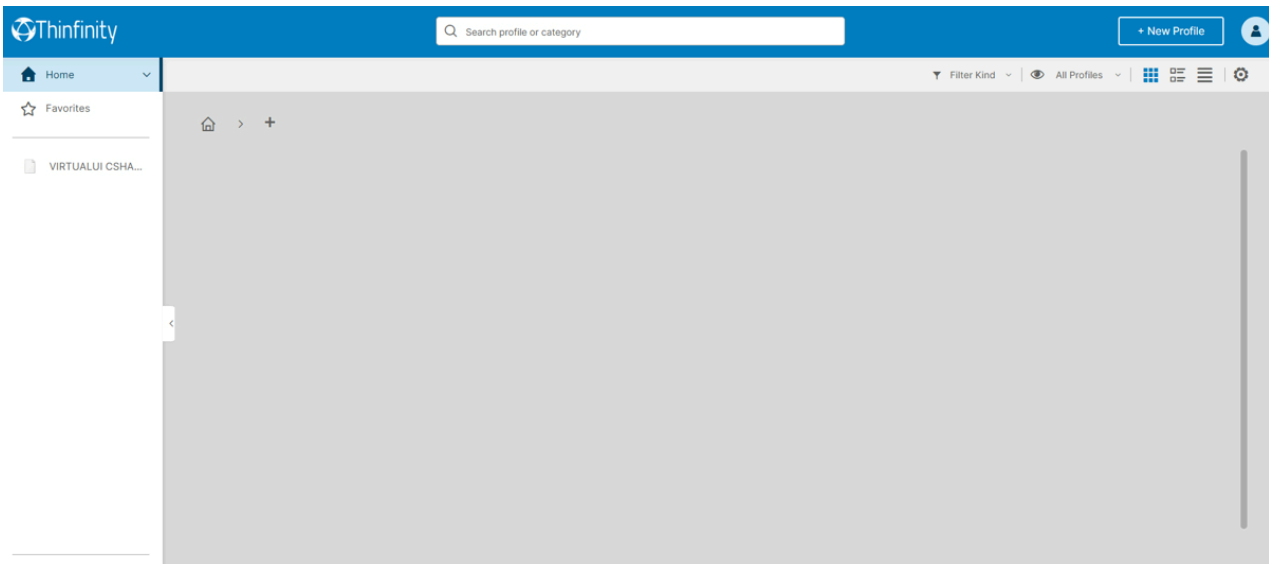
Cancel

- Press '*Apply*'. Wait for a couple of minutes.
- Verify whether Thinfinity® Gateway is running in the status message.

Connecting to a desktop

- Open your preferred HTML5-enabled web browser in the computer where Thinfinity® Remote Workspace was installed
- Type the following URL: '<http://127.0.0.1:9443>' 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:



- Click on "New Profile" or the "+", and then click "Desktop"
- In the '*Computer*' field, enter the remote desktop IP you want to connect to.
- Enter the Username and Password for the remote machine.
- Press '*Connect*'.
- 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 you'll be shown all the options you can configure to your liking.

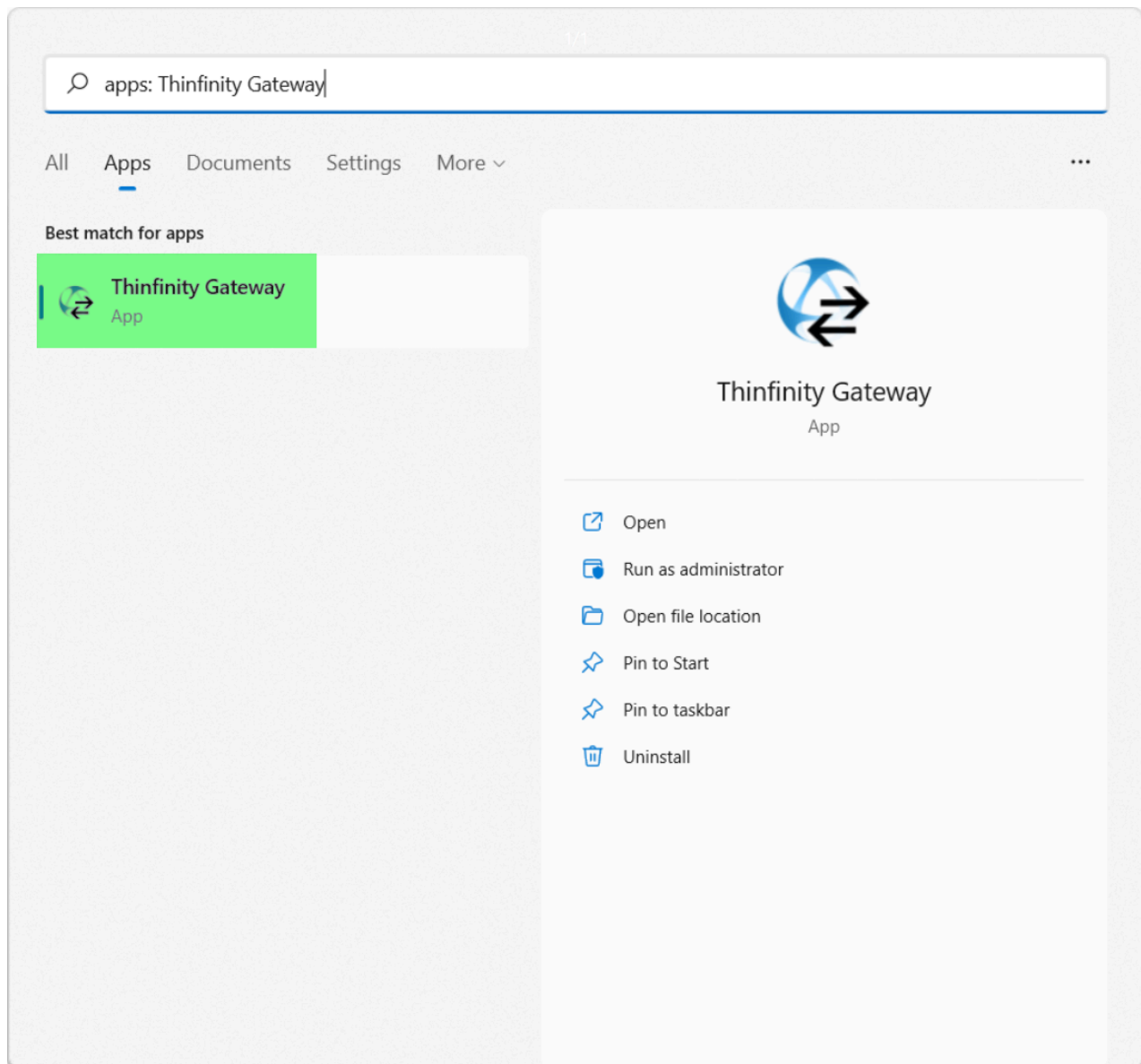
To set up different options and make Thinfinity® Remote Workspace better suit your needs, read the [Customizing Thinfinity® Remote Workspace](#) topic.

Advanced Settings Section

Gateway Manager

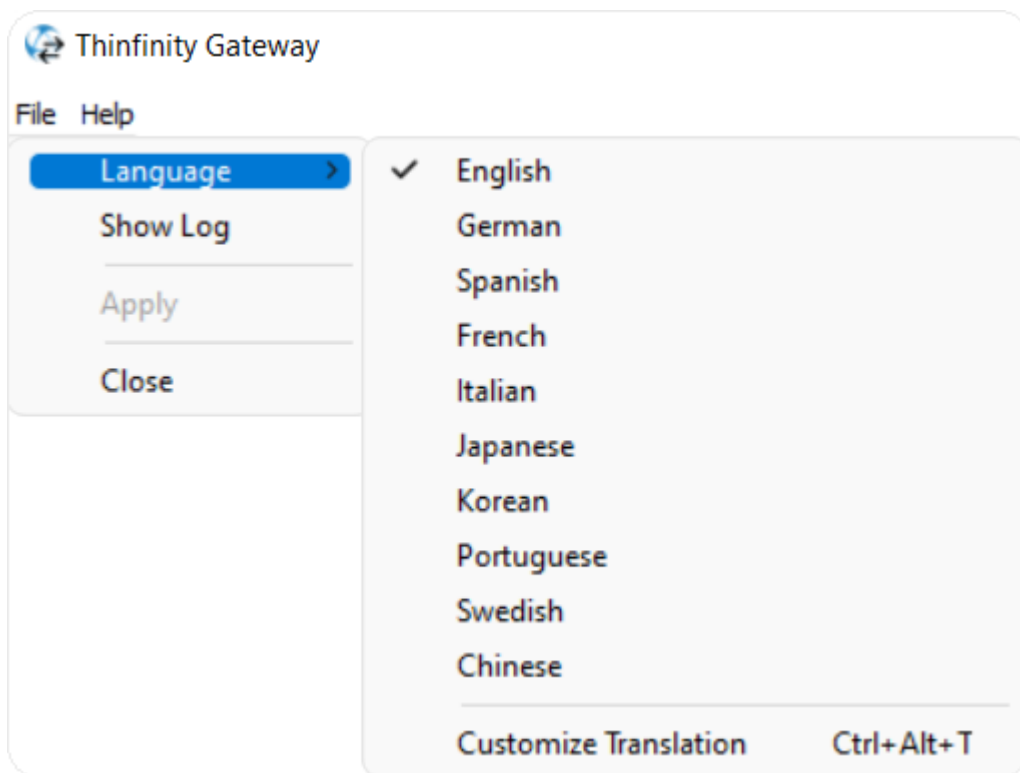
The Gateway Manager is a tool to configure gateway options in a [Load Balancing](#) scenario.

- Install Thinfinity® Remote Workspace and look for the Thinfinity® Gateway shortcut in the Start Menu:



Its main menu has two sub-menus:

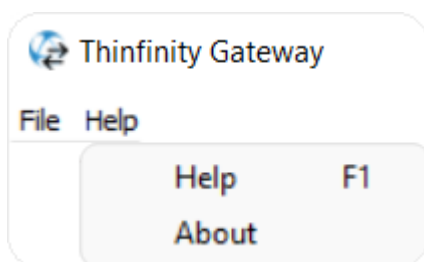
File Menu



The File Menu is composed of the following options:

OPTION	DESCRIPTION
Language	Language display options for the Thinfinity® Gateway
Show Log	Displays the Thinfinity® Gateway log.
Apply	Apply changes to the configuration
Close	Closes the Thinfinity® Gateway

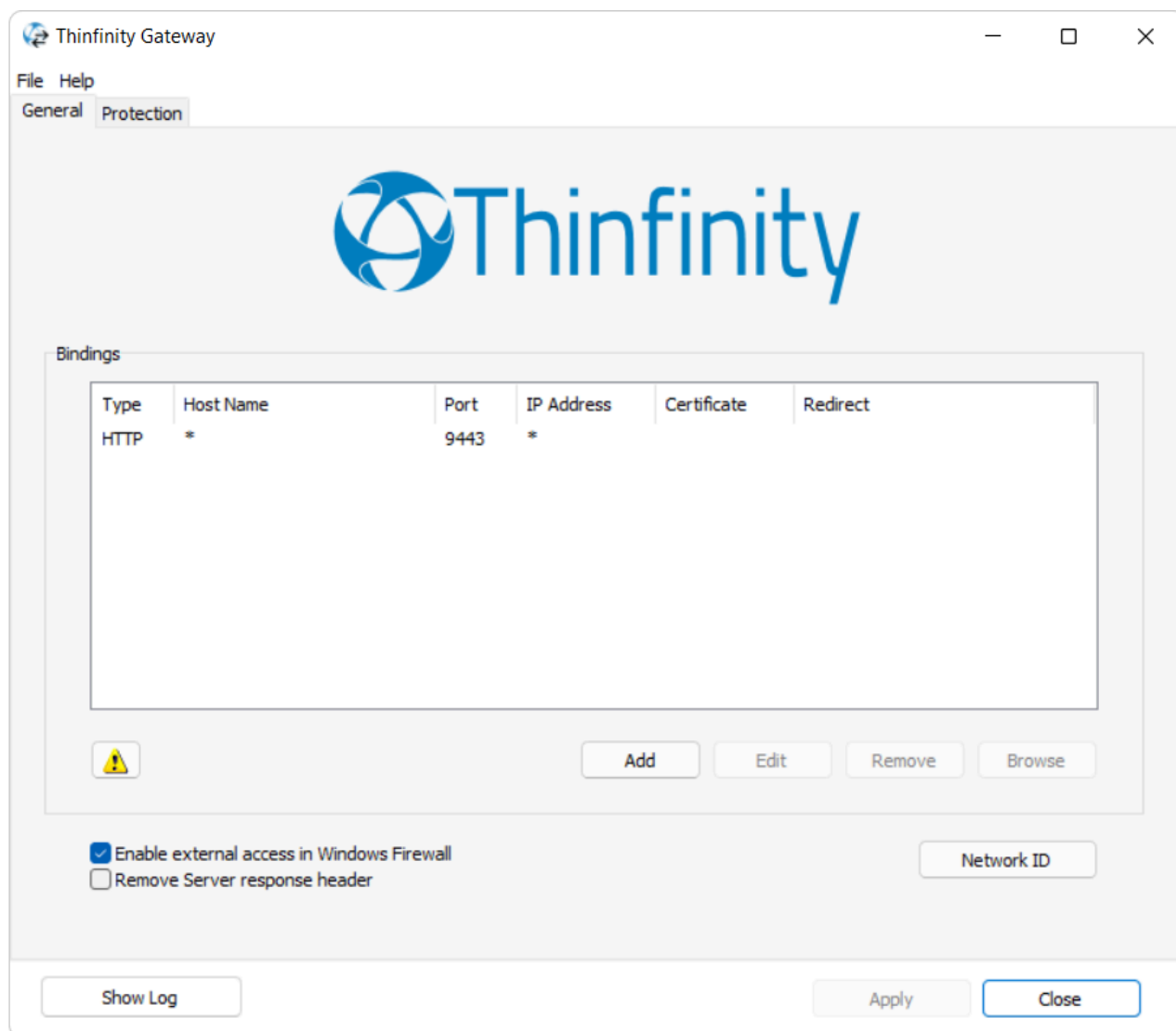
Help Menu



The Help Menu is composed of the following options:

Option	Description
About	Click on the 'About' option to see the application version and build number.

General tab



The General tab presents the following options:

Option	Description
Bindings	A list of the gateway's ports that a user can connect to in order to access this server's resources.
Add	Add a new binding to the Gateway Bindings.

Edit	Edit the selected binding
Remove	Remove a binding Bindings list.
Browse	Navigates to the selected binding.
Enable external access in Windows Firewall	Adds the currently configured bindings on the Windows Firewall exception list. This is mandatory for certain Windows Firewall configurations.
Remove Server response header	Removes headers from the Thinfinity® Remote Workspace response.
Network ID	<p>The network ID identifies this installation. Thinfinity® Remote Workspace's 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>

Protection tab

Thinfinity Gateway

File Help

General Protection

☒ Enable brute force detection

Max. login attempts: 3

Re-enable after: 10 minutes

White list | Black list

Address/Mask	Source
127.0.0.1	Runtime
	Runtime
	Runtime

Add Remove

Show Log Apply Close

Options	Description
Enable brute force detection	Enables brute force protection measures
White list	Determines the allowed IPs that can connect to Thinfinity® Remote Workspace
Black list	Determines the IPs that are blocked from connecting to Thinfinity® Remote Workspace

Managing the SSL Certificate

You can access configuration for the SSL certificate by pressing the Edit 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 Workspace 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.

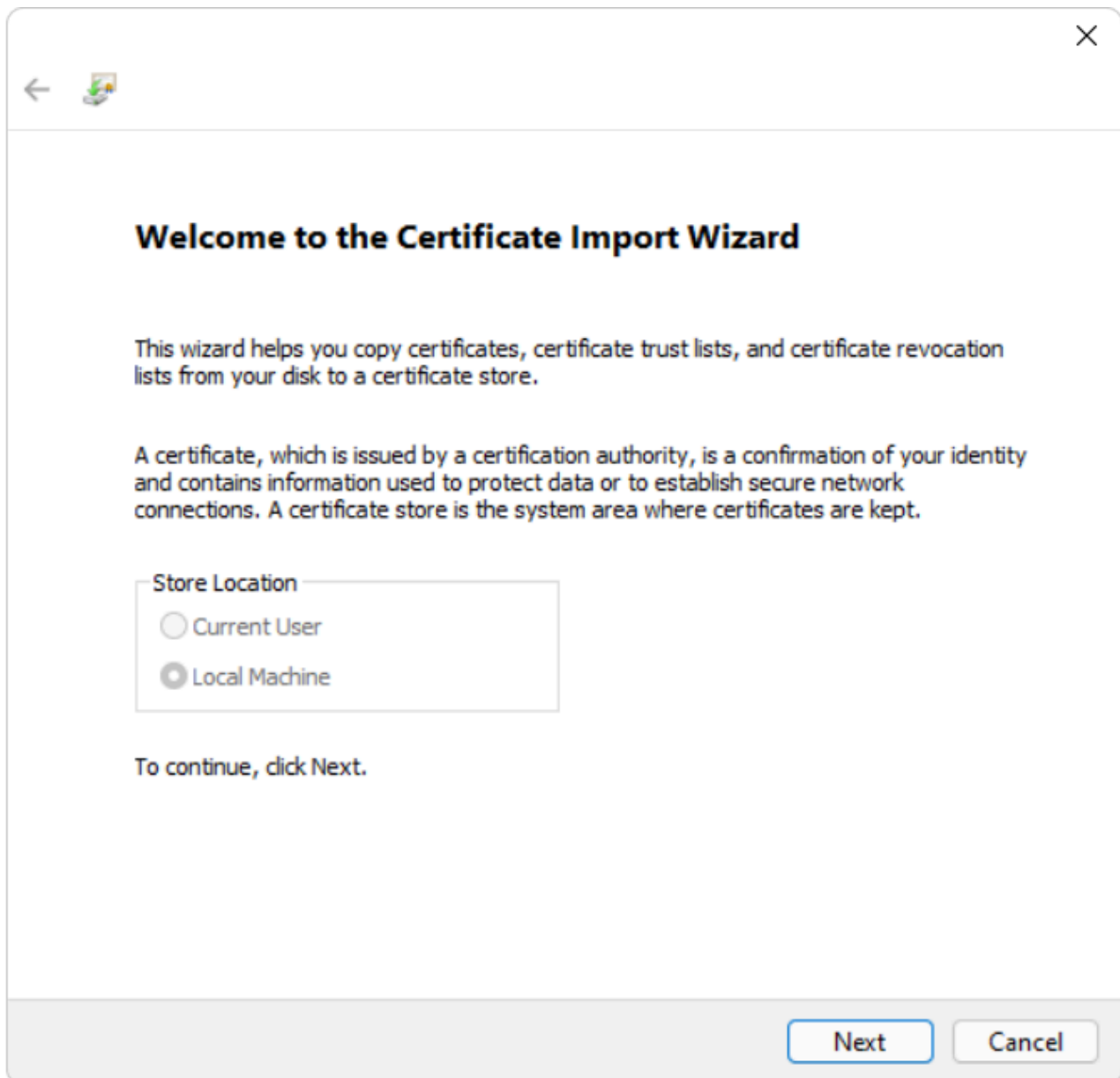
Managing the SSL Certificate:

- There are two ways of creating your own SSL certificate:

1. Create [A self-signed certificate](#)

2. Use [A CA Certificate](#)

- Once you already have your certificate files, go to the Thinfinity® Configuration Manager's General tab.
- Click on the Edit button when using HTTPS.
- On this screen, inside the Certificate menu, you can select the certificates that are located in your Personal folders in Window's certificate folder.
- If you need to add your own certificate, you can do so by clicking on the New button and then Import Certificate. Windows Import certificate menu will be displayed. Follow the instructions for adding it to the running system:



A Self-Signed Certificate

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

- Go to the Thinfinity® Configuration Manager's '*General*' tab. Click on '*Edit*' on an HTTPs connection.
- Click on '*New*' and , press the '*Create a self-signed certificate*' button.
- Fill in the form below with your organization data:

Create self-signed certificate and private key

Certificate Properties

Country Code:

State:

Locality:

Organization:

Organizational Unit:

Common Name:

E-Mail address:

Bits:

2048

>= 1024

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

Create

Close

OPTION	DESCRIPTION
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.

- The '*Common Name*' field should be filled with the server+domain that will be used to access Thinfinity® Remote Workspace (rdp.mycompany.com).
- Press '*Create*'.
- Select the location where you want the certificate to be stored.
- The application will start using this self-signed certificate just created by you.

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

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:

- Go to the Thinfinity® Configuration Manager's 'General' tab. Click on '*Edit*' on an HTTPS connection.
- Click on '*New*' and , press the '*Create a self-signed certificate*' button.
- Fill in the form below with your organization data:

Create certificate request and private key

Certificate Properties

Country Code:

State:

Locality:

Organization:

Organizational Unit:

Common Name:

E-Mail address:

Bits:

2048

>= 1024

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

Create

Close

OPTION

DESCRIPTION

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.

- The '*Common Name*' field should be filled with the server+domain that will be used to access Thinfinity® Remote Workspace (rdp.mycompany.com)
- Press '*Create*' and the application will generate two files.
- 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*'.

1. Inform a name for your private key.
2. Select a place to keep it safe.
3. Press the '*Save*' button.

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

1. Inform a name for the request file.
2. Select a directory where you can find the file later on to send to the CA.
3. Press the '*Save*' button.

- The first file is the certificate private key. It should always be kept safe with you.
- Send only the request file to the CA.

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

Thinfinity® Remote Workspace Configuration Manager

The Thinfinity® Remote Workspace Configuration Manager is a tool for administrators to set up general settings.

You can manage users, profiles, RDP preferences and settings related to the Thinfinity® service.

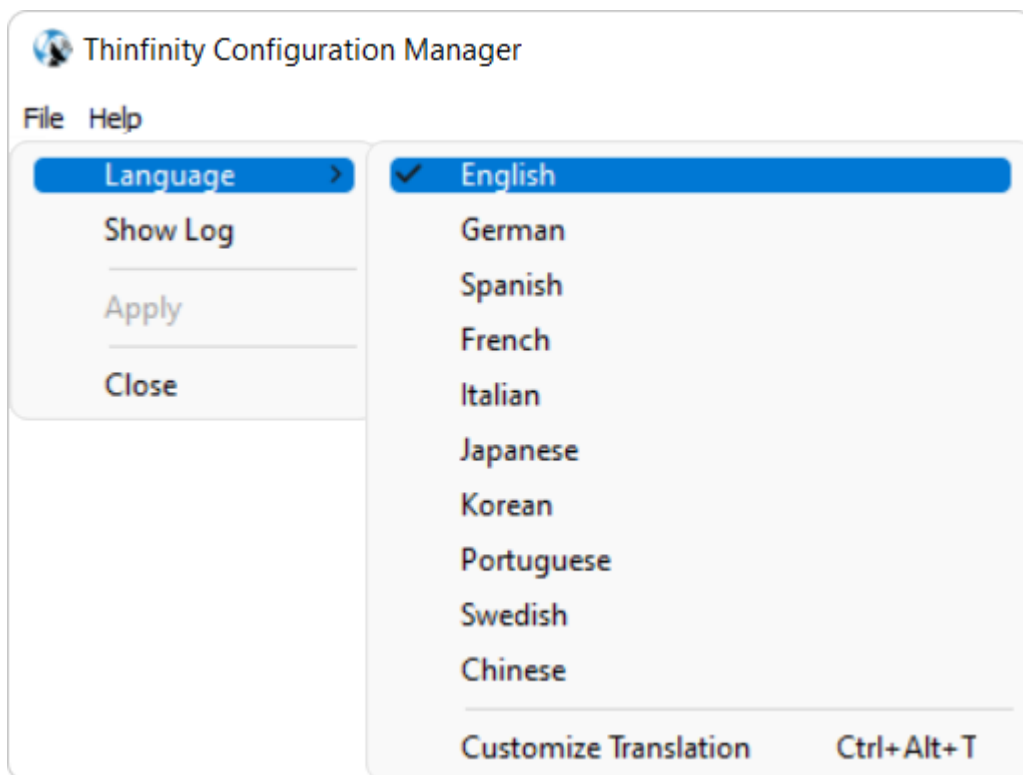
To access the Thinfinity® Configuration Manager go over the Start Menu options and look for the '*Thinfinity® Remote Workspace Configuration Manager*' item.

The Thinfinity® Remote Workspace Configuration Manager interface is composed of the following tabs:

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

The Thinfinity® Remote Workspace Configuration Manager main menu consists of two sub-menus:

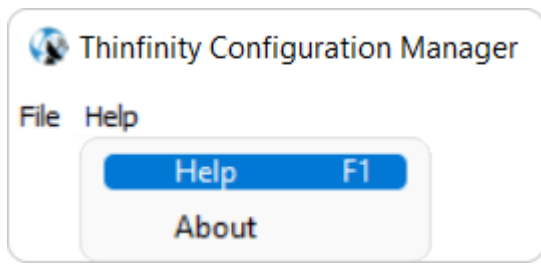
The '*File*' Menu



The File Menu is composed by the following options:

Option	Description
Language	<p>Allows you to choose different languages for the application.</p> <p>Click on the Language that you want the application to work with.</p> <p>English is the default language.</p>
Show Log	
Apply	<p>Click to save any change done on the system Settings.</p>
Close	<p>Click on this option to exit the Thinfinity® Configuration Manager.</p>

The Help Menu:

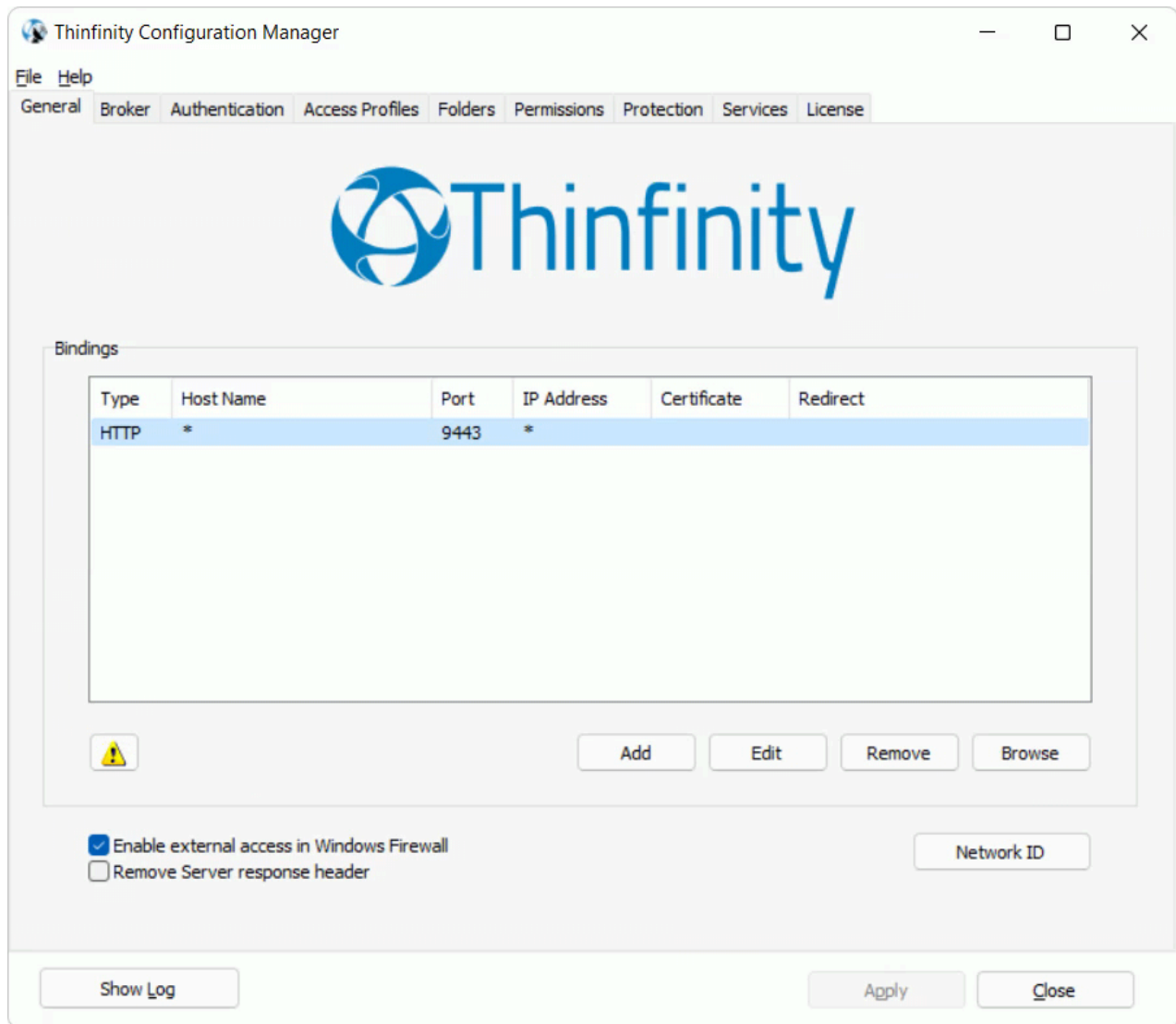


The Help Menu is composed by the following options:

Option	Description
About	Click here to see the application version and build number.

General

In the Thinfinity® Remote Workspace Configuration Manager's '*General*' tab you will find the following options:



OPTION	DESCRIPTION
Bindings	A list of the gateway's ports that a user can connect to in order to access this server's resources.
Add	Add a new binding to the Gateway Bindings.
Edit	Edit the selected binding
Remove	Remove a binding from the Bindings list.

Browse	Navigates to the selected binding.
Enable external access in Windows Firewall	Adds the currently configured bindings on the Windows Firewall exception list. This is mandatory for certain Windows Firewall configurations.
Network ID	<p>The Network ID identifies this installation. Any Thinfinity® Remote Workspace 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>

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

Broker

In the '*Broker*' tab of the Thinfinity® Remote Workspace Configuration Manager you will find the following options:

Thinfinity Configuration Manager

File Help

General Broker Authentication Access Profiles Folders Permissions Protection Services License

Primary broker

Users Limit: 10000 per broker

Secondary brokers

Pool List:

Name	Users Limit	Load-Balancing	Default
------	-------------	----------------	---------

Add Remove

Gateways

Network ID: GW-7131-1553-2220

Gateway List:

Add Remove

Show Log Apply Close

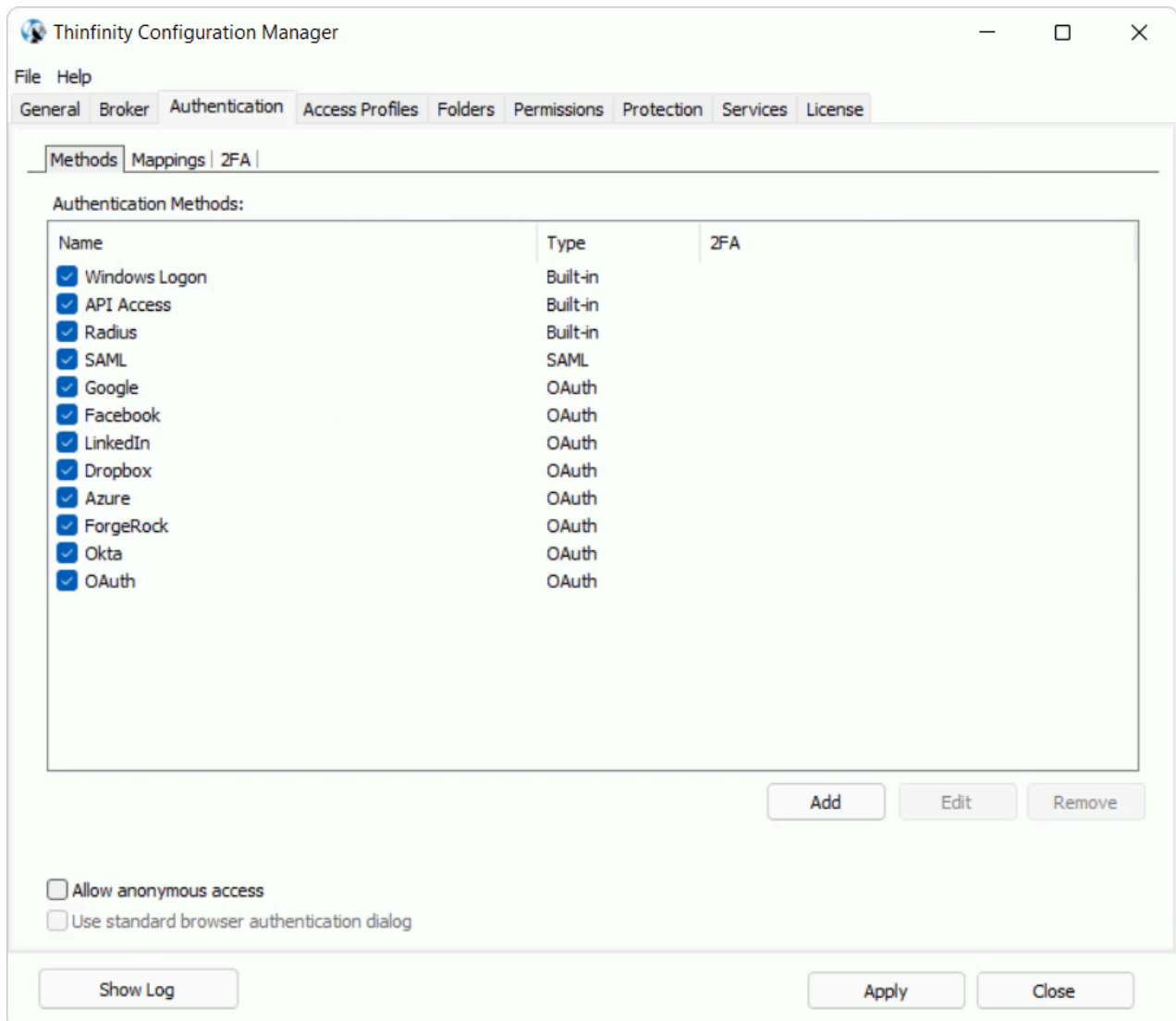
OPTION	DESCRIPTION
User Limit	Sets the limit of users that can connect to this Thinfinity® Remote Workspace server instance.
Pool List	Shows the list of secondary brokers.
Network ID	Sets the Network ID for this Thinfinity® Remote Workspace server instance.



Authentication

In the Thinfinity® Remote Workspace Configuration Manager's '*Authentication*' tab you will find the following options:

- '*Methods*' tab



OPTION	DESCRIPTION
Authentication Methods	<p>Defines the authentication methods allowed for logging in to Thinfinity® Remote Workspace.</p> <p>By default, Windows Logon (Active Directory) is enabled.</p>

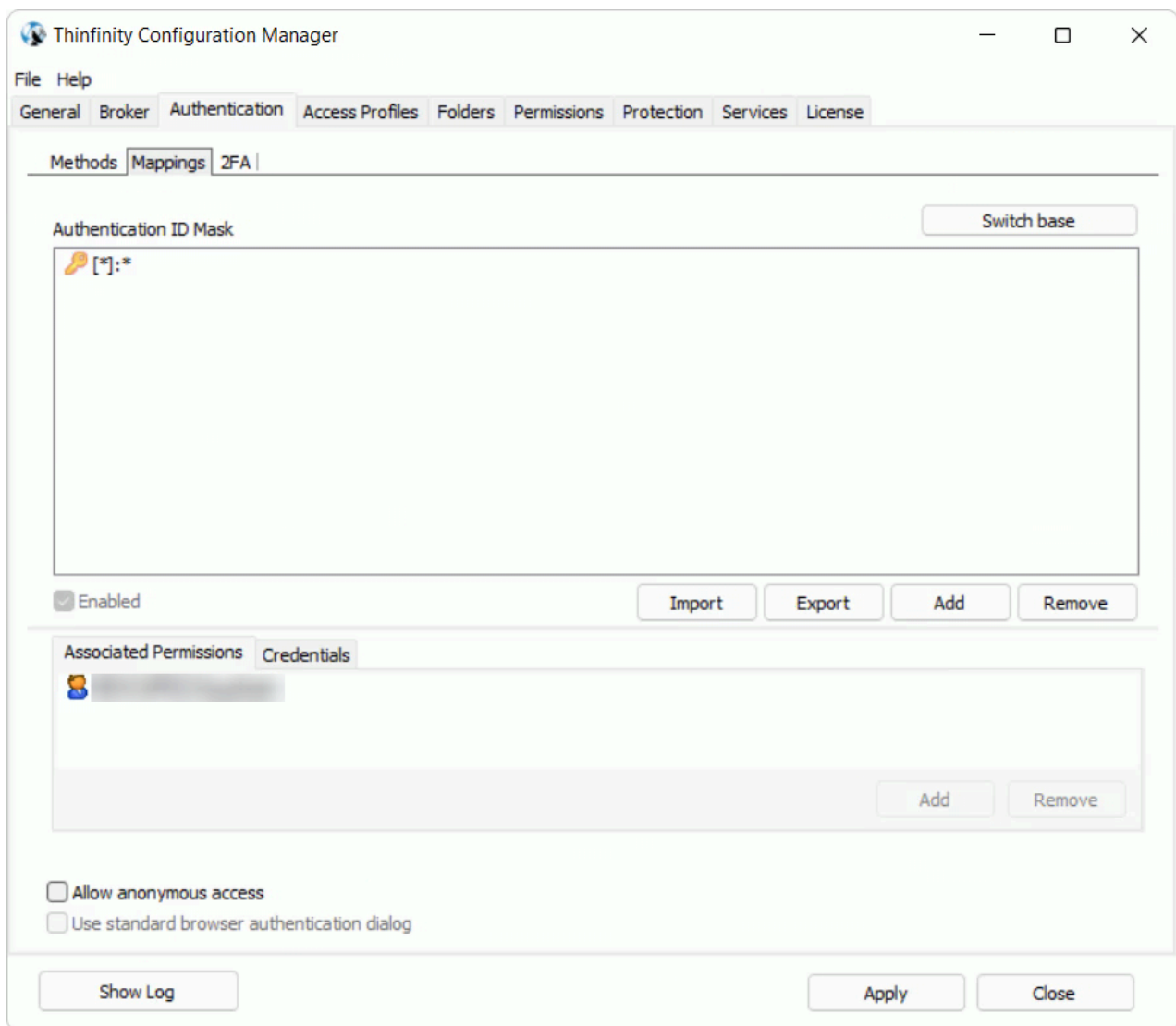
Allow anonymous access	Enables or disables anonymous access to the Thinfinity® Remote Workspace's index page
Use standard browser authentication dialog	Check this option to use the standard browser authentication dialog instead of the Thinfinity® Remote Workspace web login. This option is only available when "Authentication" is set to "Access Profiles". Check it to use the standard browser

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

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.

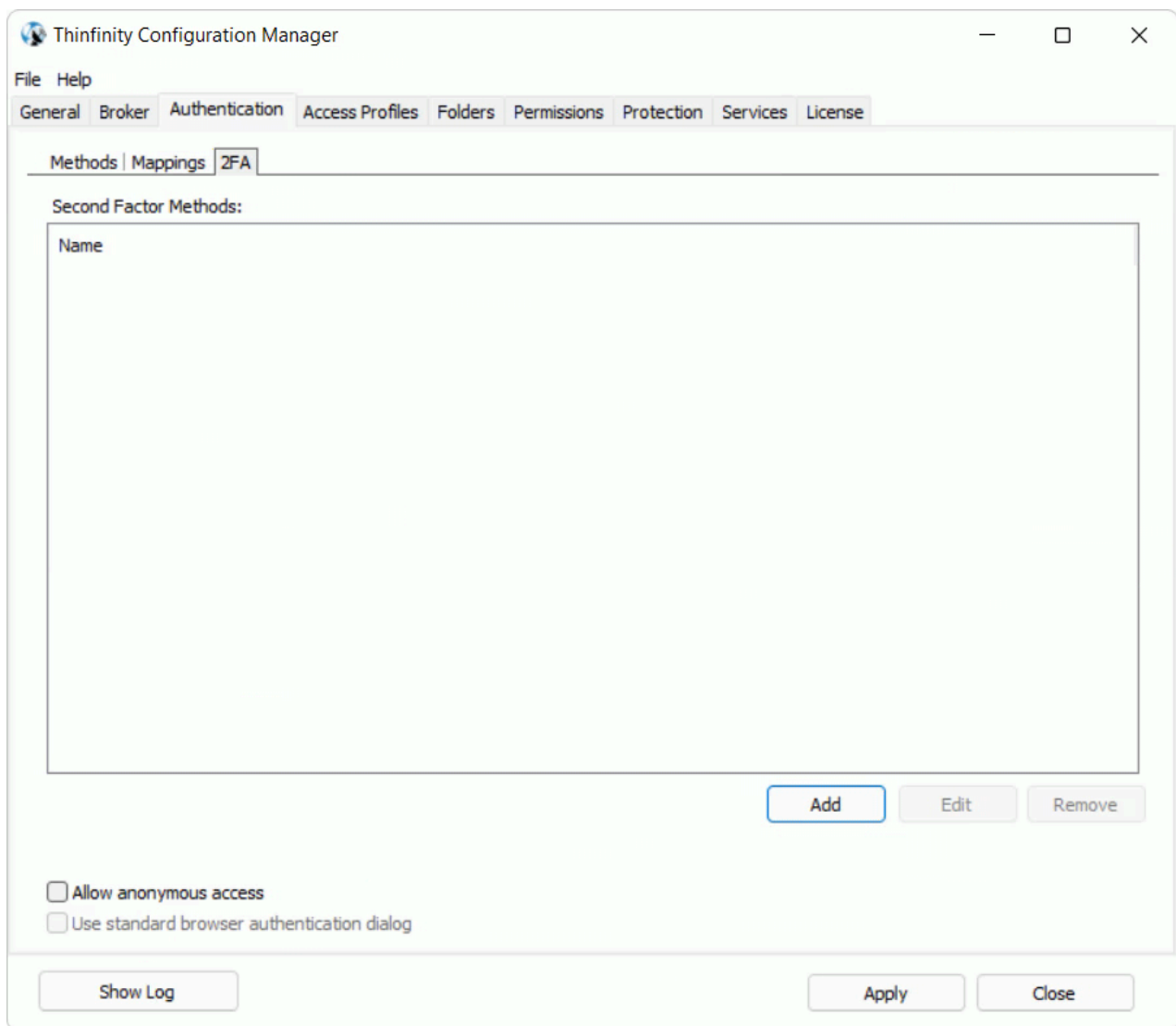
Choose between Radius, SAML, OAuth 2.0, or External DLL using the '*Add*' button on the '*Authentication*' tab.

- '*Mappings*' tab



OPTION	DESCRIPTION
Authentication ID Mask	Shows the list of Authentication Masks.
Associated Permissions	Assigns Active Directory permissions to the Authentication Masks.
Credentials	Specify Windows credentials.

- '2FA' tab



OPTION	DESCRIPTION
Second Factor Methods	Assign one of two 2FA methods available (TOTP, DUO)

Read more:

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

- [SAML](#)

- [TOTP](#)

Radius

Thinfinity® Remote Workspace's authentication can be integrated with a RADIUS account. On the links below you will find the information to set up Thinfinity® Remote Workspace to work with it.

Read more:

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

Settings

In the 'RADIUS' - 'Basic' section of the Thinfinity® Remote Workspace Configuration Manager's '*Authentications*' tab, you will find the following options:

Authentication Method Settings

Name: Radius

2FA Method: (none)

Server

Server IP: [] Port: 1812

Shared Secret: []

Authentication Type: PAP

Test Configuration

Ok Cancel

OPTION	DESCRIPTION
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

Test Configuration

methods.

Press this button to communicate with RADIUS and test the information entered in the above fields to see if it is correct.

Mappings

In the 'RADIUS' - '*Mappings*' section of the Thinfinity® Remote Workspace Configuration Manager's 'SSO' tab, you will link your RADIUS users to Active Directory users or groups. In this way, you tell Thinfinity® Remote Workspace 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. 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 '*Mappings*' 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.

The screenshot shows the 'Thinfinity Configuration Manager' window. The 'Authentication' tab is active, and the 'Mappings' sub-tab is selected. The 'Authentication ID Mask' section contains a text box with a key icon and '[*]:*'. A 'Switch base' button is located to the right of this section. Below the text box is an 'Enabled' checkbox and buttons for 'Import', 'Export', 'Add', and 'Remove'. The 'Associated Permissions' section is currently empty, with 'Add' and 'Remove' buttons at the bottom right. At the bottom of the window are checkboxes for 'Allow anonymous access' and 'Use standard browser authentication dialog', along with 'Show Log', 'Apply', and 'Close' buttons.

OPTION	DESCRIPTION
Switch Base	Press to change the order in which the ' <i>Authentication ID Mask</i> ' and the ' <i>Associated Permissions</i> ' boxes will be shown. This doesn't affect the configuration, only the view.
	<p>List of the remote users.</p> <p>Add: Add a new remote user (<u>SSO</u>). If the '<i>Authentication ID Mask</i>' box is above the the '<i>Associated Permissions</i>' box, you will then need to select it and add an Associated Permission to it. Otherwise, if the '<i>Authentication ID Mask</i>' box is below the '<i>Associated Permissions</i>' box, the remote user added will be mapped with the</p>

Authentication ID Mask

Active Directory User selected in the box above.

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.

Enabled: Select an user on the list and uncheck the '*Enabled*' field if you want to disable the access of this specific remote user.

List of Active Directory Users and Groups.

Associated Permissions

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.

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.

In the '*Credentials*' tab, you will find the following options:

The screenshot shows a dialog box titled 'Associated Permissions' with a 'Credentials' tab selected. Inside the tab, there are two input fields: 'Username:' and 'Password:'. To the right of the 'Username' field is a small button with three dots. Below the 'Password' field are two buttons: 'Test' and 'Remove'. At the bottom of the dialog, there are three buttons: 'Show Log', 'Apply', and 'Close'. There are also two checkboxes: 'Allow anonymous access' and 'Use standard browser authentication dialog'.

OPTION	DESCRIPTION
Username	Stores a valid Windows Username. Used when using an External Authentication and profiles with ' <i>Use the Authenticated Credentials</i> ' option.
Password	Stores a valid Windows Username's password. Used when using an External Authentication and profiles with ' <i>Use the Authenticated Credentials</i> ' option.
Test	Verifies the stored credentials.
Remove	Removes the stored credentials.

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

OAuth 2.0

Thinfinity® Remote Workspace Configuration Manager's 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 2.0 and complete your client ID and secret in [The 'Methods' tab](#). Click on 'Add', choose the authentication method you wish to configure. Finally, map the external users to Windows users in [The 'Mappings' tab](#).

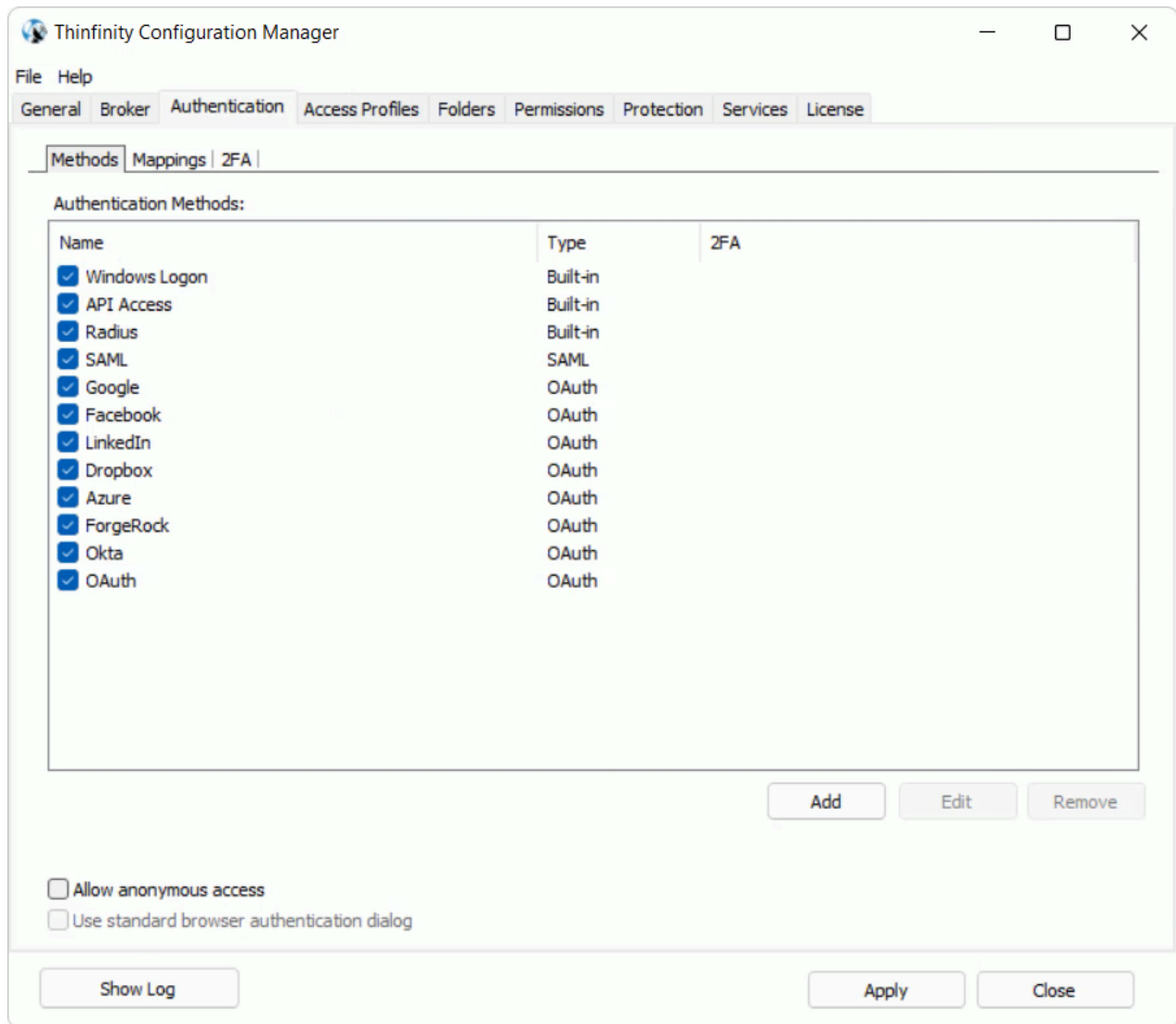
Note: Only when the '*Only use external authentication*' option in [the 'Authentication' tab](#) is checked and OAuth 2.0 is the only SSO method enabled in [the 'SSO' tab](#), a connection to the Thinfinity® Remote Workspace landing page or [virtual path](#) will be redirected to the OAuth 2.0 authentication and then return to the landing page or virtual path.

Read more:

- [More information on OAuth 2.0 authentication](#)
- [The 'Basic' tab](#)
- [The 'Server' tab](#)
- [The 'Mappings' tab](#)

Methods

In the 'OAuth 2.0' - '*Methods*' section of the Thinfinity® Remote Workspace Configuration Manager, you will find the following options:



OPTION	DESCRIPTION
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.

Settings

In the 'OAuth/2' - 'Settings' section of the Thinfinity® Remote Workspace Configuration Manager '*Authentication*' tab, you will find the following options:

General tab

Authentication Method Settings

×

Name: OAuth

Virtual Path: OAuth

2FA Method: (none) ▾

General

Server

Client ID: |

Client Secret:

Ok

Cancel

OPTION

DESCRIPTION

Client ID	<p>This client ID identifies Thinfinity® Remote Workspace in the OAuth Server.</p> <p>If you are using Google OAuth, it's the <u>Google Client ID</u> generated while configuring the Google account integration.</p>
Client Secret	<p>This client secret identifies Thinfinity® Remote Workspace in the OAuth Server.</p> <p>If you are using Google OAuth, it's the <u>Google Client Secret</u> 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 application. This option applies only to Google SSO Integration.</p>

Server tab

Authentication Method Settings

Name: OAuth

Virtual Path: OAuth

2FA Method: (none) ▾

General

Server

Authorization URL

Authorization parameters

Custom redirect URL

Token Validation Server URL

Token Validation extra parameters

Sign-Out URL:

User information

☒ Get from URL

☐ Get from Token

Profile information server URL

☒ Add default parameters

☐ Add custom parameters:

☐ Send Basic Authentication header

Login username value in returned JSON

Ok

Cancel

Server Kind	<p>Choose which kind of OAuth/2 Server you will be configuring.</p> <p>Select 'GOOGLE' to use Google OAuth 2.0 authentication, or CUSTOM to enter the parameters of another OAuth 2.0 server.</p>
Authorization URL	<p>This is the OAuth 2.0 server address where Thinfinity® Remote Workspace validates the corresponding OAuth 2.0 user. This address is used in combination with the values specified in the 'Other Keys...' field.</p>
Parameters (key1=value1&key2=value2&...)	<p>Complete other keys and their values following the query format specified. They will be sent to the authorization URL.</p> <p>Most of the times, the OAuth 2.0 servers require a scope that tells what user information Thinfinity® Remote Workspace needs access to in order to perform the user validation. The information specified here will be returned in the profile consultation.</p>
Token Validation Server URL	<p>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.</p>
Profile information server URL	<p>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.</p>
Login username value in returned JSON	<p>In here you can specify 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 'Mappings' tab.</p>

Mappings

In the '*OAuth/2*' - '*Mappings*' section of the Thinfinity® Remote Workspace Configuration Manager's '*Authentication*' tab, you will link your OAuth/2 users to Active Directory users or groups. In this way, you tell Thinfinity® Remote Workspace 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.

Thinfinity Configuration Manager

File Help

General Broker Authentication Access Profiles Folders Permissions Protection Services License

Methods Mappings 2FA

Authentication ID Mask Switch base

[*]:*

☒ Enabled Import Export Add Remove

Associated Permissions Credentials

Add Remove

☐ Allow anonymous access
☐ Use standard browser authentication dialog

Show Log Apply Close

OPTION	DESCRIPTION
Switch Base	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>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</p>

Authentication ID Mask

Active Directory User selected in the box above.

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.

Enabled: Select an user on the list and uncheck the 'Enabled' field if you want to disable the access of this specific remote user.

List of Active Directory Users and Groups.

Associated Permissions

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.

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.

In the 'Credentials' tab, you will find the following options:

The screenshot shows a dialog box titled 'Associated Permissions' with a 'Credentials' tab selected. Inside the tab, there are two input fields: 'Username:' and 'Password:'. To the right of the 'Username' field is a button with three dots (...). Below the 'Password' field are two buttons: 'Test' and 'Remove'. At the bottom of the dialog, there are three buttons: 'Show Log', 'Apply', and 'Close'. There are also two checkboxes: 'Allow anonymous access' and 'Use standard browser authentication dialog'.

OPTION	DESCRIPTION
Username	Stores a valid Windows Username. Used when using an External Authentication and profiles with "Use the Authenticated Credentials" option.
Password	Stores a valid Windows Username's password. Used when using an External Authentication and profiles with "Use the Authenticated Credentials" option.
Test	Verifies the stored credentials.
Remove	Removes the stored credentials.

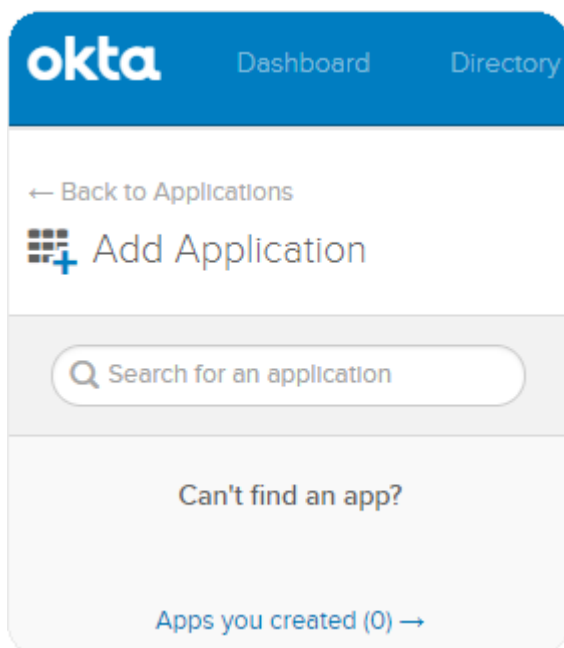
Always remember to press '*Apply*' in order to save the changes.

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 Workspace:

- Navigate to your Okta space, go to the Applications tab, and create a new application using the '*Create New App*' button:



- Select '*OpenID Connect*' as the Authentication Method:

Create a New Application Integration

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

- Give the application a name, and type in the URL you use to reach Thinfinity® Remote Workspace. Then press 'Save':

Create OpenID Connect Integration

GENERAL SETTINGS

Application name

Thinfinity Login

Application logo (Optional) ?

Browse files...

CONFIGURE OPENID CONNECT

Login redirect URIs ?

https://MyWebsite.com

+ Add URI

Logout redirect URIs ?

+ Add URI

Save

Cancel

- 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® Remote Workspace website address and *"/Okta"* at the end of the URL:

LOGIN

Login redirect URIs ?

https://MyWebsite.com

X

+ Add URI

Logout redirect URIs ?

+ Add URI

Login initiated by

App Only

▼

Initiate login URI

https://MyWebsite.com\Okta

- Copy and paste both '*Client ID*' and '*Client Secret*' for future references:

Client Credentials

Edit

Client ID

Ooa243zhoFVbu8SH4356

📋

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

Client secret

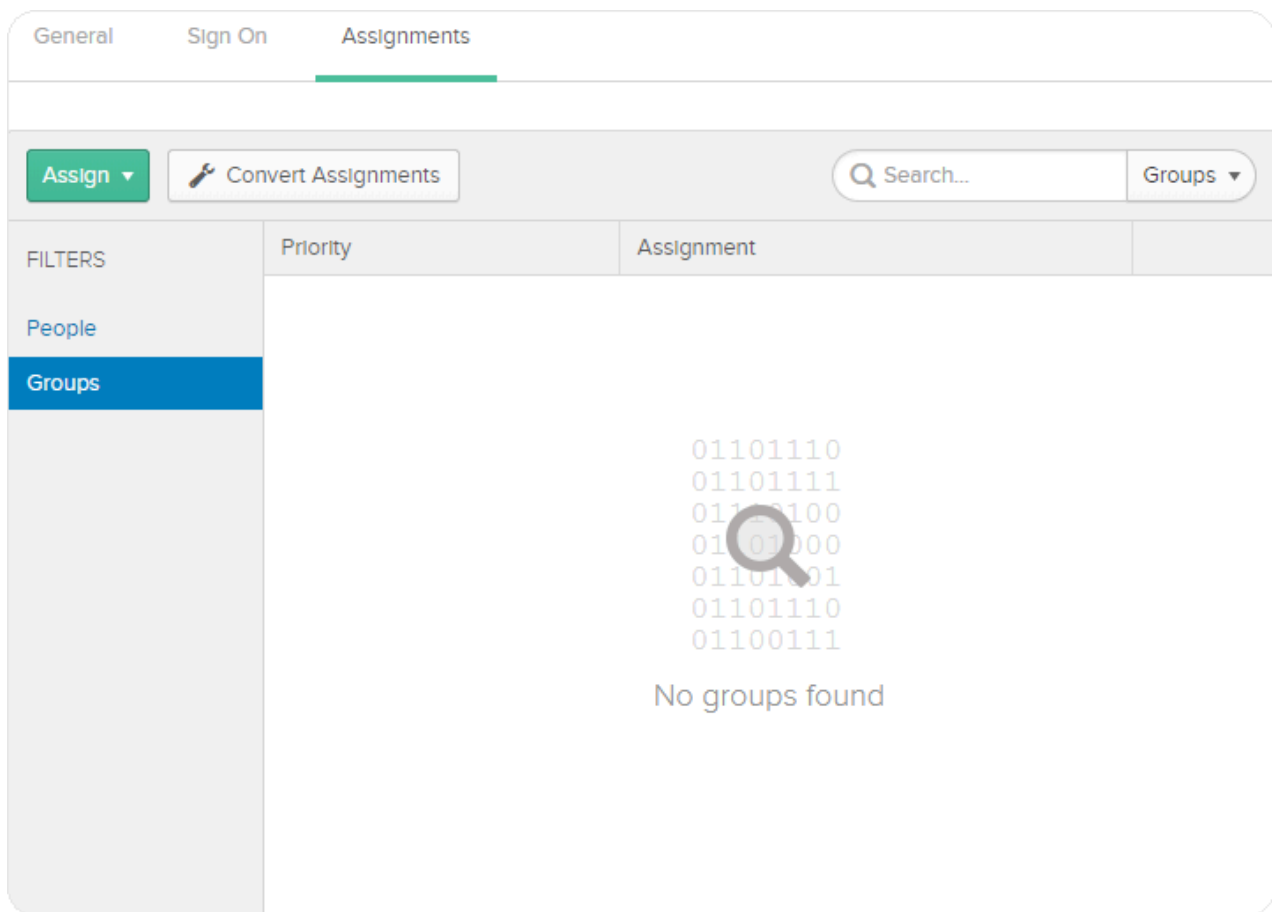
.....

👁

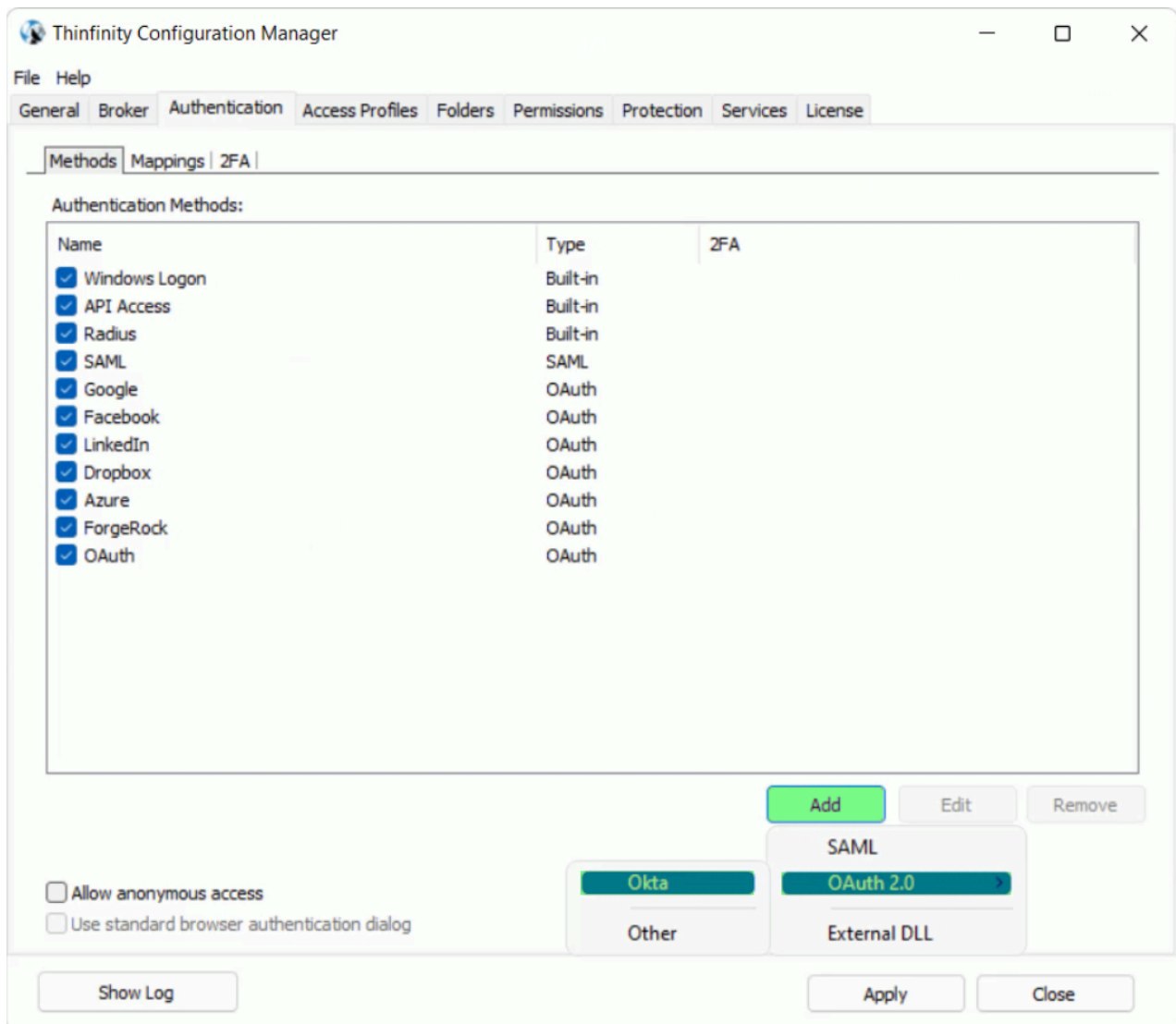
📋

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.

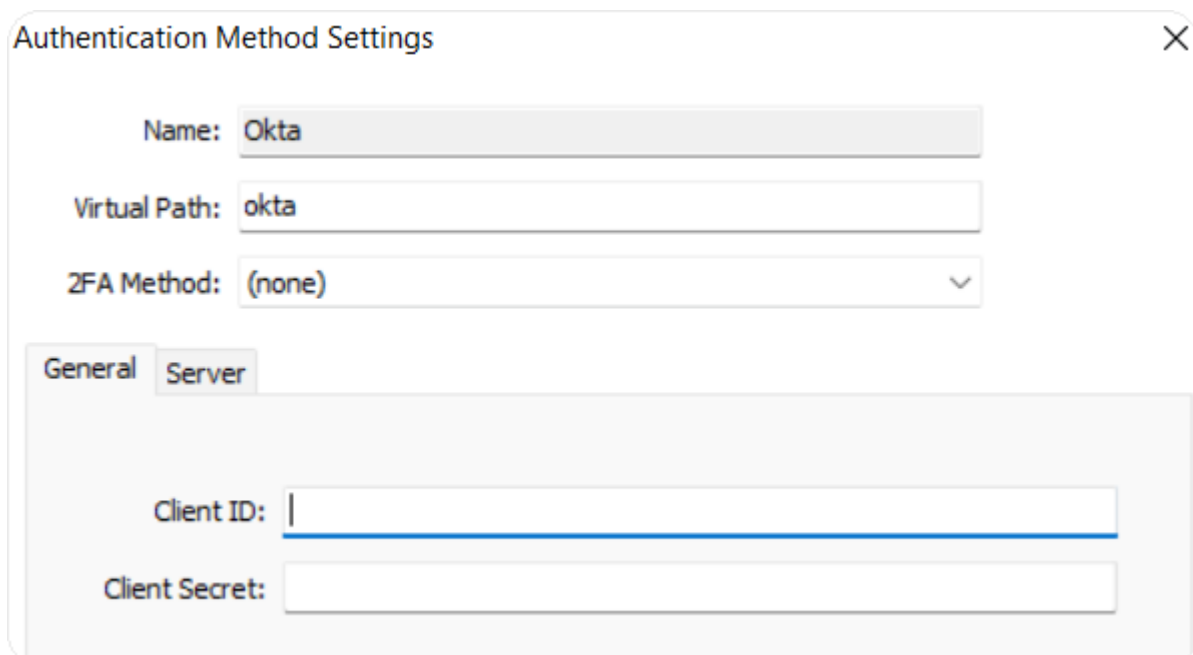
- Click on the '*Assignments*' tab and add your users to the Application:



- Now, open the Thinfinity® Remote Workspace Configuration Manager and navigate to the 'Authentication' tab. Click on OAuth 2.0 and choose 'Okta':



- Enter your '*Client ID*' and '*Client Secret*':



- 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)

Authentication Method Settings

✕

Name: Okta

Virtual Path: okta

2FA Method: (none) ▾

General

Server

Authorization URL

https://[MyOktaSpace].okta.com/oauth2/v1/authorize|

Authorization parameters

scope=openid+profile+offline_access&state=okta

Custom redirect URL

Token Validation Server URL

https://[MyOktaSpace].okta.com/oauth2/v1/token

Token Validation extra parameters

https://[MyOktaSpace].okta.com/oauth2/v1/userinfo

Sign-Out URL:

User information

☒ Get from URL

☐ Get from Token

Profile information server URL

https://[MyOktaSpace].okta.com/oauth2/v1/userinfo

☐ Add default parameters

☒ Add custom parameters:

☐ Send Basic Authentication header

Login username value in returned JSON

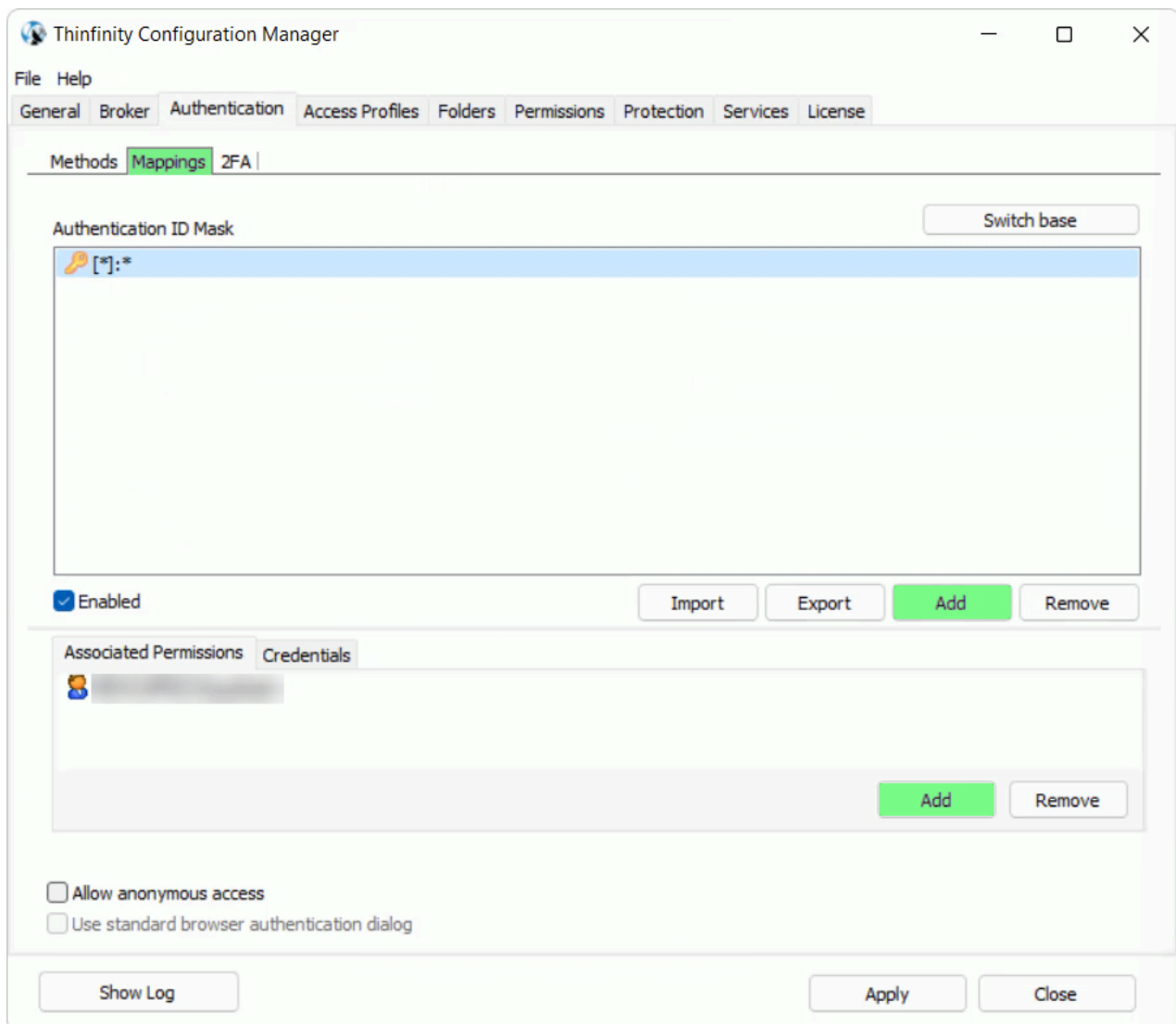
preferred_username

Ok

Cancel

Press 'OK' after you finish configuring the Authentication Method

- 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.

- Navigate to the Thinfinity® Remote Workspace landing page, and you should see the '*Sign in with Okta*' option listed as an Authentication Method:



Enter your credentials


Username

Password



Sign in

Or

 Sign in with Okta

Configure OAuth with Auth0

This tutorial will show you how to enable 2FA using Auth0 with Thinfinity® Remote Workspace.

Auth0 Guardian mobile application is required for 2FA.

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


Create Application

Name

MyThinfintyOAuth

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


Choose an application type



Native

Mobile or Desktop,
apps that run natively
in a device.


eg: iOS SDK



Single Page Web
Applications

A JavaScript front-end
app that uses an API.


eg: AngularJS +
NodeJS



Regular Web
Applications

Traditional web app
(with refresh).

eg: Java ASP.NET



Machine to
Machine
Applications

CLI, Daemons or
Services running on
your backend.

eg: Shell Script

CREATE

- Copy your 'Client ID' and 'Client Secret':

115

Name	<input type="text" value="MyThinfinityOAuth"/>	
Domain	<input type="text" value="cybelesoft.auth0.com"/>	
Client ID	<input type="text" value=""/>	
Client Secret	<input type="password" value="*****"/>	

☐ Reveal client secret.

The Client Secret is not base64 encoded.

- In the '*Allowed Callback URLs*', 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	<input type="text" value="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.

- To enable 2FA , click on the '*Multifactor Auth*' and enable '*Push Notifications*':

The screenshot shows the 'Multifactor Auth With Guardian' settings page in the Thinfinity Configuration Manager. On the left is a sidebar with navigation links: Dashboard, Applications, APIs, SSO Integrations, Connections, Users, Rules, Hooks, Multifactor Auth (highlighted), Hosted Pages, Emails, and Logs. The main content area has a title 'Multifactor Auth With Guardian' and a warning box stating: 'Use of this feature requires the purchase of an addon to your Auth0 subscription. Please contact us with any questions.' Below this is a description: 'Adds an additional factor to conventional logins to prevent unauthorized access. Use Push Notifications, SMS or both. [Learn more](#)'. There are two toggle switches: 'Push Notifications' (turned on) and 'SMS' (turned off). A note at the bottom says: 'Auth0 also supports Google Authenticator and Duo. If you use any of these, click here [to configure them](#).'

- Open the Thinfinity® Remote Workspace Configuration Manager, navigate to the 'Authentication' tab, press 'Add' → 'OAuth2.0' → 'Other':

The screenshot shows the 'Thinfinity Configuration Manager' window with the 'Authentication' tab selected. The 'Methods' sub-tab is active, displaying a table of authentication methods. The table has columns for 'Name', 'Type', and '2FA'. All methods listed are checked. Below the table are checkboxes for 'Allow anonymous access' and 'Use standard browser authentication dialog'. At the bottom right, there are 'Add', 'Edit', and 'Remove' buttons. The 'Add' button is highlighted, and a dropdown menu is open showing 'SAML', 'OAuth 2.0' (selected), and 'External DLL'. There is also an 'Other' button next to the dropdown. At the bottom of the window are 'Show Log', 'Apply', and 'Close' buttons.

Name	Type	2FA
<input checked="" type="checkbox"/> Windows Logon	Built-in	
<input checked="" type="checkbox"/> API Access	Built-in	
<input checked="" type="checkbox"/> Radius	Built-in	
<input checked="" type="checkbox"/> SAML	SAML	
<input checked="" type="checkbox"/> Google	OAuth	
<input checked="" type="checkbox"/> Facebook	OAuth	
<input checked="" type="checkbox"/> LinkedIn	OAuth	
<input checked="" type="checkbox"/> Dropbox	OAuth	
<input checked="" type="checkbox"/> Azure	OAuth	
<input checked="" type="checkbox"/> ForgeRock	OAuth	
<input checked="" type="checkbox"/> Okta	OAuth	

- Add the following information:

Authentication Method Settings

Name: OAuth

Virtual Path: OAuth

2FA Method: (none)

General

Server

Authorization URL

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

Authorization parameters

scope=openid+email

Custom redirect URL

Token Validation Server URL

https://[MyDomain].auth0.com/token

Token Validation extra parameters

Sign-Out URL:

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

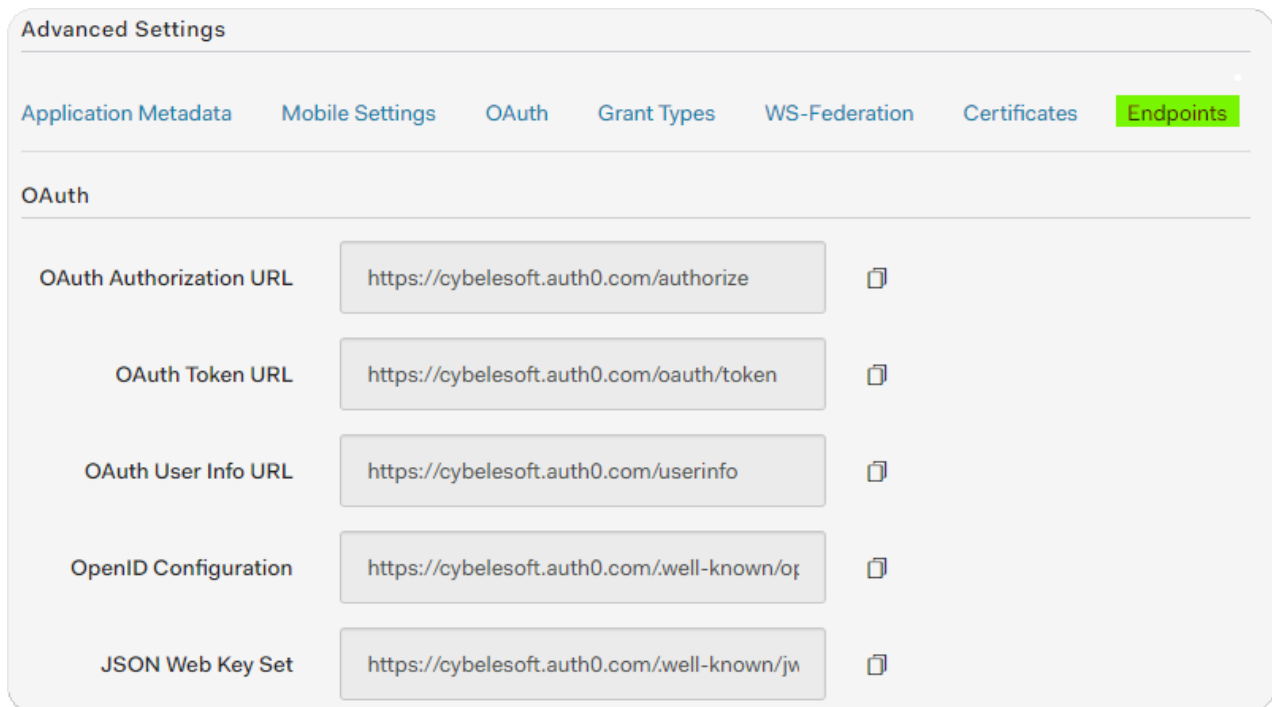
Login username value in returned JSON

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

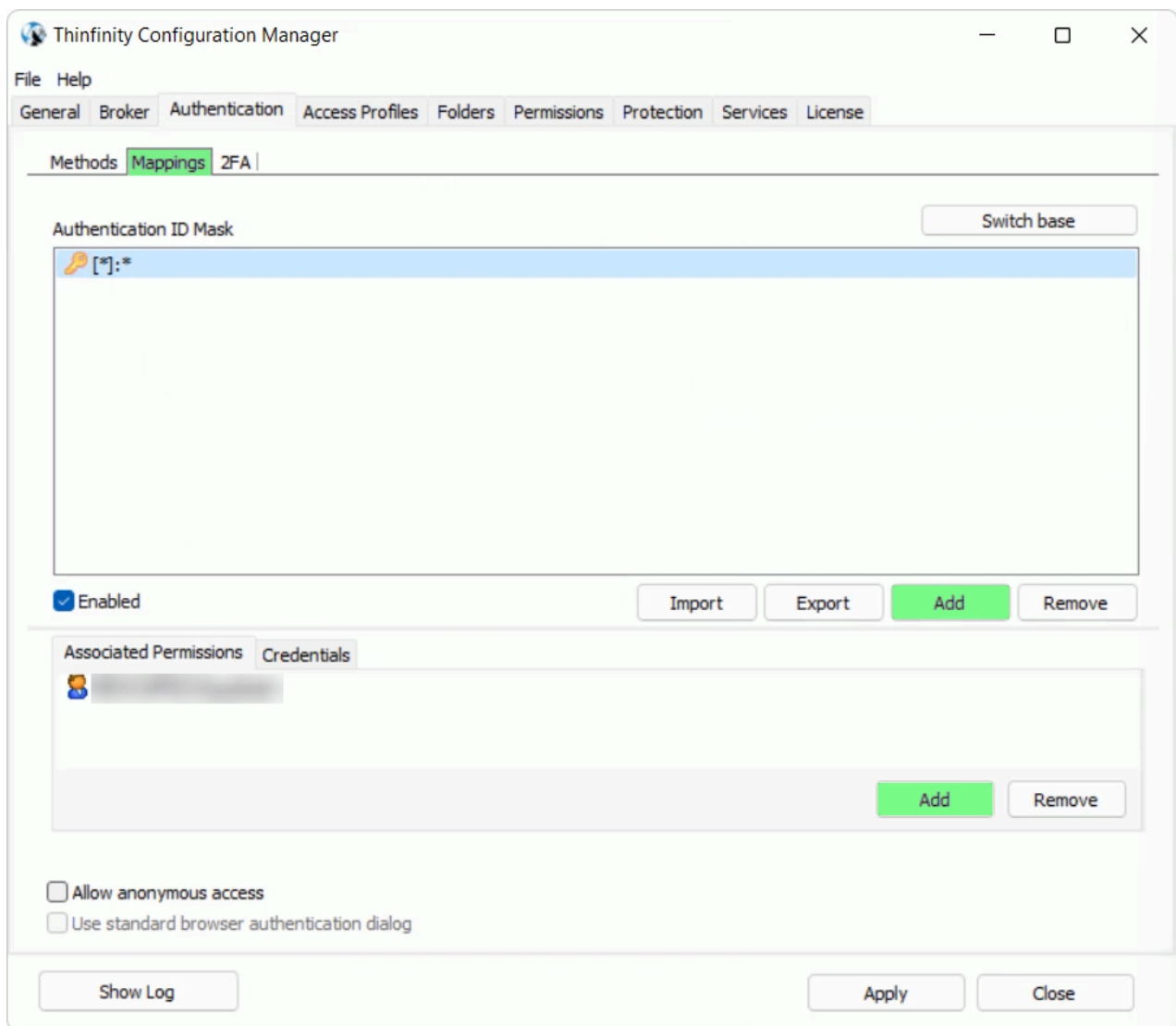
Application Metadata Mobile Settings OAuth Grant Types WS-Federation Certificates **Endpoints**

OAuth

OAuth Authorization URL	https://cybelesoft.auth0.com/authorize	
OAuth Token URL	https://cybelesoft.auth0.com/oauth/token	
OAuth User Info URL	https://cybelesoft.auth0.com/userinfo	
OpenID Configuration	https://cybelesoft.auth0.com/.well-known/openid-configuration	
JSON Web Key Set	https://cybelesoft.auth0.com/.well-known/jwks.json	

Click on '*Ok*' after you entered the information.

- 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.
- Navigate to the Thinfinity® Remote Workspace landing page, and you should see the 'Sign in with OAuth' option listed as an Authentication Method:



Enter your credentials

Username

Password



Sign in

Or

Sign in with OAuth

TOTP (Time-based One-time Password)

Thinfinity® Remote Workspace's authentication can be integrated with a TOTP (Time-based One-time Password) app. On the link below, you will find the information to set up Thinfinity® Remote Workspace to work with it:

[TOTP Settings](#)

TOTP Settings

In the '2FA' section of the Thinfinity® Remote Workspace Configuration Manager's 'Authentication' tab, you will find the following options:

The screenshot shows the 'Thinfinity Configuration Manager' window. The 'Authentication' tab is selected, and the '2FA' sub-tab is active. The 'Second Factor Methods' section contains a large text area labeled 'Name'. Below this text area are three buttons: 'Add' (highlighted in green), 'Edit', and 'Remove'. Below the 'Add' button is a dropdown menu with 'TOTP' and 'DUO' options. At the bottom left, there are two checkboxes: 'Allow anonymous access' and 'Use standard browser authentication dialog'. At the bottom right, there are three buttons: 'Show Log', 'Apply', and 'Close'.

OPTION	DESCRIPTION
Issuer	Enter the name you want the TOTP method to have on your TOTP application.
Google Authenticator Compatible	Enable this option for making the TOTP method Google Authenticator compatible.

TOTP - Settings

✕

Issuer:

Thinfinity Remote Workspace

☒

Google Authenticator compatible

Digits:

6 digits

▼

Algorithm:

SHA-1

▼

Precision:

30 seconds

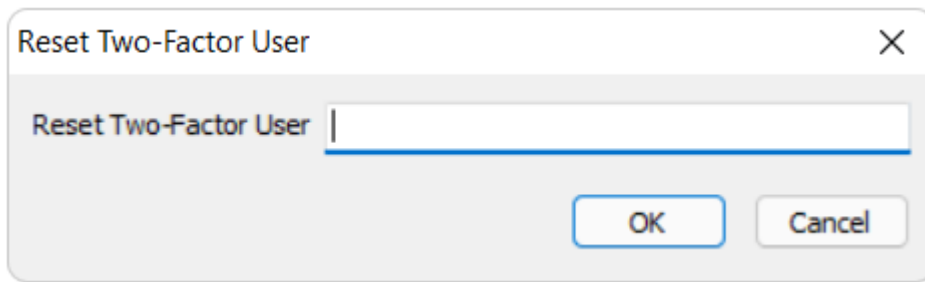
▼

Reset 2FA key for user

Ok

Cancel

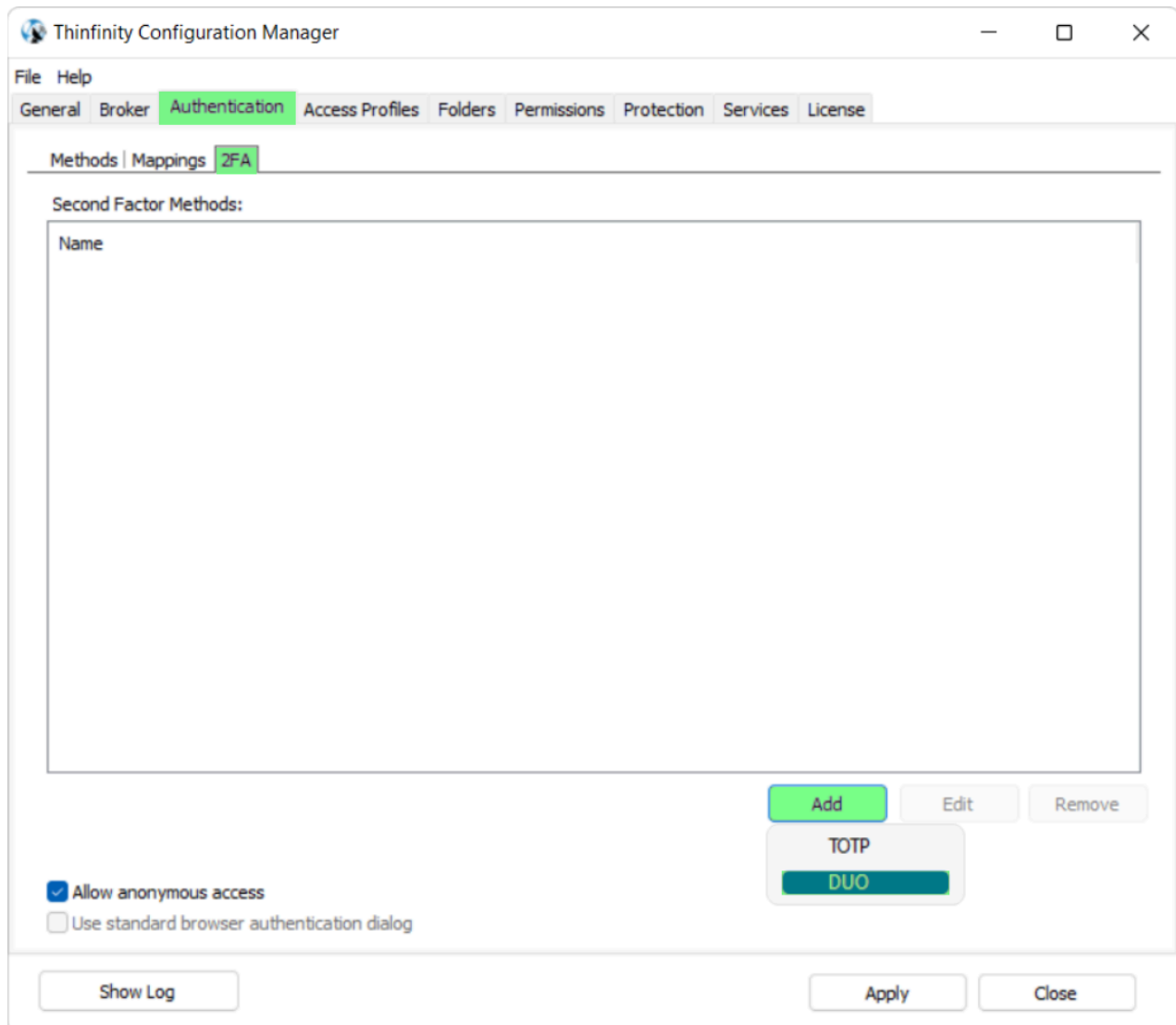
OPTION	DESCRIPTION
Issuer	Enter the name you want the TOTP method to have on your TOTP application.
Google Authenticator Compatible	Enable this option for making the TOTP method Google Authenticator compatible.
Digits	Choose the amount of digits you want the TOTP to accept.
Algorithm	Choose the algorithm to be used by the TOTP method
Precision	Choose the amount of seconds for the TOTP token to be valid.
Reset 2FA key for user	Reset the Two Factor Authentication method for a specific user.



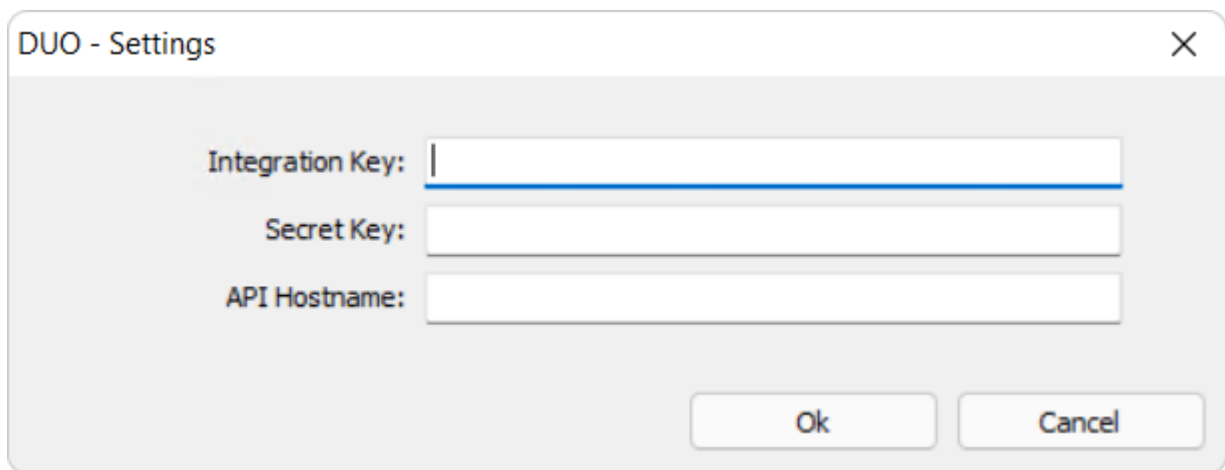
OPTION	DESCRIPTION
Reset Two-Factor User	Enter the user you want to release the device registered to it's name, so it can be re-registered on a different device.

DUO Authentication Method Settings

You can access this configuration by going to the '*Authentication*' tab, then go to the '*2FA*', click on '*Add*' and select '*DUO*'



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

A screenshot of a 'DUO - Settings' dialog box. It has a title bar with a close button (X) in the top right corner. The dialog contains three text input fields: 'Integration Key:', 'Secret Key:', and 'API Hostname:'. The 'Integration Key' field is currently active, indicated by a blue cursor. At the bottom right, there are two buttons: 'Ok' and 'Cancel'.

OPTION	DESCRIPTION
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 Workspace:

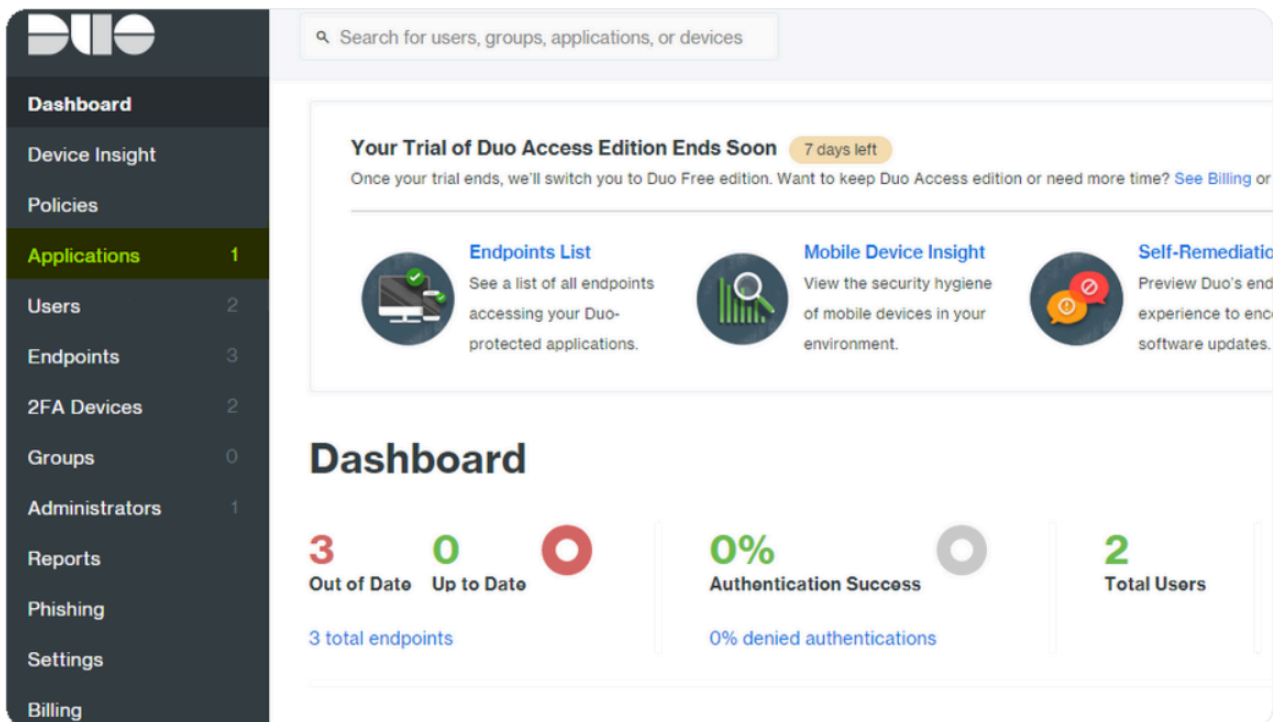
- [How to configure DUO](#)

How to configure DUO

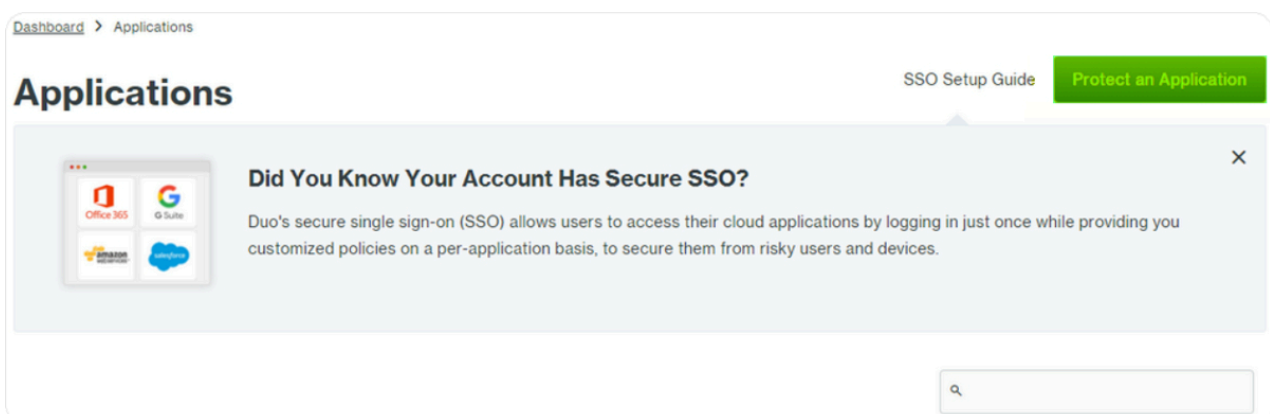
To configure DUO's Two-Factor authentication, please follow these steps :

On DUO's Web Interface :

- Navigate to the Applications tab on Duo's administrator website



- Click on "Protect an Application"



- 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](#)

- 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	WWHEZXD
Secret key	Click to view.
Don't write down your secret key or share it with anyone.	
API hostname	.duosecurity.com

- Now open the Thinfinity® Configuration Manager, navigate to the 'Authentication' tab, click on '2FA', then on 'Add' and then select 'DUO'

The screenshot shows the Thinfinity Configuration Manager application window. The 'Authentication' tab is selected, and the '2FA' sub-tab is active. The 'Second Factor Methods' section is empty, with a table header 'Name'. Below the table are 'Add', 'Edit', and 'Remove' buttons. A dropdown menu is open, showing 'TOTP' and 'DUO' options. At the bottom left, there are checkboxes for 'Allow anonymous access' (checked) and 'Use standard browser authentication dialog' (unchecked). At the bottom right, there are 'Show Log', 'Apply', and 'Close' buttons.

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

The screenshot shows the 'DUO - Settings' dialog box. It contains three input fields: 'Integration Key:', 'Secret Key:', and 'API Hostname:'. At the bottom right, there are 'Ok' and 'Cancel' buttons.

- Navigate to the Thinfinity® Remote Workspace login page and enter valid credentials



Enter your credentials

Username

Password



Sign in

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



[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.

SAML Authentication Method Settings

When you use SAML as an authentication method, you need to set some parameters:

Authentication Method Settings

Name: SAML

Virtual Path: SAMLAssertionConsumerService

2FA Method: (none) ▾

General

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: ...

Ok

Cancel

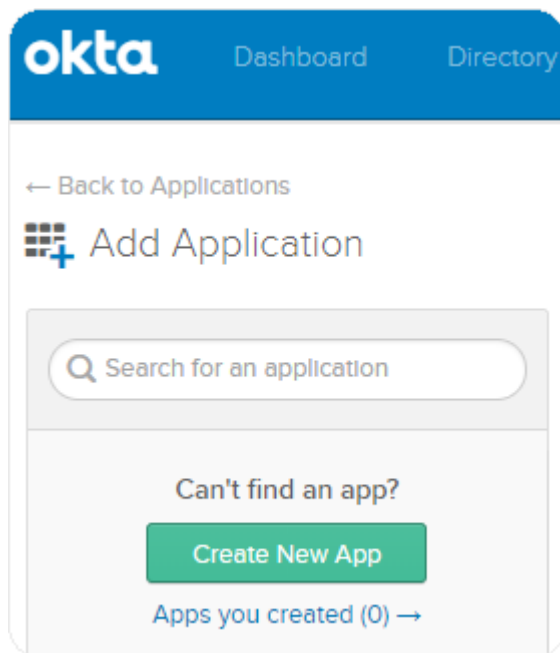
In the following topic we'll cover how to properly configure SAML with Okta as an authentication method using Thinfinity® Remote Workspace:

- [Configure SAML with Okta](#)

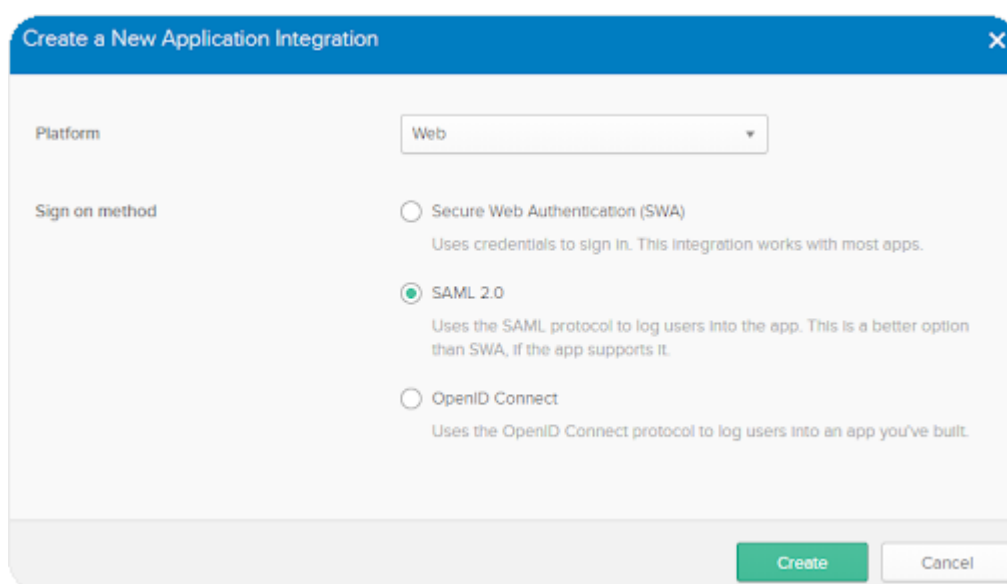
Configure SAML with Okta

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

- Navigate to your Okta space, go to the Applications tab, and create a new application using the 'Create New App' button



- Chose 'SAML 2.0' as the Authentication Method



- Assign a name to the application


1

General Settings

App name

Thinfinty SAML

App logo (optional) ?



Browse..

Upload Logo

App visibility

☐ Do not display application icon to users

☐ Do not display application icon in the Okta Mobile app

Cancel

Next

- Configure the '*Single sign-on URL*' and '*Audience URI*'

A

SAML Settings

GENERAL

Single sign on URL ?

https://[MyThinfintyWebSite]/SAMLAssertionConsumerService

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

https://[MyThinfintyWebSite]

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Unspecified ▼

Application username ?

Okta username ▼

Show Advanced Settings

The '*Single Sign-on URL*' address should be the following :
'https://[MyThinfintyWebSite]/SAMLAssertionConsumerService'

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

- 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

i

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

- 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

The following is needed to configure Thinfinity SAML

1 Identity Provider Single Sign-On URL:

`https://cybelesoft[REDACTED].okta.com/app/[REDACTED]/sso/saml`

2 Identity Provider Issuer:

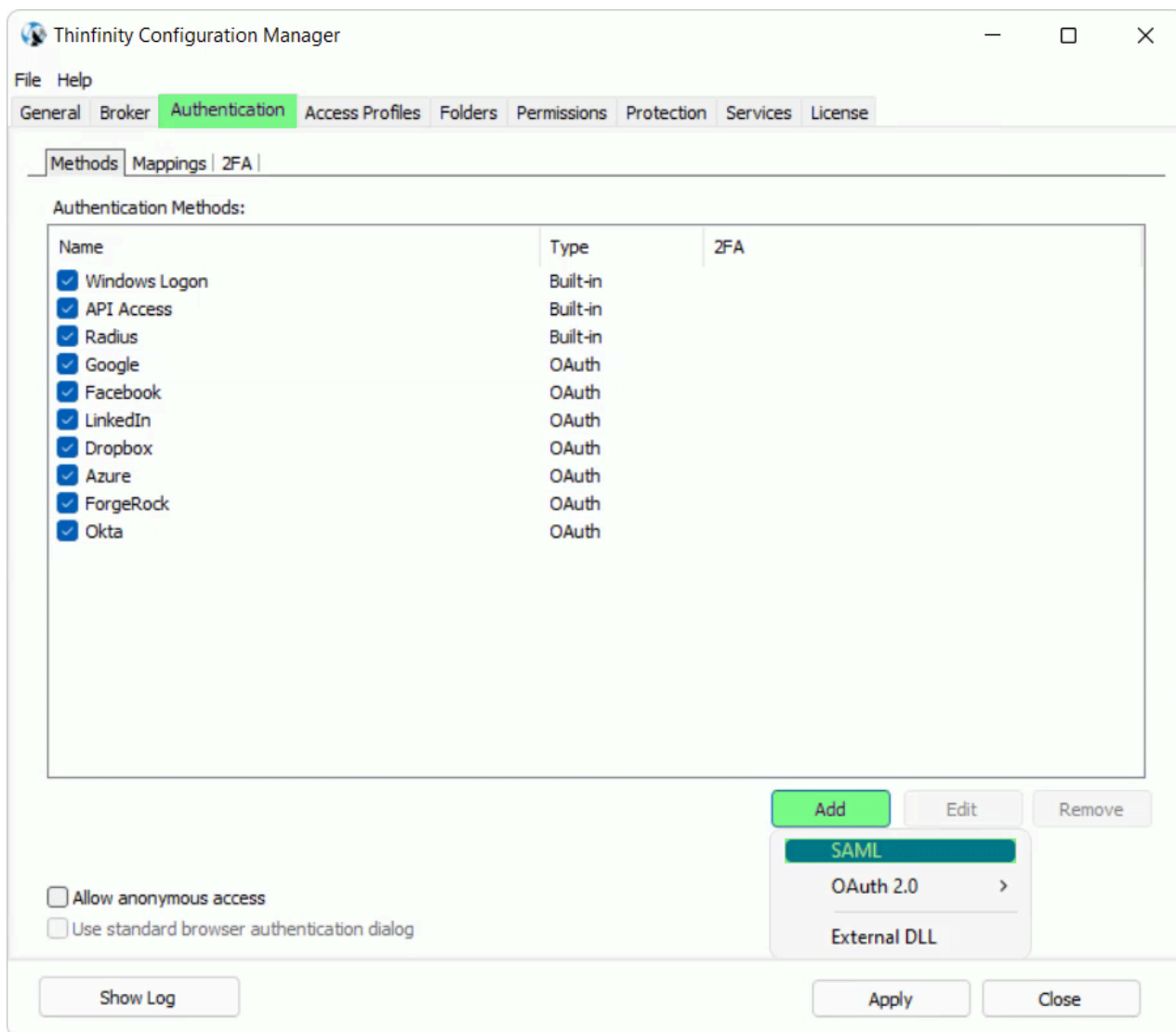
`http://www.okta.com/exk[REDACTED]`

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDrjCCApagAwIBAgIGAWYvxQzxMA0GCSqGSIb3DQEBCwUAMIGXMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxDGAWBgNVBAMMD2N5YmVsZXNvZnQtdTEcMBoGCSqGSIb3
[REDACTED]
YRp9mdgFVAAfU1JwGPBUsoVLbCXe30+dt5NknuEyxrDKg==
-----END CERTIFICATE-----
```

[Download certificate](#)

- Now, open the Thinfinity® Configuration Manager, navigate to the 'Authentication' tab, press the 'Add' option and click on 'SAML':



- 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.
 Identification 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:

Authentication Method Settings

×

Name: Okta SAML

Virtual Path: SAMLAssertionConsumerService1

2FA Method: (none) ▾

General

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

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

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

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

☐ Sign Authentication Request

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

Sign-Out URL:

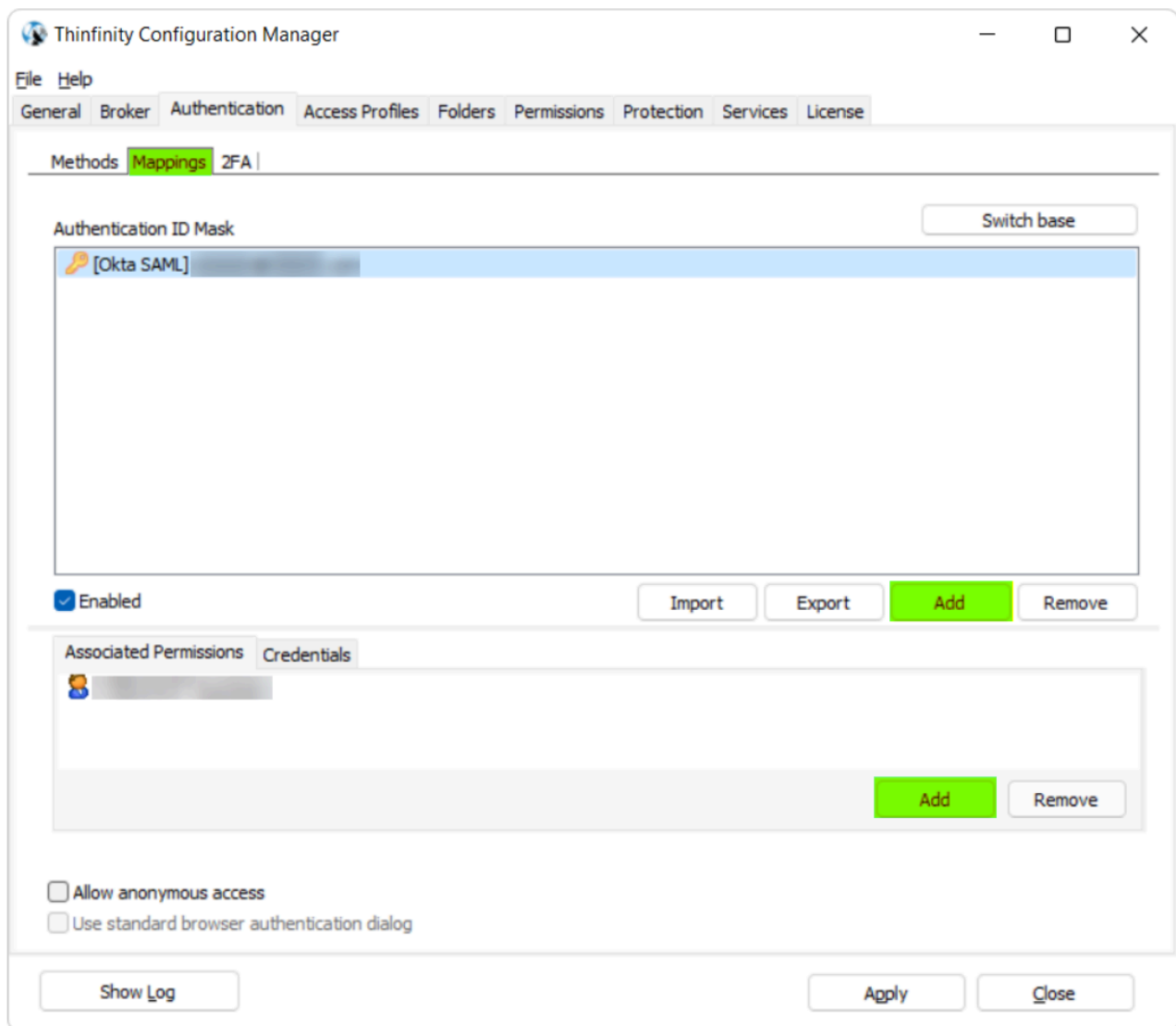
Partner Certificate File: C:\Temp\okta.cert ...

Ok

Cancel

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

- Click on the 'Mappings' tab. You can add the email address of the Okta user you want to validate under the 'Authentication ID Mask' section, by pressing 'Add'. Then you can add the Active Directory User on the 'Associated Permissions' section, also by pressing 'Add':



- After you add the appropriate mappings, click on the 'Apply' button.
- Navigate to the Thinfinity® Remote Workspace landing page, and you should see the 'Sign in with Okta SAML' option listed as an Authentication Method:



Enter your credentials

Username

Password



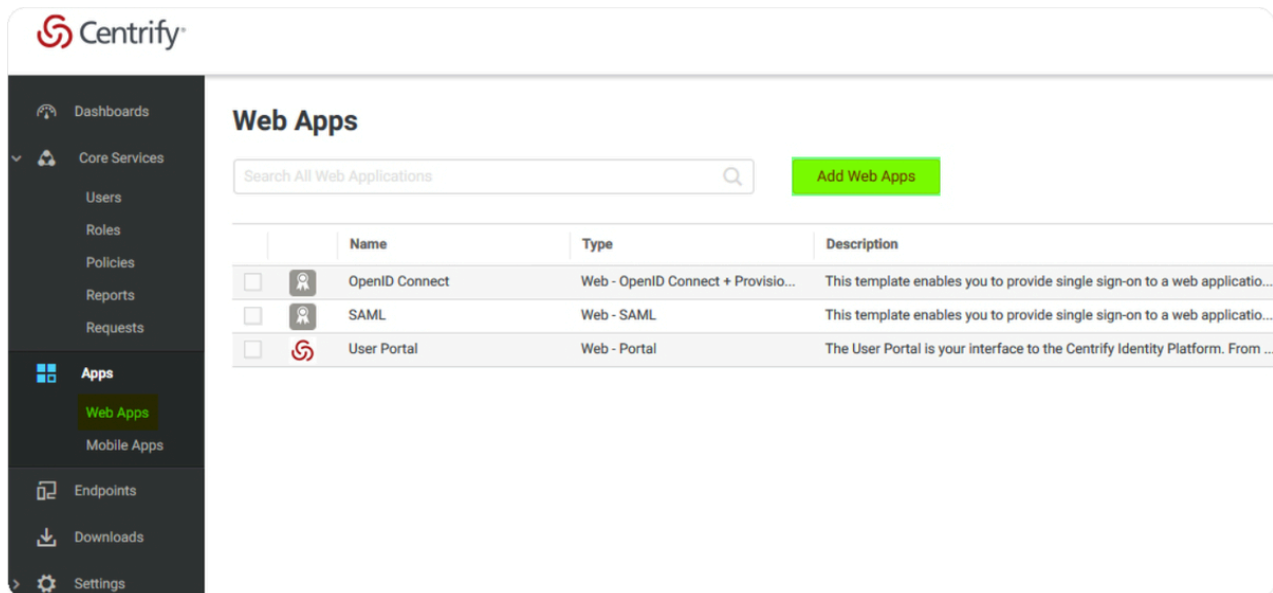
Sign in

Or

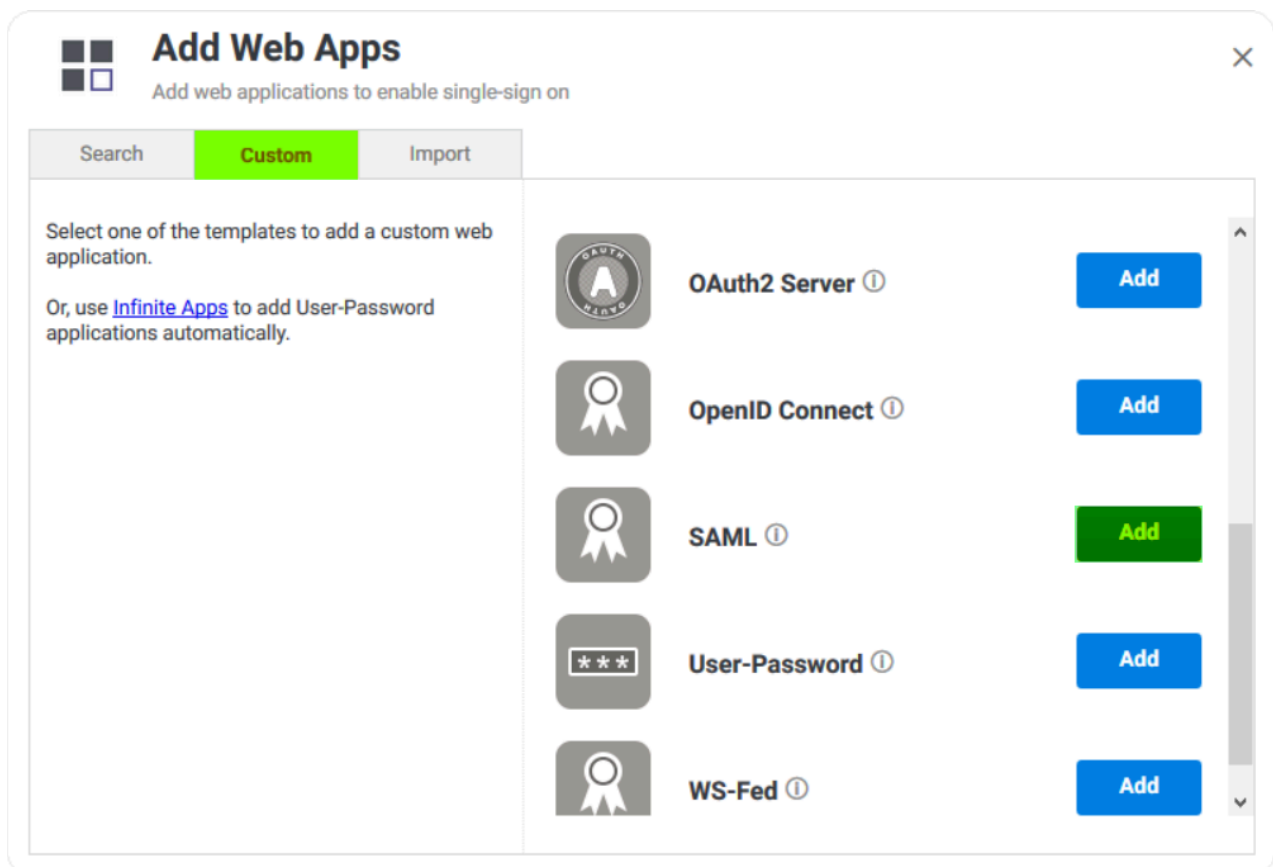
Sign in with Okta SAML

Configure SAML with Centrify

- On the Centrify's Admin Portal. Click on Apps → Web Apps



- Click on Custom and next to SAML, press Add



- 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 your SAML Service Provider.

IdP Entity ID / Issuer ⓘ

Signing Certificate ⓘ

Thumbprint:

Subject: CN=Centrify Customer AAZ0594 Application Signing Certificate

Algorithm: sha256RSA

Expires: 12/31/2038 9:00:00 PM

- Click on Manual Configuration, and copy the IdP Entity ID, and download the certificate provided by Centrify, then copy the Single Sign on URL, and the Single Logout URL

Single Sign On URL ⓘ

Single Logout URL ⓘ

Single Sign On Error URL ⓘ

- 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 ⓘ

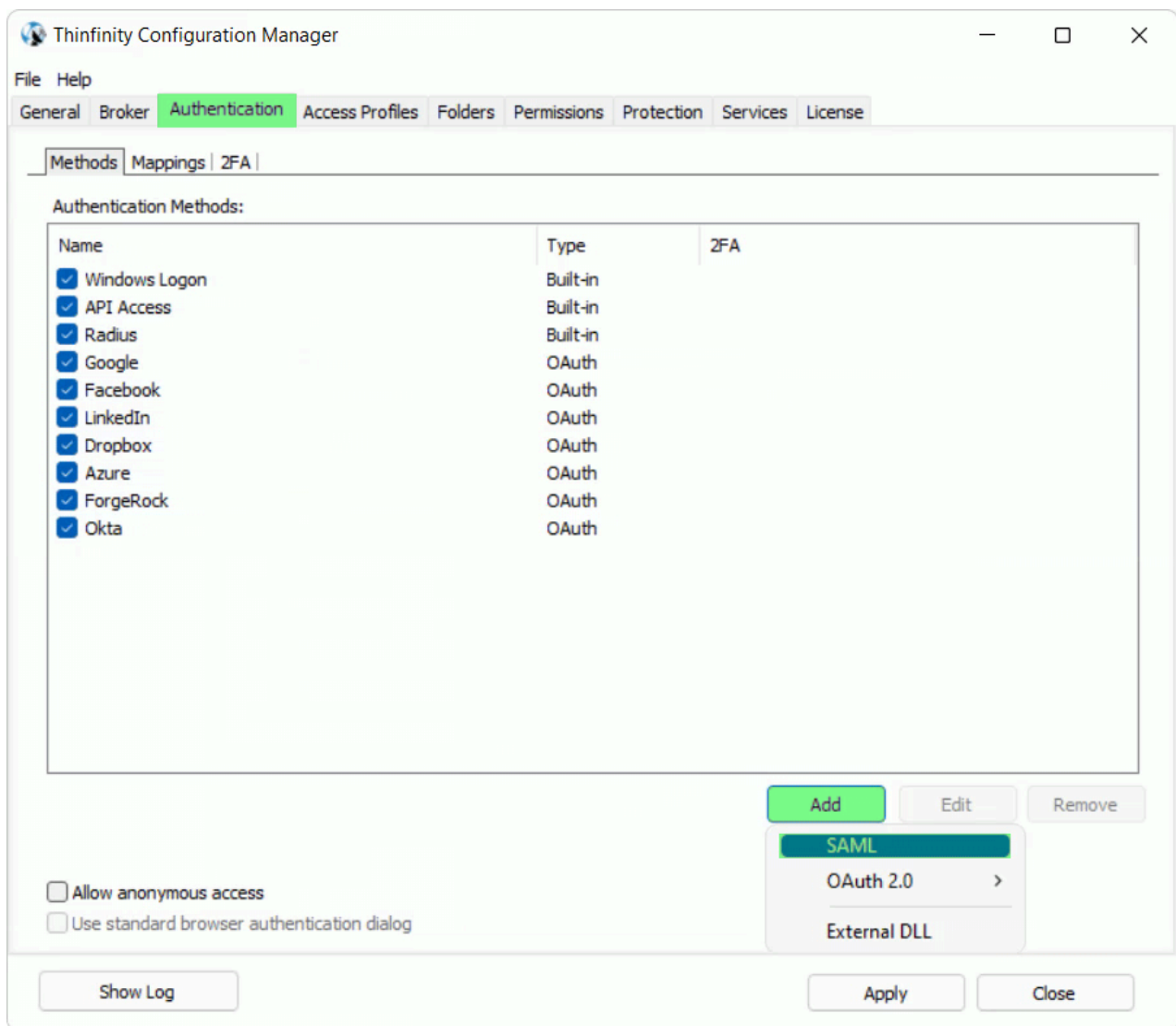
https://YourThinfinitySite:[Port]/SAMLAssertionConsumerService

Recipient * ⓘ ☒ Same as ACS URL

- After doing these changes, click on the Save button.

Now we need to configure Thinfinity® Remote Workspace with all this information.

- Open the Thinfinity® Configuration Manager and navigate to the Authentication tab, press Add, and then SAML:



- Now we must configure the connection itself:

Authentication Method Settings

×

Name: SAML

Virtual Path: SAMLAssertionConsumerService

2FA Method: (none) ▾

General

Service Identifier: https://YourThinfinitySite:[Port]

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

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

Identification Entity ID: https://pod4.centrixy.com/

☐ Sign Authentication Request

Single Sign-On Service URL: https://.my.centrixy.com/applogin/appkey/fc

Sign-Out URL: https://.my.centrixy.com/applogout/appkey/

Partner Certificate File: C:\Temp\Centrixy SHA256 Tenant Signing Certifi ...


Ok

Cancel

```
Service identifier = https://YourThinfinitySite:[Port]
Service Cert File = [Path_To_Your_Certificate]
Service Cert Pass = [Certificate_Password]
Identification Entity = [IdP Entity ID / Issuer]
Single Sing on Service URL = [Single Sign on URL]
Sign-out URL = [Single Logout URL]
Partnet Cert File = [Certificate Provided by Centrixy]
```

Once you configured it properly, click "Ok" and then "Apply".


- Now go the Thinfinity® Remote Workspace landing page and you should see the Sign in with SAML option now available to use:



Enter your credentials


Username

Password



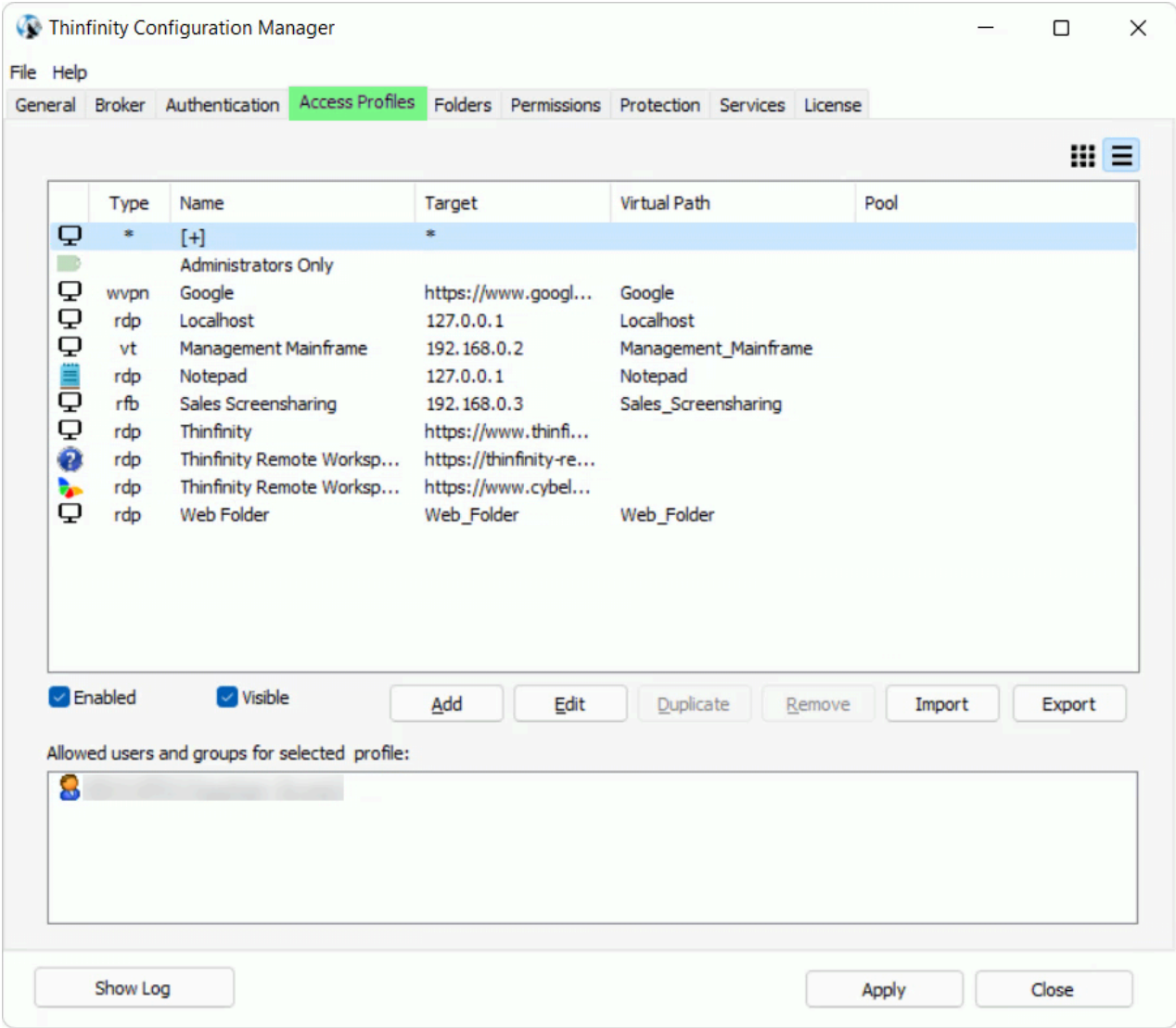
Sign in

Or

 Sign in with SAML

Access Profiles

Under the 'Access Profiles' tab of the Thinfinity® Remote Workspace Configuration Manager, you are able to tailor these profiles and let users seamlessly and safely connect to their desktops or applications via RDP, VNC/RFB, Telnet/SSH, Web Links, Web VPN and Web Folder connections using the current company's security policy:



OPTION	DESCRIPTION
Profile List	This list shows the available profiles. You can enable or disable them by checking the box to the left of the name.

Add	Press this button to add a new profile. You can add an RDP Profile , or a Weblink Profile .
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 .
Duplicate	Select a profile and press this button to duplicate it.
Remove	Select a profile and press this button to remove it.
Import	Imports a .CSV or .JSON file with an Access Profiles list
Export	Exports the current Access Profiles list to a .CSV or .JSON file.
Allowed users and groups for selected	See here the allowed users or group(s) of

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

- Restrict the application access with Active Directory Authentication.
- Specify different access levels for different users and groups of users.
- Make the users' experience faster by configuring predetermined RDP preferences for each profile.
- Unify authentications in a Single Sign-on scheme.
- Allow external application to manage Thinfinity® Remote Workspace users and machine permissions through the use of a Web Service.



The '['+']' Access Profile

Thinfinity® Remote Workspace



RDP Access Profile

Thinfinity® Remote Workspace





RDS Web Feed Access Profile

Thinfinity® Remote Workspace



VNC/RFB Access Profile

Thinfinity® Remote Workspace



Telnet/SSH Access Profile

Thinfinity® Remote Workspace



Web Link Access Profile

Thinfinity® Remote Workspace



Web VPN Access Profile

Thinfinity® Remote Workspace



Web Folder Access Profile

Thinfinity® Remote Workspace



Label Access Profile

Thinfinity® Remote Workspace



How to create an Access Profile connection

In this section, you'll find step-by-step guides to create and edit each of the Access Profile connection types, and folders that contain these profiles, with Thinfinity® Remote Workspace:



RDP Access Profile

Thinfinity® Remote Workspace



RDS Web Feed Access Profile

Thinfinity® Remote Workspace



VNC/RFB Access Profile

Thinfinity® Remote Workspace



Telnet/SSH Access Profile

Thinfinity® Remote Workspace



Web Link Access Profile

Thinfinity® Remote Workspace



Web VPN Access Profile

Thinfinity® Remote Workspace



Label Access Profile

Thinfinity® Remote Workspace



RDP Access Profile

An RDP Access Profile connects users to their desktop and applications.

You'll find the steps to create, edit, disable and remove such RDP connections below:



Creating an RDP Access Profile

Thinfinity® Remote Workspace



Editing an RDP Access Profile

Thinfinity® Remote Workspace



Disabling an RDP Access Profile

Thinfinity® Remote Workspace



Removing an RDP Access Profile

Thinfinity® Remote Workspace



Creating an RDP Access Profile

- Go to the Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Add' > 'RDP' to create a new profile and the following window will be presented:

Thinfinity Configuration Manager - Profile Editor

Name: None

Virtual Path:

Access Key: New Key

Label(s): Select Label

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General | Display | Resources | Program | Experience | Advanced | Printer | Permissions | Restrictions | Access Hours | Auth

Computer: Broker Pool:

☐ Connect to a Hyper-V Virtual Machine

☐ Connect to a Virtual Desktop on an RDS Collection

☐ Enable Wake-on-LAN (WoL)

Session Limit: Minutes

Credentials:

☒ Use the authenticated credentials

☐ Ask for new credentials

☐ Use these credentials: ☐ Create if it doesn't exist

User name:

Password:

Ok Cancel

OPTION

DESCRIPTION

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: http(s)://ThinfinityDomain:port/VirtualPath/. The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Workspace web interface.
Access Key	Used in combination with Thinfinity® Remote Workspace 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.
Select Label	Prompts you to select an existing Label for this specific profile.
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.
RDP/RDS Web Feed	Select the 'RDP' option to have a regular profile that connects to a remote machine or application through RDP. Select the 'RDS Web Feed' option to pull the Microsoft RD Web Access connections into the web interface.
Computer	Use this field to change the profile name. The profile name is shown to users to identify the connection.
Broker Pool	Specify which broker pool this profile belongs to.
Session Limit	Set up a session time limit for this profile.
Connect to a Hyper-V Virtual Machine	Check this option if you want to connect to a Hyper-V Virtual Machine through its machine ID or GUID. Learn in details how to set up a Hyper-V profile .

Connect to a Virtual Desktop on an RDS Collection	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, 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.
Enable Wake-on-LAN (WoL)	Check this option if you want to allow a computer to be turned on or awakened by a network message.
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 Workspace. if this is

- Read the next topic '[Editing an RDP Access Profile](#)' to learn how to configure this profile.

You can find more information on each property that you can modify on the RDP Profile Editor here:



RDP Profile Editor

Thinfinitv® Remote Workspace



Editing an RDP Access Profile

Configuring an RDP Access Profile properly will allow you to take advantage of all its features and create an access scheme that would suit your company's needs best.

Remember that each profile defines a single computer's desktop or application access, except for the '[+]' profile that gives access to all computers.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Edit' to configure the profile and the following window will be presented:

Thinfinity Configuration Manager - Profile Editor

Name: Localhost

Virtual Path: Localhost

Access Key: tiYlfmYqjp8tN2Va3WSkrK1vGNfvTLby

Label(s): \

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General | Display | Resources | Program | Experience | Advanced | Printer | Permissions | Restrictions | Access Hours | Authentication

Computer: 127.0.0.1

Broker Pool:

☐ Connect to a Hyper-V Virtual Machine

☐ Connect to a Virtual Desktop on an RDS Collection

☐ Enable Wake-on-LAN (WoL)

Session Limit: 0 Minutes

Credentials:

☒ Use the authenticated credentials

☐ Ask for new credentials

☐ Use these credentials: ☐ Create if it doesn't exist

User name:

Password:

Ok Cancel

- First of all, type in a descriptive name for the profile in the '*Name*' field.
- Specify the computer this profile will connect to. Enter the internal IP or computer name on the '*Computer*' field.
- Set the credentials to log into the remote machine:

OPTION	DESCRIPTION
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 Workspace, if this is the only profile the user has.

- Go to the '*Permissions*' tab and set up the permission preferences as follow:

OPTION	DESCRIPTION
Allow anonymous access	Use this option, if you want this profile to be available for everyone. This means that everybody accessing Thinfinity® Remote Workspace will see this profile. Checking this option will disable the user.
Group or users access	<p>To use specific users for this profile, uncheck "Allow anonymous access", press "Add" and choose the users and groups from the local domain.</p> <p>This means that only users that authenticate with their correct Windows username and password will be able to use this profile. (*)</p>

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

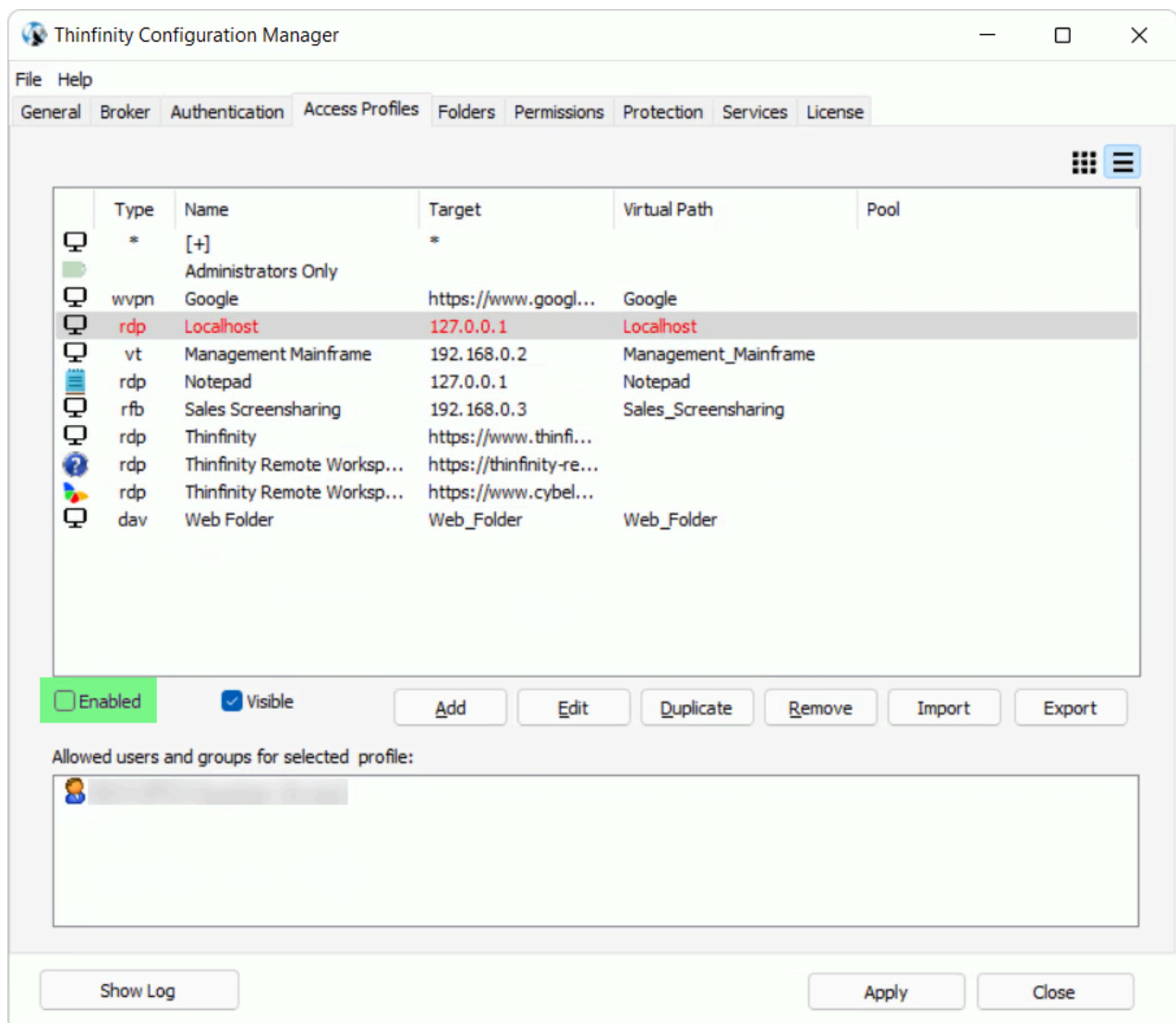
- When you are done, press '*Ok*'.

Disabling an RDP Access Profile

Disabling an RDP Access Profile will make it unavailable to all users.

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

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the [Access Profiles](#) topic first.
- Select the profile you want to disable.
- Click the check-box next to 'Enabled':

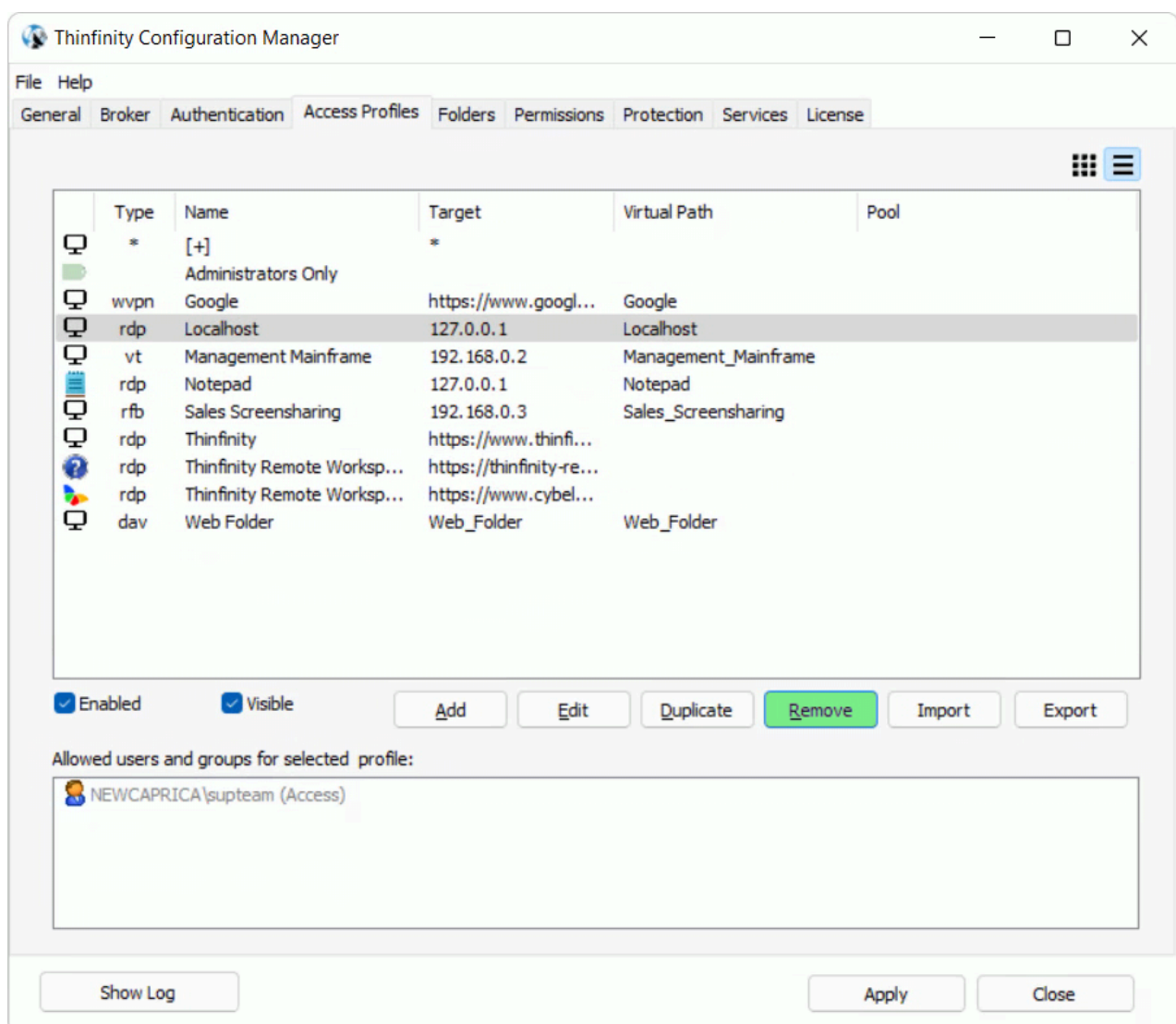


- Observe that the profile name will turn red.
- Press 'Apply' to save the changes.

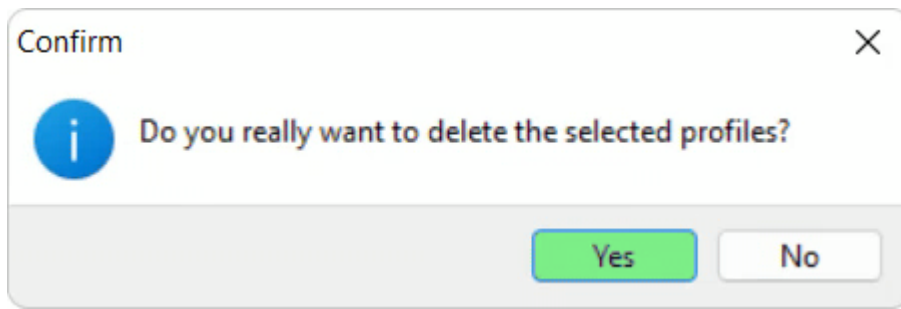
Removing an RDP Access Profile

Remember that once you remove an RDP Access Profile, you won't be able to recover it.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the topic [Access Profiles](#) first.
- Select the profile you want to remove.
- Press the 'Remove' button:



- Press 'Yes' on the confirmation message:



- Press '*Apply*' to save the changes.

RDS Web Feed Access Profile

An RDS Web Feed Access Profile connects users to Microsoft RD Web Access profiles as regular Thinfinity® Remote Workspace profiles.

You'll find the steps to create, edit, disable and remove such RDS Web Feed connections below:



Creating an RDS Web Feed Access Profile

Thinfinity® Remote Workspace



Editing an RDS Web Feed Access Profile

Thinfinity® Remote Workspace



Disabling an RDS Web Feed Access Profile

Thinfinity® Remote Workspace



Removing an RDS Web Feed Access Profile

Thinfinity® Remote Workspace



Creating an RDS Web Feed Access Profile

- Go to the Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Add' > 'RDP' to create a new profile, then check the 'RDS Web Feed' option on the following window:

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

☒ Visible ☐ Default profile

☐ RDP ☒ RDS Web Feed

General | Permissions | Restrictions | Access Hours | Authentication Methods

RD Web URL:

Credentials:

☒ Use the authenticated credentials

☐ Ask for credentials

☐ Use these credentials:

User name:

Password:

Ok Cancel

OPTION

DESCRIPTION

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)://ThinfinityDomain:port/VirtualPath/</code> . The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Workspace web interface.
Access Key	Used in combination with Thinfinity® Remote Workspace 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.
Select Label	Prompts you to select an existing Label for this specific profile.
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

- Read the next topic '[Editing an RDS Web Feed Access Profile ↗](#)' to learn how to configure this profile.

You can find more information on each property that you can modify, for an RDS Web Feed connection, on the RDP Profile Editor here:



RDP Profile Editor

Thinfinity® Remote Workspace



Editing an RDS Web Feed Access Profile

Configuring an RDS Web Feed Access Profile properly will allow you to take advantage of all its features and create an access scheme that would suit your company's needs best.

Remember that each profile defines a single computer's desktop or application access, except for the '[+]' profile that gives access to all computers.

- Go to Thinfinity® Remote Workspace Configuration Manager's '*Access Profiles*' tab.
- Press '*Edit*' to configure the profile.
- First of all, type in a descriptive name for the profile in the '*Name*' field.
- Select the '*RDS Web Feed*' Option:

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

☒ Visible ☐ Default profile

☐ RDP ☒ RDS Web Feed

General | Permissions | Restrictions | Access Hours

RD Web URL:

Credentials:

☒ Use the authenticated credentials

☐ Ask for credentials

☐ Use these credentials:

User name:

Password:

Ok Cancel

- Complete the '*RD Web URL*' field with the Microsoft RD Web Access URL.
- Set the credentials to log into the remote machine:

OPTION	DESCRIPTION
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 Workspace, if this is the only profile the user have

- Go to the '*Permissions*' tab and set up the permission preferences as follow:

OPTION	DESCRIPTION
Allow anonymous access	Use this option, if you want this profile to be available for everyone. This means that everybody accessing Thinfinity® Remote Workspace will see this profile. Checking this option will disable the user selection.
Group or users access	<p>To use specific users for this profile, uncheck "Allow anonymous access", press "Add" and choose the users and groups from the local domain.</p> <p>This means that only users that authenticate with their correct Windows username and password will be able to use this profile.(*)</p>

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

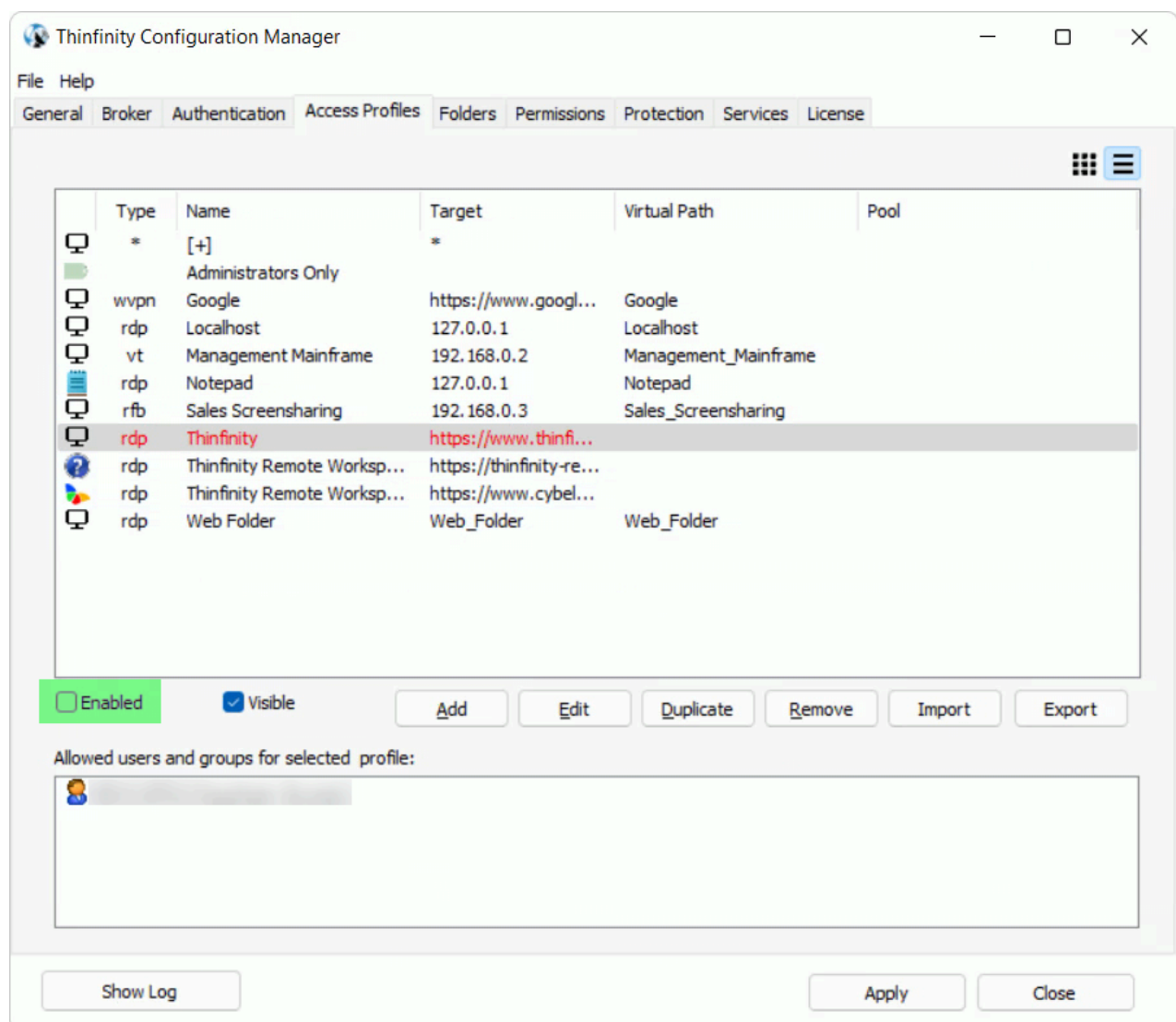
- When you are done with the previous steps, press '*Ok*'.

Disabling an RDS Web Feed Access Profile

Disabling an RDS Web Feed Access Profile will make it unavailable to all users.

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

- Go to Thinfinity® Remote Workspace Configuration Manager's '*Access Profiles*' tab. If it is not there, read the [Access Profiles](#) topic first.
- Select the profile you want to disable.
- Click the check-box next to '*Enabled*':



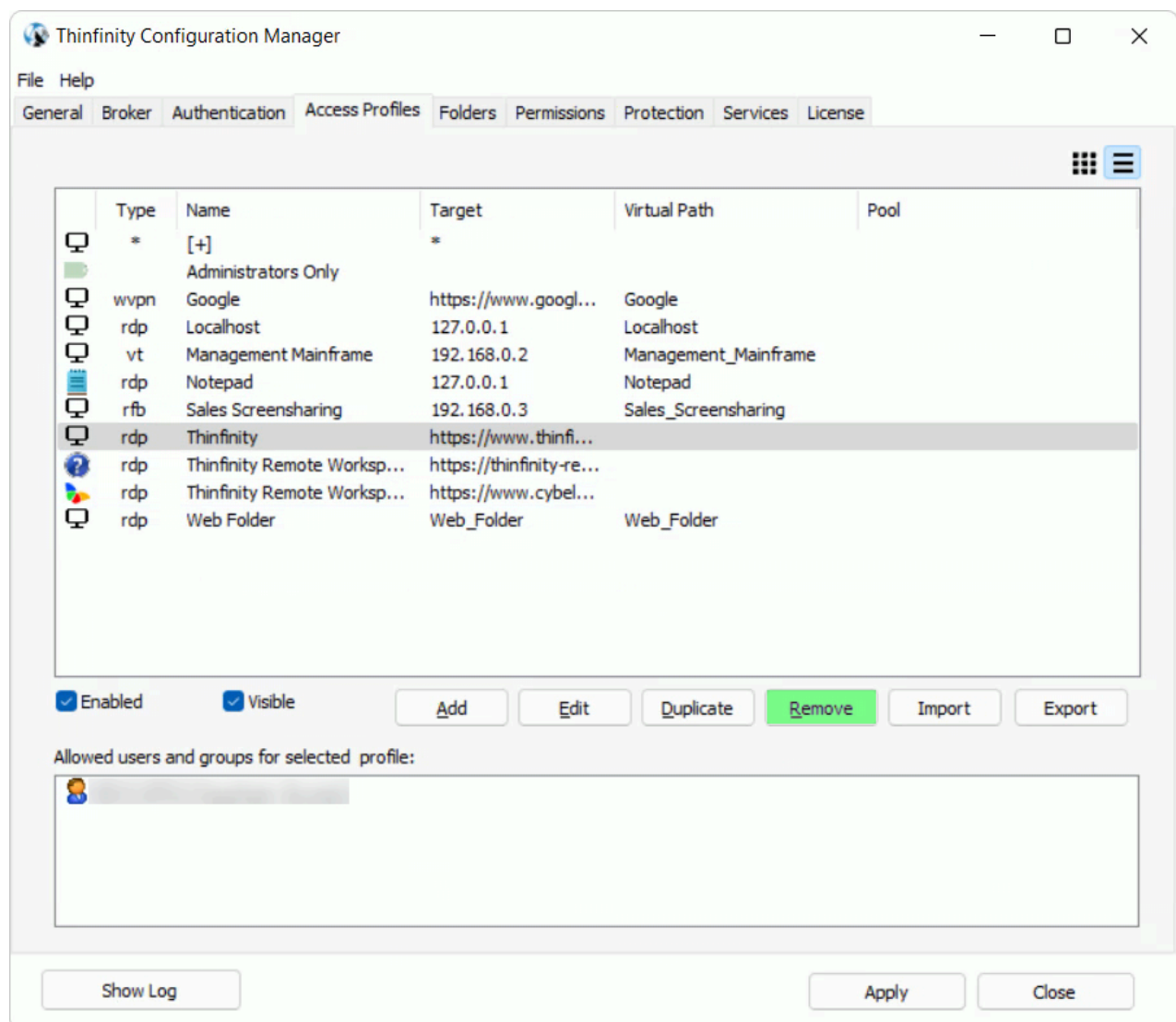
- Observe that the profile name will turn red.

- Press '*Apply*' to save the changes.

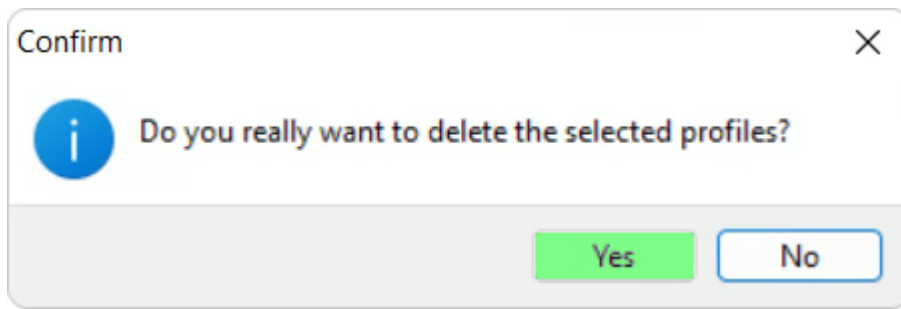
Removing an RDS Web Feed Access Profile

Remember that once you remove an RDS Web Feed Access Profile, you won't be able to recover it.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the topic [Access Profiles](#) first.
- Select the profile you want to remove.
- Press the 'Remove' button:



- Press 'Yes' on the confirmation message:



- Press '*Apply*' to save the changes.

VNC/RFB Access Profile

A VNC/RFB Access Profile connects users to a screen-sharing session.

You'll find the steps to create, edit, disable and remove such VNC/RFB connections below:



Creating a VNC/RFB Access Profile

Thinfinity® Remote Workspace



Editing a VNC/RFB Access Profile

Thinfinity® Remote Workspace



Disabling a VNC/RFB Access Profile

Thinfinity® Remote Workspace



Removing a VNC/RFB Access Profile

Thinfinity® Remote Workspace



Creating a VNC/RFB Access Profile

- Go to the Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Add' > 'VNC/RFB' to create a new profile and the following window will be presented:

Thinfinitiy Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Display | Permissions | Restrictions | Access Hours | Authentication Methods

Computer:

Port:

Broker Pool:

Password:

Session Limit: Minutes

☐ Enable Wake-on-LAN (WoL)

Ok Cancel

OPTION	DESCRIPTION
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: http(s)://ThinfinityDomain:port/VirtualPath/. The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Workspace web interface.
Access Key	Used in combination with Thinfinity® Remote Workspace 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.
Select Label	Prompts you to select an existing Label for this specific profile.
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.
Computer	Use this field to change the profile name. The profile name is shown to users to identify the connection.
Port	Port used by the VNC/RFB server installed on the destination machine.
Password	Password configured in the VNC/RFB server installed on the destination machine.
Broker Pool	Specify which broker pool this profile belongs to.

- Read the next topic '[Editing a VNC/RFB Access Profile ↗](#)' to learn how to configure this profile.

You can find more information on each property that you can modify on the VNC/RFB Profile Editor [here](#):



VNC/RFB Profile Editor

Thinfinity® Remote Workspace



Editing a VNC/RFB Access Profile

Configuring a VNC/RFB Access Profile properly will allow you to take advantage of all its features and create an access scheme that would suit your company's needs best.

Remember that each profile defines a single computer's desktop or application access, except for the '[+]' profile that gives access to all computers.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Edit' to configure the profile and the following window will be presented:

Thinfinitiy Configuration Manager - Profile Editor

Name: Sales Screensharing

Virtual Path: Sales_Screensharing

Access Key: tiae9PR.\$GVI7N7Vq39apacm\$znuBbz\$X

Label(s): \

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Display | Permissions | Restrictions | Access Hours | Authentication Methods

Computer: 192.168.0.3

Port: 5900

Broker Pool:

Password:

Session Limit: 0 Minutes

☐ Enable Wake-on-LAN (WoL)

Ok Cancel

- First of all, type in a descriptive name for the profile in the '*Name*' field.
- Specify the computer this profile will connect to. Enter the internal IP or computer name on the '*Computer*' field.
- Set the '*Port*' and '*Password*' to log into the remote machine:

OPTION	DESCRIPTION
Port	Port used by the VNC/RFB server installed on the destination machine.
Password	Password configured in the VNC/RFB server installed on the destination machine.

- Go to the '*Permissions*' tab and set up the permission preferences as follows:

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

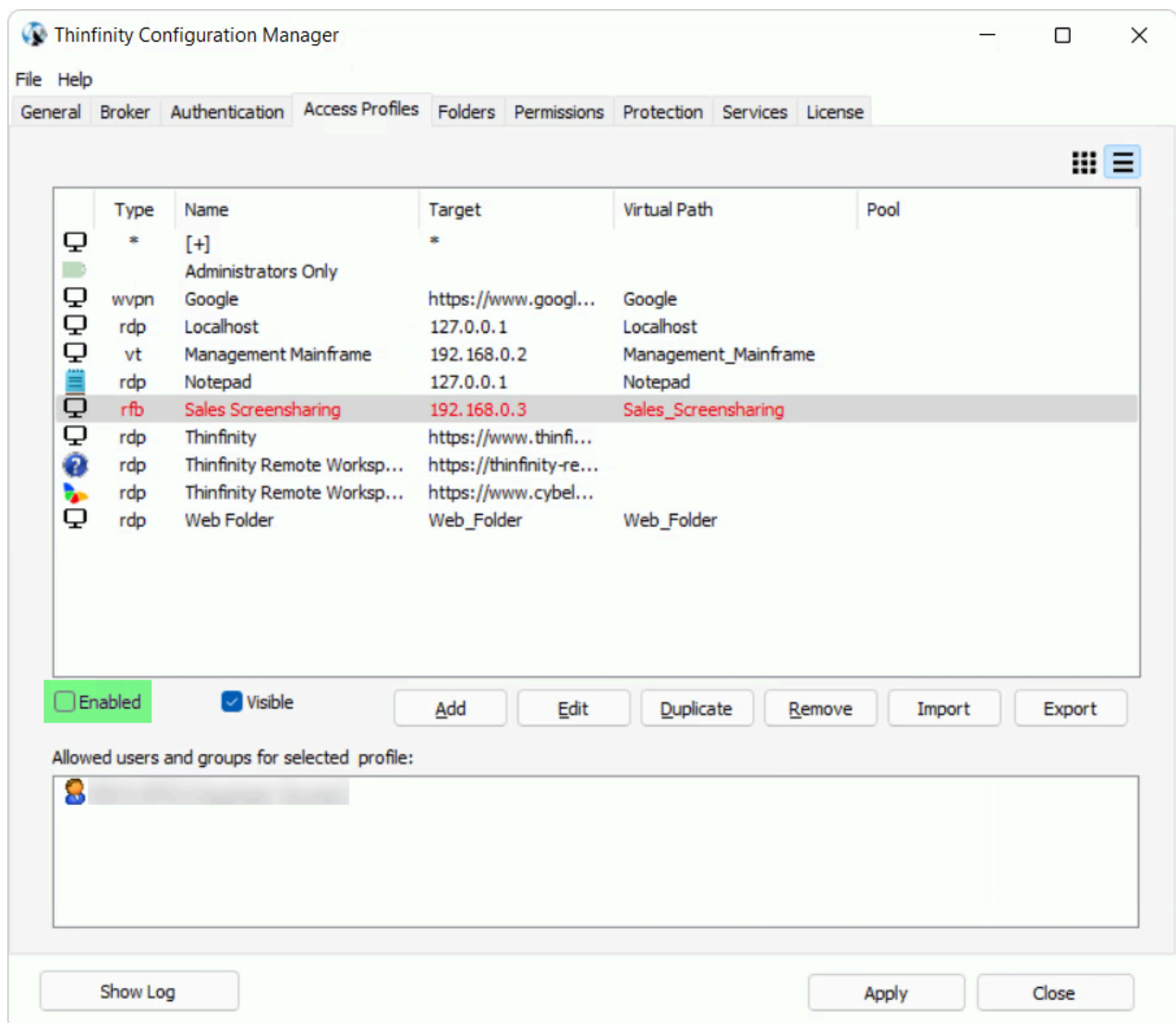
- When you are done with the previous steps, press '*OK*'.

Disabling a VNC/RFB Access Profile

Disabling a VNC/RFB Access Profile will make it unavailable to all users.

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

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the [Access Profiles](#) topic first.
- Select the profile you want to disable.
- Click the check-box next to 'Enabled':

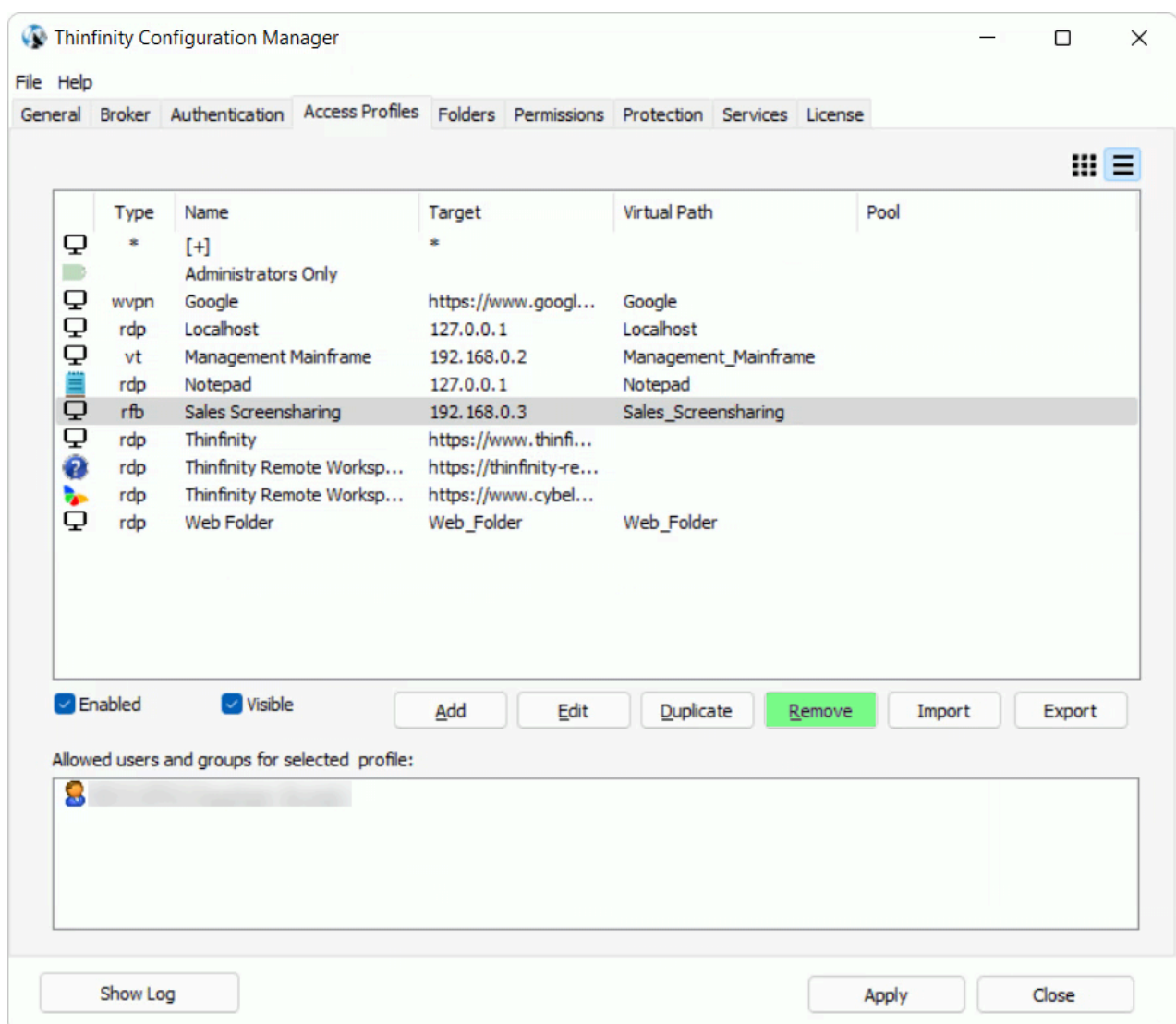


- Observe that the profile name will turn red.
- Press 'Apply' to save the changes.

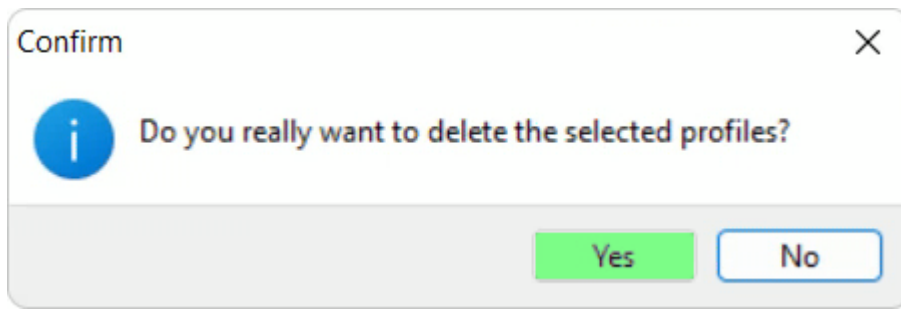
Removing a VNC/RFB Access Profile

Remember that once you remove a VNC/RFB Access Profile, you won't be able to recover it.

- Go to Thinfinity® Remote Workspace Configuration Manager's '*Access Profiles*' tab. If it is not there, read the topic [Access Profiles](#) first.
- Select the profile you want to remove.
- Press the '*Remove*' button:



- Press 'Yes' on the confirmation message:



- Press '*Apply*' to save the changes.

Telnet/SSH Access Profile

A Telnet/SSH Access Profile connects users to either a Telnet or an SSH session.

You'll find the steps to create, edit, disable and remove such Telnet/SSH connections below:



Creating a Telnet/SSH Access Profile

Thinfinity® Remote Workspace



Editing a Telnet/SSH Access Profile

Thinfinity® Remote Workspace



Disabling a Telnet/SSH Access Profile

Thinfinity® Remote Workspace



Removing a Telnet/SSH Access Profile

Thinfinity® Remote Workspace



Creating a Telnet/SSH Access Profile

- Go to the Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Add' > 'Telnet/SSH' to create a new profile and the following window will be presented:

Thinfinitiy Configuration Manager - Profile Editor

Name: None

Virtual Path:

Access Key: New Key

Label(s): Select Label

☒ Visible ☐ Default profile

General | Display | Options | Permissions | Restrictions | Access Hours | Authentication Methods

Address: Port:

☐ Enable Keep Alive ☐ SSL

☐ Disable Telnet Protocol Negotiation ☐ SSH

☐ Disable Server Echo

Character Set:

Keyboard Name:

Broker Pool:

Session Limit: Minutes

Ok Cancel

OPTION	DESCRIPTION
Address	Specify the URL/resource you want to connect to.
Port	Port used by the Telnet/SSH server installed on the destination machine.

Enable Keep alive	Enables keep-alive mechanism, needed for some Telnet servers to prevent disconnections.
Disable Telnet Protocol Negotiation	Check this option if you want to omit the protocol negotiation when connecting.
Disable Server Echo	Check this option if you don't want the server to echo every character it receives.
SSL	Enables the SSL (Secure Sockets Layer) protocol for the host.
SSH	Enables the SSH protocol for the host.
Character Set Translation	Select the character set that better suits your language needs
Keyboard Name	Specify a keyboard set
Broker Pool	Specify which broker pool this profile belongs to.
Session Limit	Set up a session time limit for this profile.

- Read the next topic '[Editing a Telnet/SSH Access Profile ↗](#)' to learn how to configure this profile.

You can find more information on each property that you can modify on the Telnet/SSH Profile Editor here:



Telnet/SSH Profile Editor
Thinfinity® Remote Workspace



Editing a Telnet/SSH Access Profile

Configuring a Telnet/SSH Access Profile properly will allow you to take advantage of all its features and create an access scheme that would suit your company's needs best.

Remember that each profile defines a single computer's desktop or application access, except for the '[+]' profile that gives access to all computers.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Edit' to configure the profile and the following window will be presented:

Thinfinity Configuration Manager - Profile Editor

Name: Management Mainframe

Virtual Path: Management_Mainframe

Access Key: foa24WkiGpIENDV1xrKBadMh9-Td@p9W

Label(s): \

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Display | Options | Permissions | Restrictions | Access Hours | Authentication Methods

Address: 192.168.0.2

Port: 23

☐ Enable Keep Alive ☐ SSL

☐ Disable Telnet Protocol Negotiation ☐ SSH

☐ Disable Server Echo

Character Set: MsDos USA

Keyboard Name: [Standard]

Broker Pool:

Session Limit: 0 Minutes

Ok Cancel

- First of all, type in a descriptive name for the profile in the '*Name*' field.
- Specify the computer this profile will connect to. Enter the internal IP address or computer name on the '*Address*' field.
- Set the '*Port*' to log into the remote machine:

bt - fix table below

OPTION	DESCRIPTION
Port	Port used by the destination server for Telnet/SSH Connections.

- Go to the '*Permissions*' tab and set up the permission preferences as follows:

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

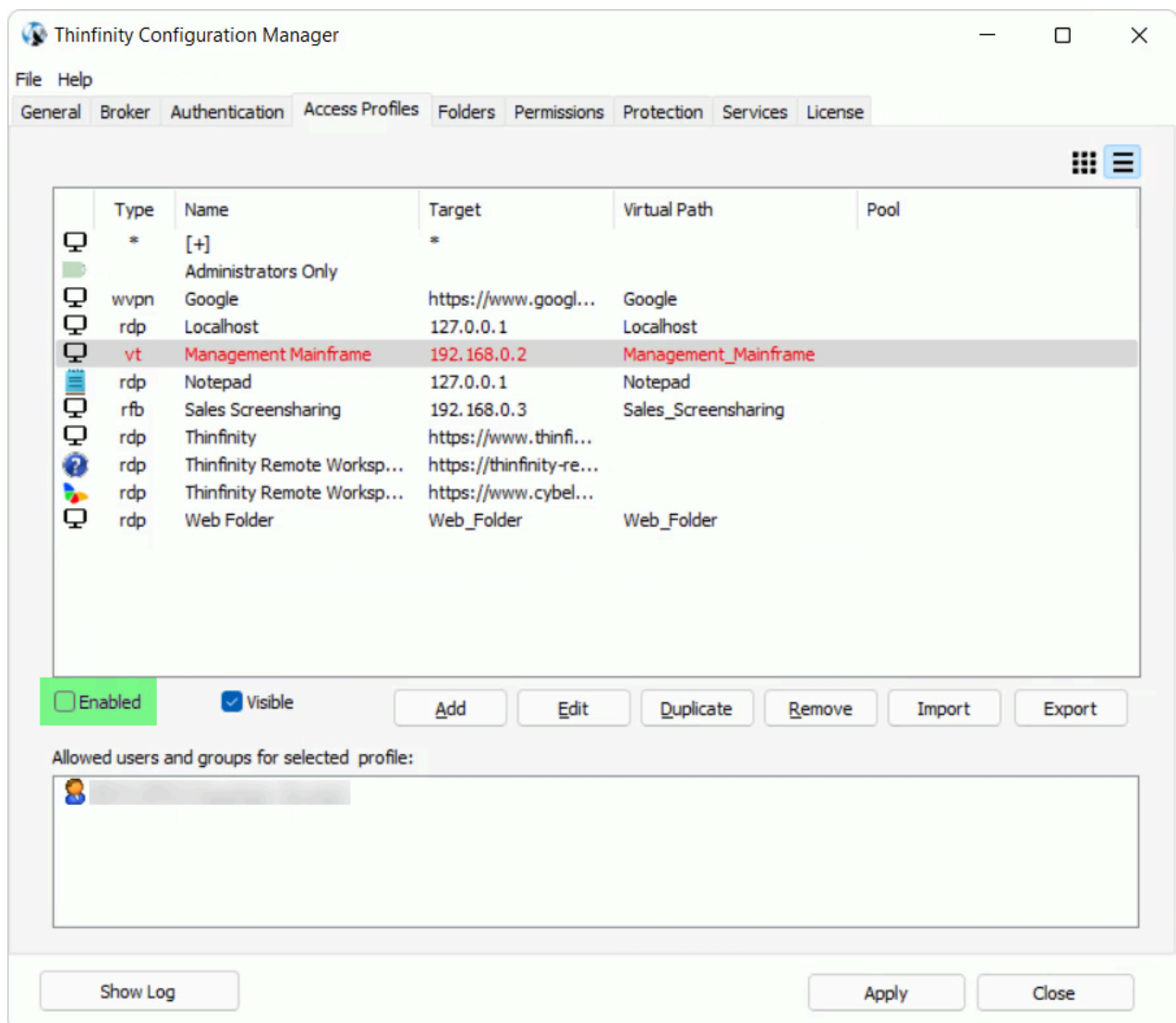
- When you are done with the previous steps, press '*OK*'.

Disabling a Telnet/SSH Access Profile

Disabling a Telnet/SSH Access Profile will make it unavailable to all users.

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

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the [Access Profiles](#) topic first.
- Select the profile you want to disable.
- Click the check-box next to 'Enabled':

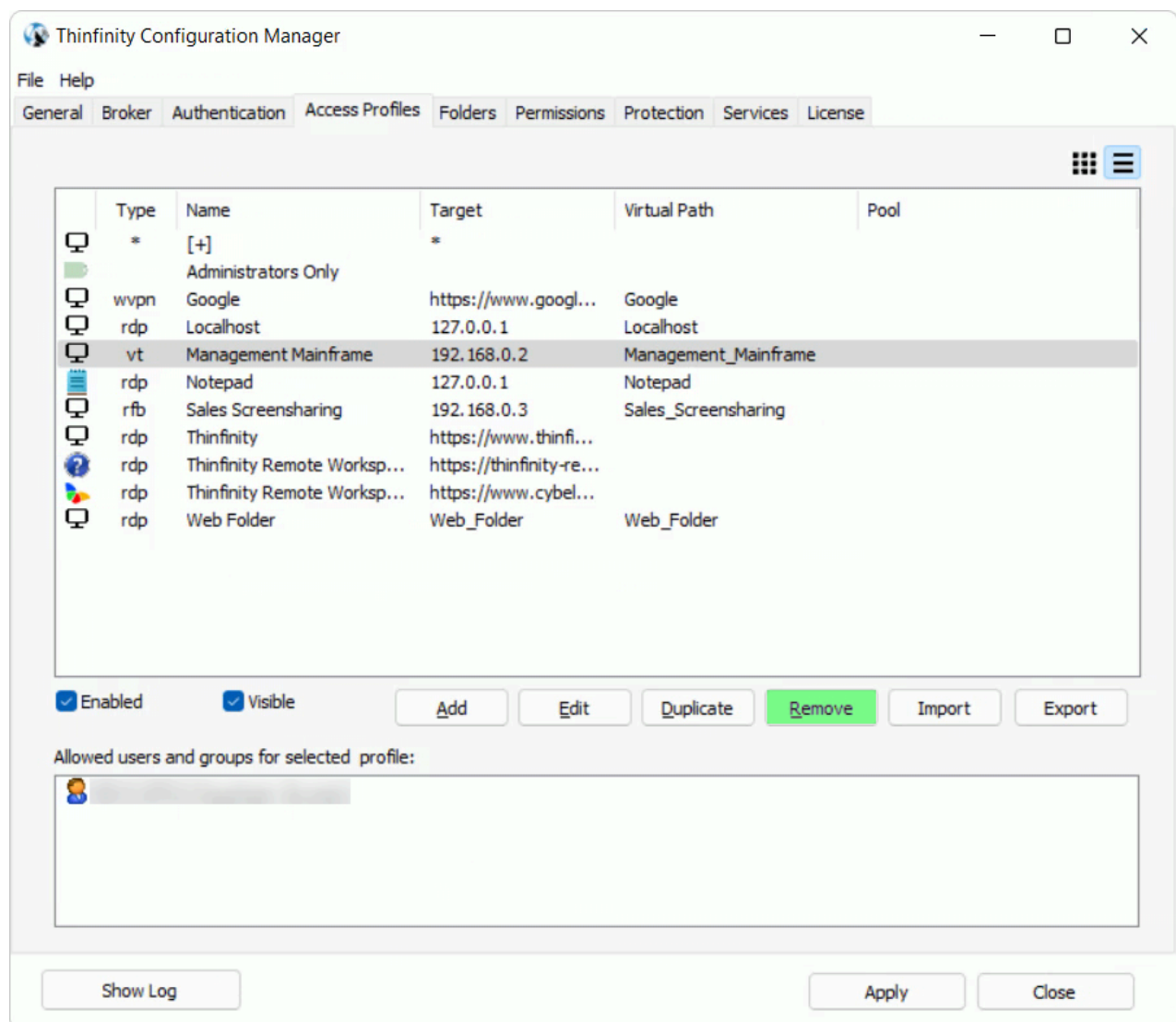


- Observe that the profile name will turn red.
- Press 'Apply' to save the changes.

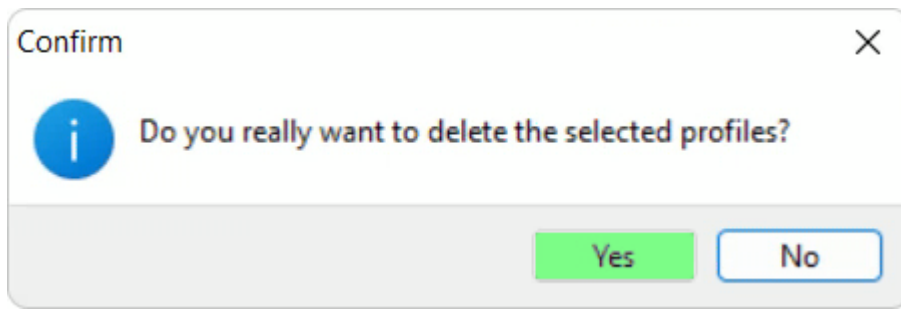
Removing a Telnet/SSH Access Profile

Remember that once you remove a Telnet/SSH Access Profile, you won't be able to recover it.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the topic [Access Profiles](#) first.
- Select the profile you want to remove.
- Press the 'Remove' button:



- Press 'Yes' on the confirmation message:



- Press '*Apply*' to save the changes.

Web Link Access Profile

A Web Link Access Profile allows users access to an informed URL.

You'll find the steps to create, edit, disable and remove such Web Link connections below:



Creating a Web Link Access Profile

Thinfinity® Remote Workspace



Editing a Web Link Access Profile

Thinfinity® Remote Workspace



Disabling a Web Link Access Profile

Thinfinity® Remote Workspace



Removing a Web Link Access Profile

Thinfinity® Remote Workspace



Creating a Web Link Access Profile

- Go to the Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Add' > 'Web Link' to create a new profile.
- Select the option 'Web Link' and the following screen will be presented:

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

General | Permissions | Restrictions | Access Hours | Authentication Methods

Web URL:

OPTION	DESCRIPTION
Web URL	Enter here the URL of the web page you want this profile to link to.
	Press this button to get the web page icon directly from the URL entered in the 'Web

Get Icon

URL' field. This icon will replace the Icon set in the 'Icon' option above. To change it back, press on the icon. [Read more](#).

- Read the next topic '[Editing a Web Link Access Profile ↗](#)' to learn how to configure this profile.

You can find more information on each property that you can modify on the Web Link Profile Editor here:



Web Link Profile Editor
Thinfinity® Remote Workspace



Editing a Web Link Access Profile

Configuring a Web Link Access Profile properly will allow you to take advantage of all its features and create an access scheme that would suit your company's needs best.

Remember that each profile defines a single computer's desktop or application access, except for the '[+]' profile that gives access to all computers.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Select the profile you want to modify and press 'Edit':

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Permissions | Restrictions | Access Hours | Authentication Methods

Web URL:

Get Icon

Ok Cancel

- First of all, type in a descriptive name for the profile in the '*Name*' field.
- Specify the '*Web URL*' you want the profile to connect to.
- Go to the '*Permissions*' tab and set up the permission preferences as follows:

OPTION	DESCRIPTION
Allow anonymous access	Use this option, if you want this profile to be available for everyone. This means that everybody accessing Thinfinity® Remote Workspace will see this profile. Checking this option will disable the user selection.
Group or users access	<p>To use specific users for this profile, uncheck "Allow anonymous access", press "Add" and choose the users and groups from the local domain.</p> <p>This means that only users that authenticate with their correct Windows username and password will be able to use this profile.(*)</p>

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

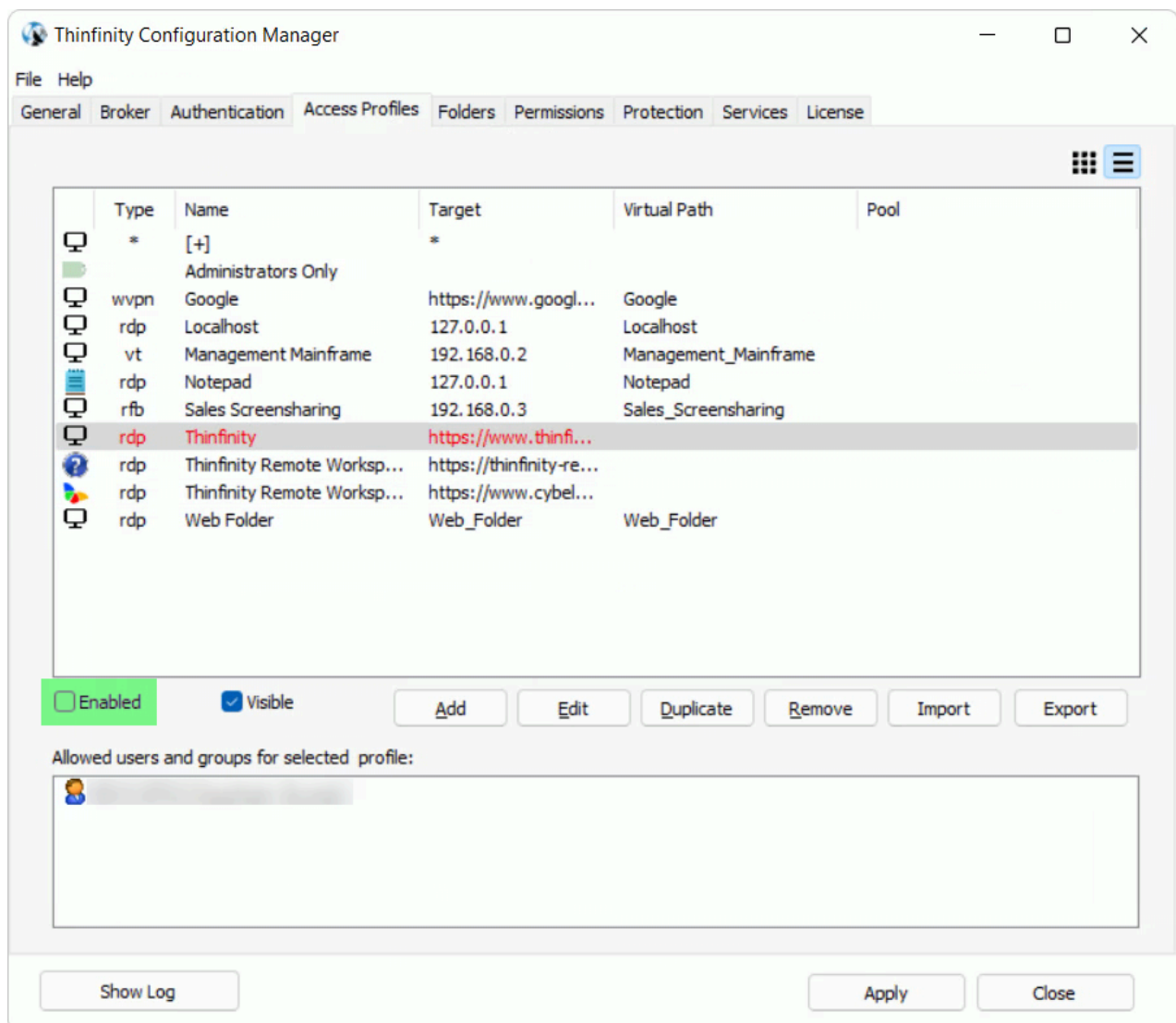
- When you are done with the previous steps, press '*Ok*'.

Disabling a Web Link Access Profile

Disabling a Web Link Access Profile will make it unavailable to all users.

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

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the [Access Profiles](#) topic first.
- Select the profile you want to disable.
- Click the check-box next to 'Enabled':

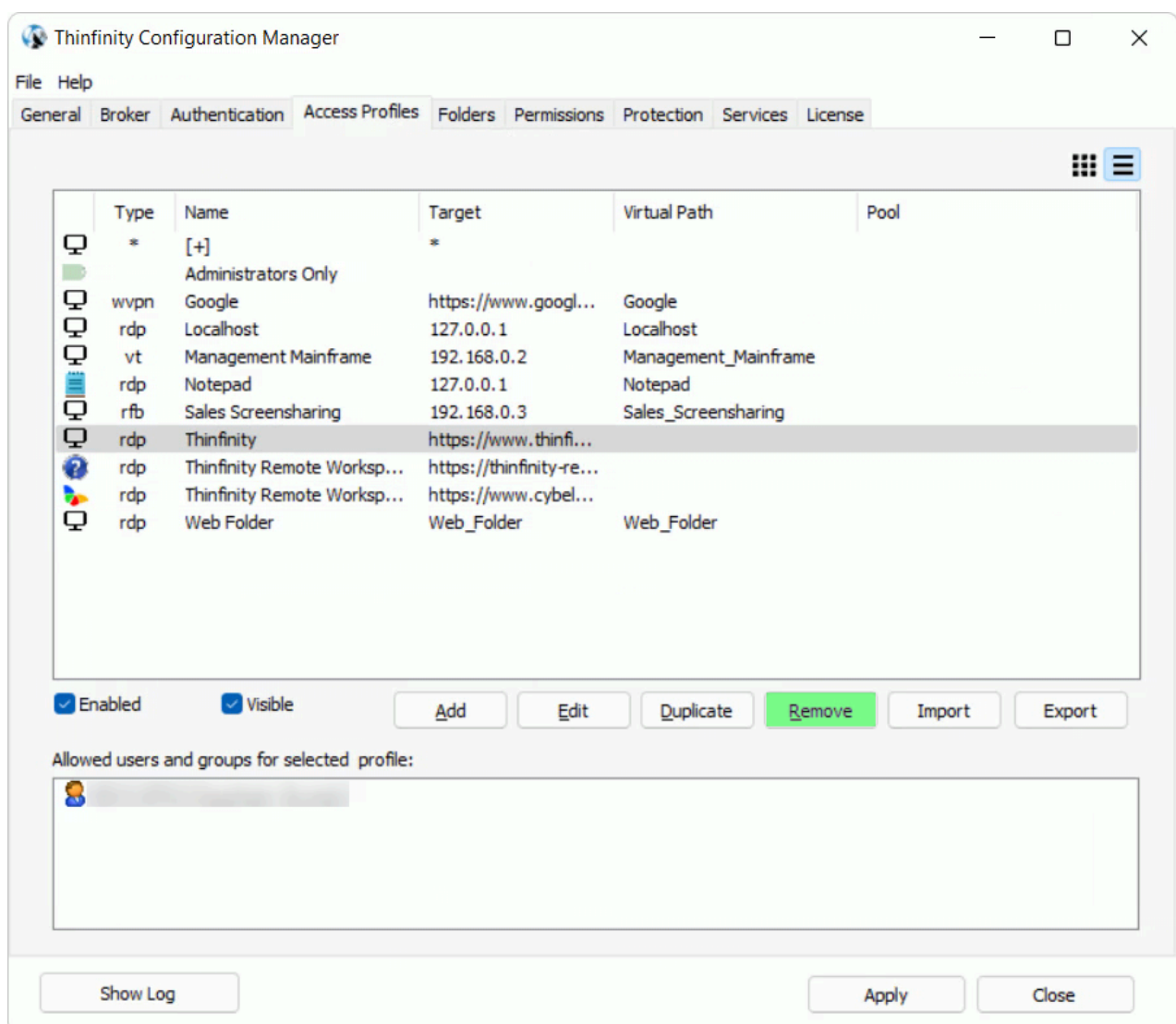


- Observe that the profile name will turn red.
- Press 'Apply' to save the changes.

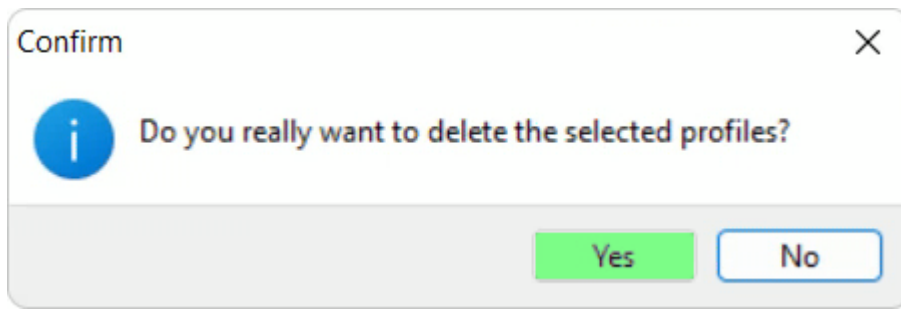
Removing a Web Link Access Profile

Remember that once you remove a Web Link Access Profile, you won't be able to recover it.

- Go to Thinfinity® Remote Workspace Configuration Manager's '*Access Profiles*' tab. If it is not there, read the topic [Access Profiles](#) first.
- Select the profile you want to remove.
- Press the '*Remove*' button:



- Press 'Yes' on the confirmation message:



- Press '*Apply*' to save the changes.

Read more:

- [Testing Internal Access](#)

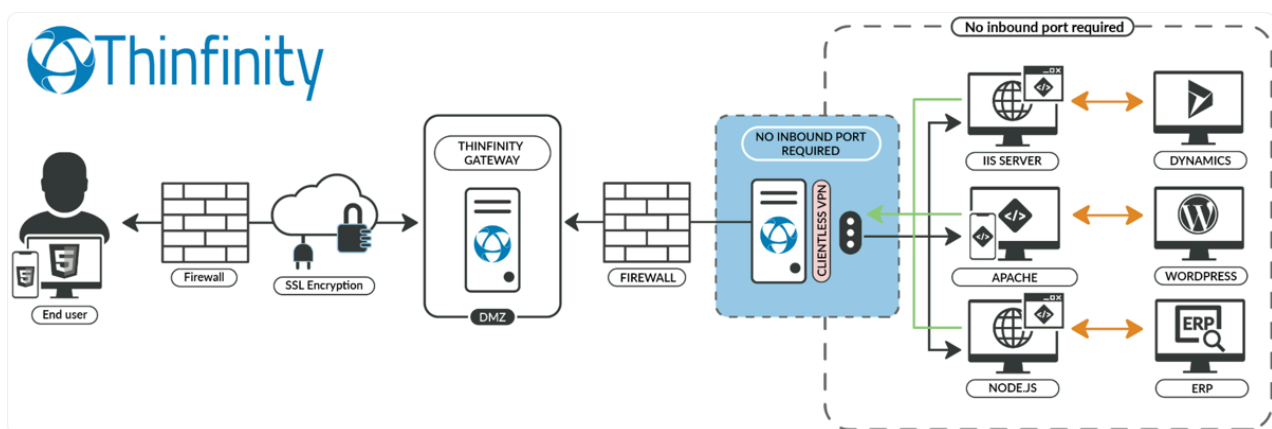
Web VPN Access Profile

More often than not, employees are required to interact with several sites or web applications that are only accessible through a company's private network. To mitigate this need, companies have been obliged to deal with pesky VPN solutions, which are time consuming and require a great deal of expertise to properly and securely set up.

Ongoing security updates, compliance checks and compatibility issues are likely to impact directly on IT resources while also adding considerable stress on network performance.

Many VPNs do not provide the tools for unmanaged devices to securely connect to an organization's network.

This image exemplifies how a Web VPN is configured with Thinfinity® Remote Workspace:



Thinfinity® Remote Workspace includes an ingenious Clientless VPN which enables IT Admins to easily and effortlessly deliver access to Enterprise Intranet Applications.

Thinfinity® Remote Workspace manages to do all this, without the need to install an additional client on the end-user machine. Simply whitelist the domain(s) you need to provide access to, and it will securely forward this connection to the end user's HTML5 browser.

Thanks to this new approach, legacy VPNs are now a thing of the past. Employees are no longer required to connect to a corporate network, removing the unnecessary security risk of them accessing restricted devices or data.

You'll find the steps to create, edit, disable and remove such Web VPN connections below:



Creating a Web VPN Access Profile

Thinfinity® Remote Workspace



Editing a Web VPN Access Profile

Thinfinity® Remote Workspace



Disabling a Web VPN Access Profile

Thinfinity® Remote Workspace



Removing a Web VPN Access Profile

Thinfinity® Remote Workspace



Creating a Web VPN Access Profile

- Go to the Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Add' > 'Web VPN' to create a new profile and the following window will be presented:

Thinfinty Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key: None

Label(s):

☒ Visible ☐ Default profile

New Key Select Label

General | Permissions | Restrictions | Access Hours | Authentication Methods

Main entry point:

☐ Rewrite urls to "/" (Optimize for SPA) Custom Headers

☒ Sanitize input (Prevent XSS)

Valid domains:

Broker Pool:

Ok Cancel

OPTION	DESCRIPTION
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: http(s)://ThinfinityDomain:port/VirtualPath/. The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Workspace web interface.
Access Key	Used in combination with Thinfinity® Remote Workspace 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.
Select Label	Prompts you to select an existing Label for this specific profile.
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.
Main entry point	Use this field to specify the Web VPN URL you wish to access with this profile.
Rewrite URLs to "/"	With this option checked, you are able to rewrite URLs to '/' or with custom headers.
Valid domains	Specify the valid domains for this Web VPN profile specifically.
	Specify which broker pool this profile

- Read the next topic '[Editing a Web VPN Access Profile ↗](#)' to learn how to configure this profile.

You can find more information on each property that you can modify on the Web Link Profile Editor here:



Web VPN Profile Editor
Thinfinity® Remote Workspace



Editing a Web VPN Access Profile

Configuring a Web VPN Access Profile properly will allow you to take advantage of all its features and create an access scheme that would suit your company's needs best.

Remember that each profile defines a single computer's desktop or application access, except for the '[+]' profile that gives access to all computers.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Edit' to configure the profile and the following window will be presented:

Thinfinity Configuration Manager - Profile Editor

Name: Google

Virtual Path: Google

Access Key: fqsmBaW40f0vNff5gE2atbLQ4Nfd\$uU4

Label(s): \

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Permissions | Restrictions | Access Hours | Authentication Methods

Main entry point: https://www.google.com

☐ Rewrite urls to "/" (Optimize for SPA)

☒ Sanitize input (Prevent XSS)

Valid domains:

Broker Pool:

Custom Headers

Ok Cancel

- Type in a descriptive name for the profile in the '*Name*' field
- Specify the URL address this profile will connect to on the '*Main entry point*' field.
- Go to the '*Permissions*' tab and set up the permission preferences as follow:

OPTION	DESCRIPTION
Allow anonymous access	Use this option, if you want this profile to be available for everyone. This means that everybody accessing Thinfinity® Remote Workspace will see this profile. Checking this option will disable the user.
Group or users access	<p>To use specific users for this profile, uncheck "Allow anonymous access", press "Add" and choose the users and groups from the local domain.</p> <p>This means that only users that authenticate with their correct Windows username and password will be able to use this profile. (*)</p>

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

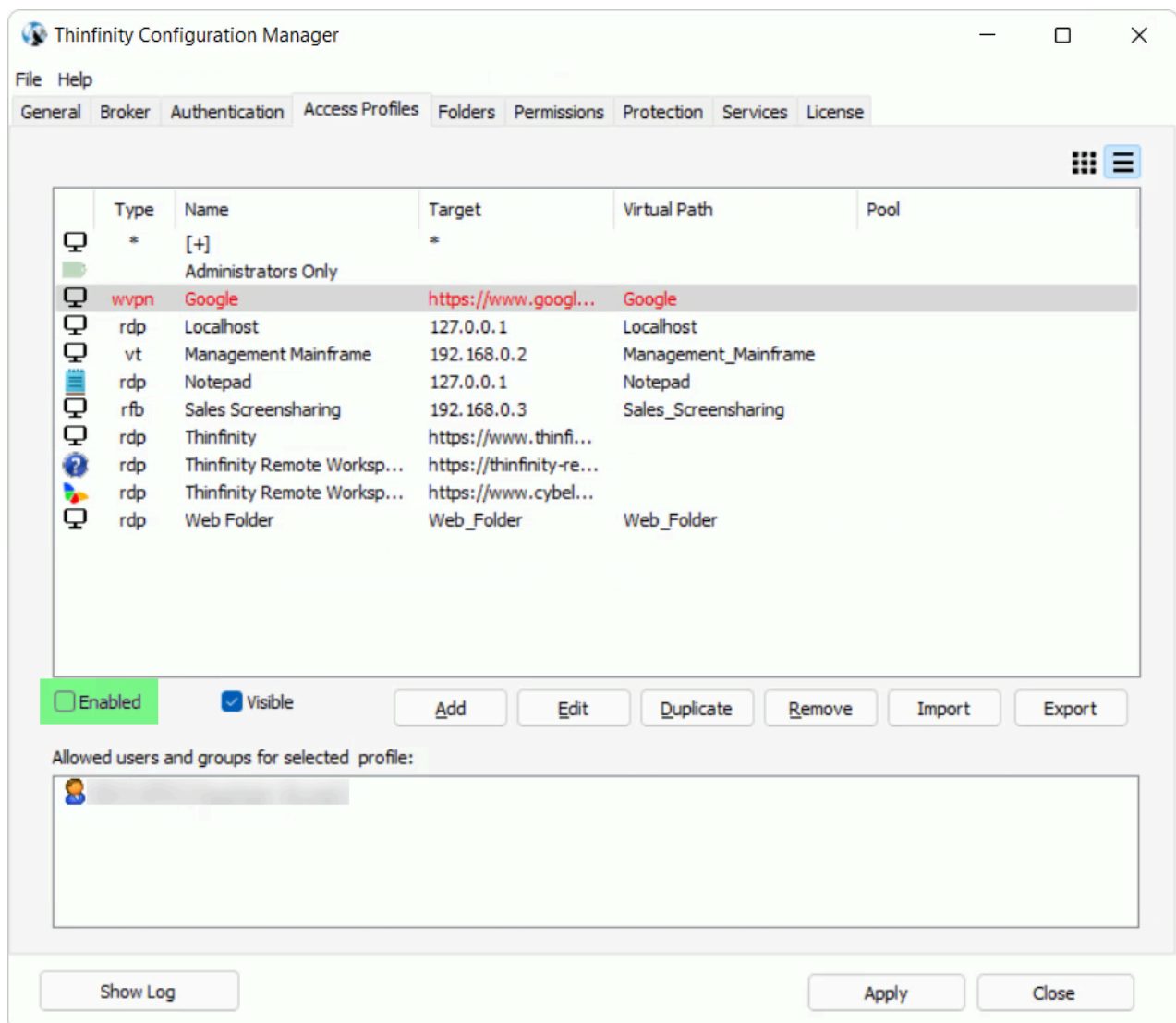
- When you are done, press '*Ok*'.

Disabling a Web VPN Access Profile

Disabling a Web VPN Access Profile will make it unavailable to all users.

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

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the [Access Profiles](#) topic first.
- Select the profile you want to disable.
- Click the check-box next to 'Enabled':

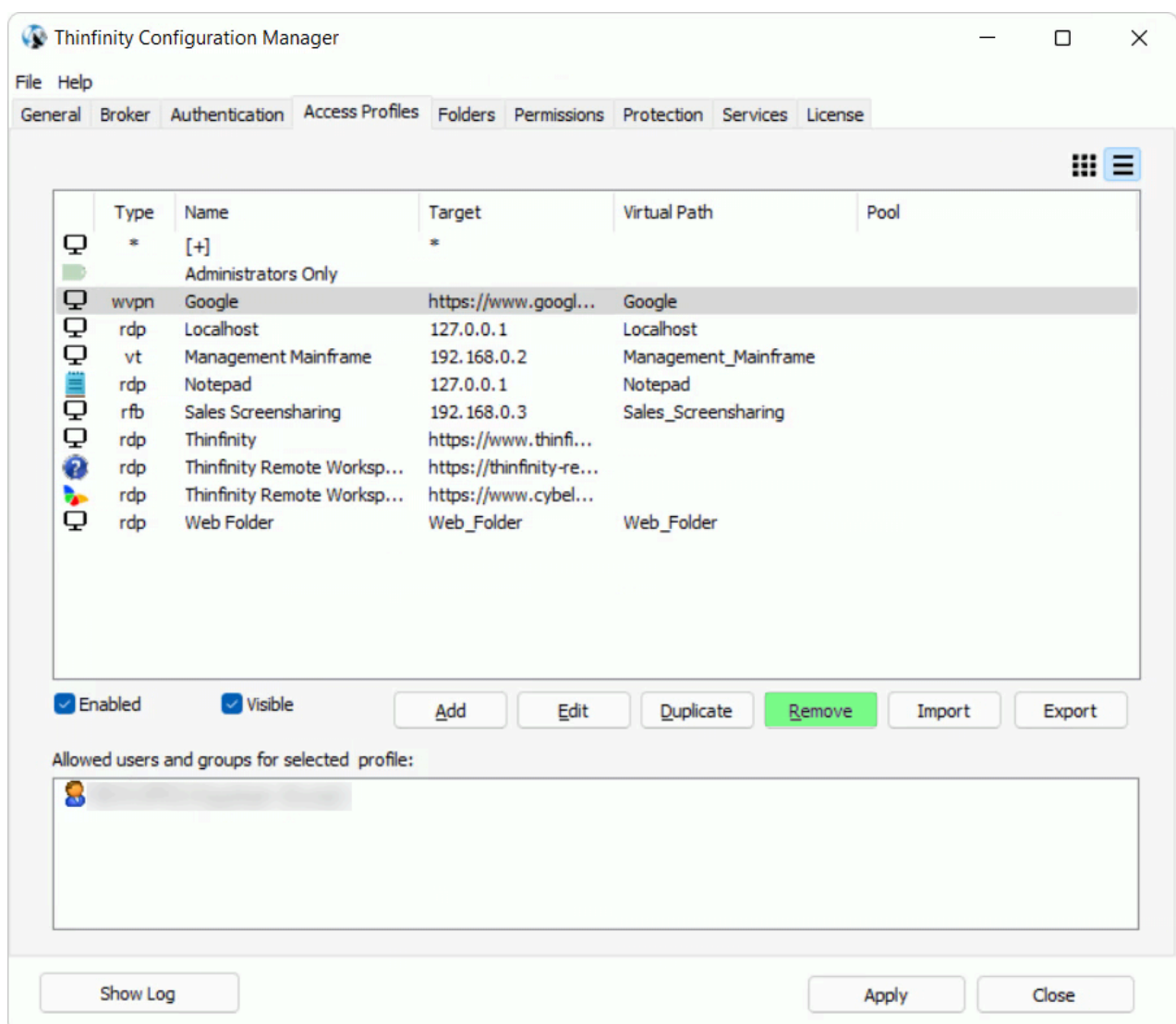


- Observe that the profile name will turn red.
- Press 'Apply' to save the changes.

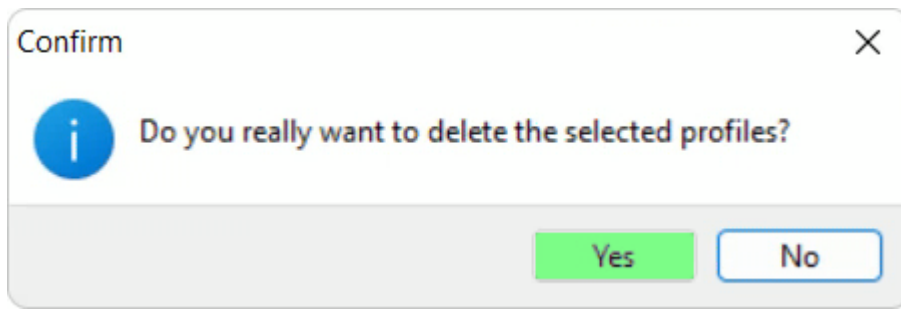
Removing a Web VPN Access Profile

Remember that once you remove a Web VPN Access Profile, you won't be able to recover it.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the topic [Access Profiles](#) first.
- Select the profile you want to remove.
- Press the 'Remove' button:



- Press 'Yes' on the confirmation message:



- Press '*Apply*' to save the changes.

Web Folder Access Profile

A Web Folder Access Profile gives users access to a shared folder from either the server where Thinfinity® Remote Workspace is installed, or some other server.

You'll find the steps to create, edit, disable and remove such Web Folder connections below:



Creating a Web Folder Access Profile

Thinfinity® Remote Workspace



Editing a Web Folder Access Profile

Thinfinity® Remote Workspace



Disabling a Web Folder Access Profile

Thinfinity® Remote Workspace



Removing a Web Folder Access Profile

Thinfinity® Remote Workspace



Creating a Web Folder Access Profile

- Go to the Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Add' > 'Web Folder' to create a new profile and the following window will be presented:

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

Buttons: None, New Key, Select Label

Tabs: General | Permissions | Restrictions | Access Hours | Authentication Methods

☒ Local server

Server URL:

Root Path:

☒ Use the authenticated credentials
☐ Ask for new credentials
☐ Use these credentials:

 User name:

 Password:

Buttons: Ok, Cancel

OPTION	DESCRIPTION
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: http(s)://ThinfinityDomain:port/VirtualPath/. The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Workspace web interface.
Access Key	Used in combination with Thinfinity® Remote Workspace 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.
Select Label	Prompts you to select an existing Label for this specific profile.
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.
Local server	With this option, you can point to a folder within the server where Thinfinity® Remote Workspace is installed.
Server URL	If ' <i>Local server</i> ' is disabled, you can point to the server with the folder you wish to share in here.
Root Path	Specify the path of the folder you wish to share.
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

- Read the next topic '[Editing a Web Folder Access Profile ↗](#)' to learn how to configure this profile.

You can find more information on each property that you can modify on the Web Link Profile Editor here:



Web Folder Profile Editor

Thinfinity® Remote Workspace



Editing a Web Folder Access Profile

Configuring a Web Folder Access Profile properly will allow you to take advantage of all its features and create an access scheme that would suit your company's needs best.

Remember that each profile defines a single computer's desktop or application access, except for the '[+]' profile that gives access to all computers.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Edit' to configure the profile and the following window will be presented:

Thinfinity Configuration Manager - Profile Editor

Name: Web Folder

Virtual Path: Web_Folder

Access Key: f0yaGmZiLf7ENSQmxHrL4KiaNjaMpU5

Label(s): \

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Permissions | Restrictions | Access Hours

☒ Local server

Server URL:

Root Path:

☒ Use the authenticated credentials

☐ Ask for new credentials

☐ Use these credentials:

User name:

Password:

Ok Cancel

- First of all, type in a descriptive name for the profile in the '*Name*' field.
- Specify the computer this profile will connect to, be it the '*Local server*' where this app is installed, or specify the '*Server URL*' of the server which contains the folder you wish to share. You would then need to point to the '*Root Path*' of the folder itself.
- Set the credentials to log into the remote machine:

OPTION	DESCRIPTION
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 Workspace, if this is the only profile the user has.

- Go to the '*Permissions*' tab and set up the permission preferences as follow:

OPTION	DESCRIPTION
Allow anonymous access	Use this option, if you want this profile to be available for everyone. This means that everybody accessing Thinfinity® Remote Workspace will see this profile. Checking this option will disable the user.
Group or users access	<p>To use specific users for this profile, uncheck "Allow anonymous access", press "Add" and choose the users and groups from the local domain.</p> <p>This means that only users that authenticate with their correct Windows username and password will be able to use this profile. (*)</p>

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

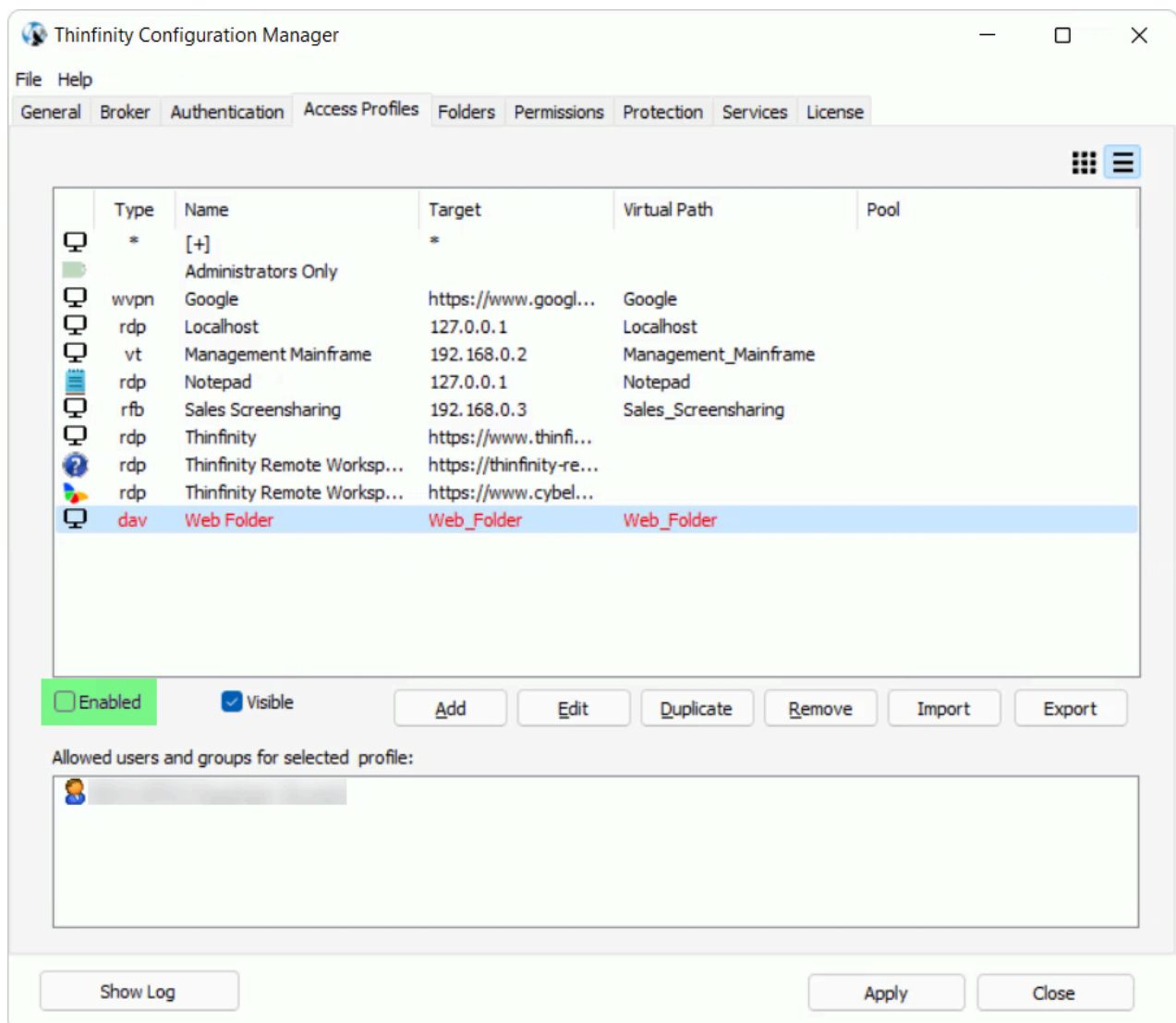
- When you are done, press '*Ok*'.

Disabling a Web Folder Access Profile

Disabling a Web Folder Access Profile will make it unavailable to all users.

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

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the [Access Profiles](#) topic first.
- Select the profile you want to disable.
- Click the check-box next to 'Enabled':

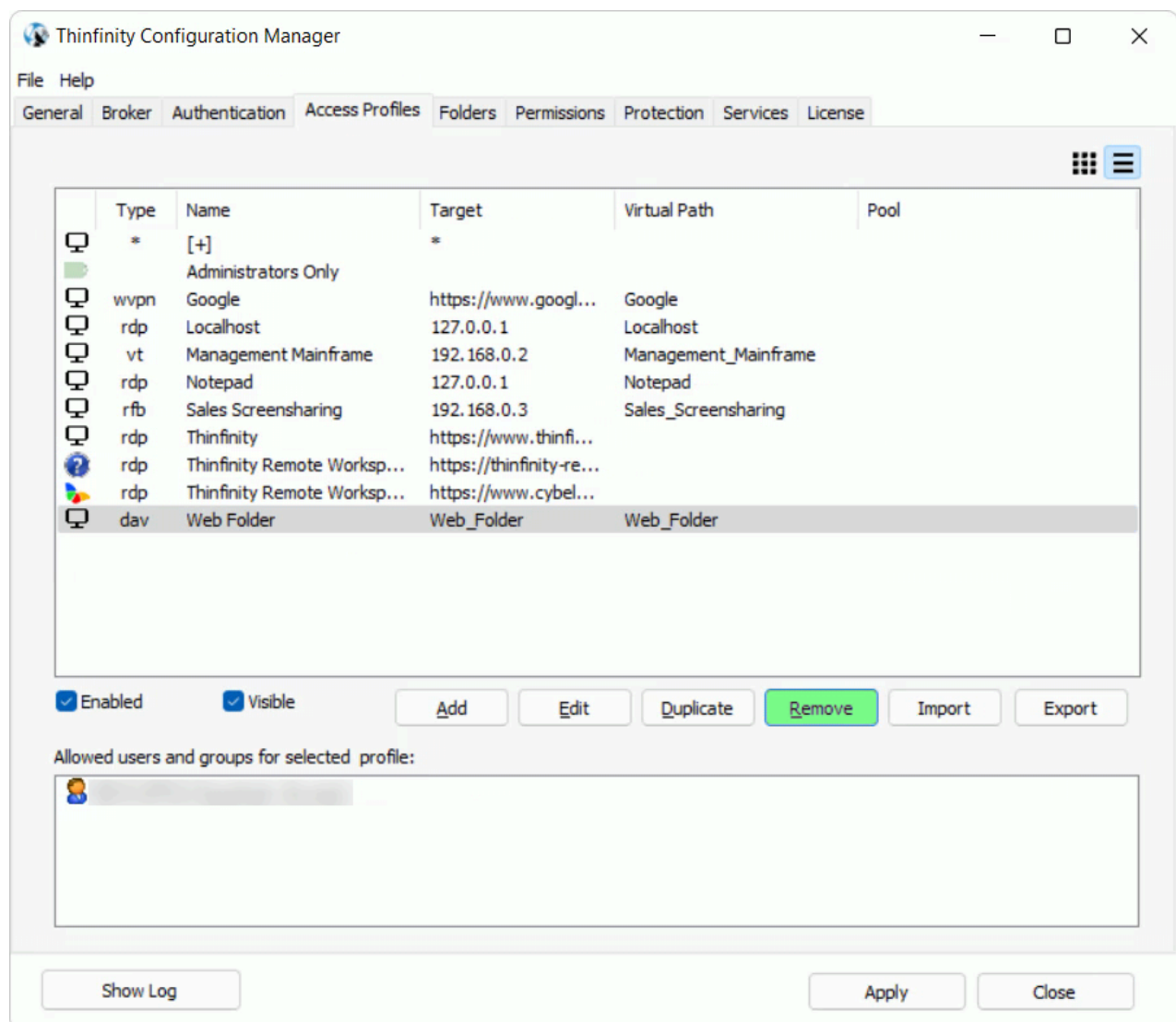


- Observe that the profile name will turn red.
- Press 'Apply' to save the changes.

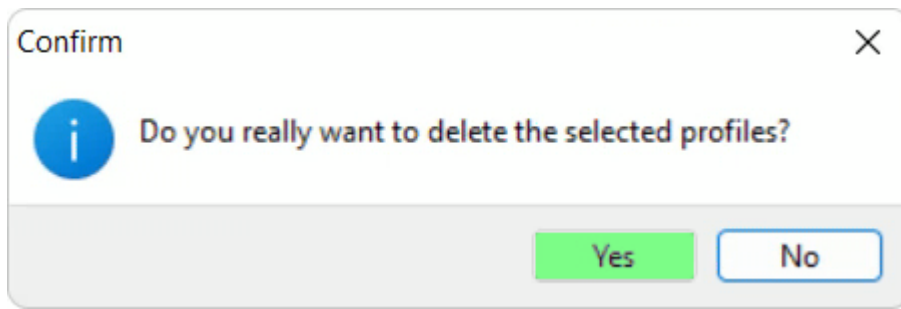
Removing a Web Folder Access Profile

Remember that once you remove a Web Folder Access Profile, you won't be able to recover it.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the topic [Access Profiles](#) first.
- Select the profile you want to remove.
- Press the 'Remove' button:



- Press 'Yes' on the confirmation message:



- Press '*Apply*' to save the changes.

Label Access Profile

A Label Access Profile is essentially a folder to place all your connections to better organize your Thinfinity® Remote Workspace landing page.

You'll find the steps to create, edit, disable and remove such Labels below:



Creating a Label Access Profile

Thinfinity® Remote Workspace



Editing a Label Access Profile

Thinfinity® Remote Workspace



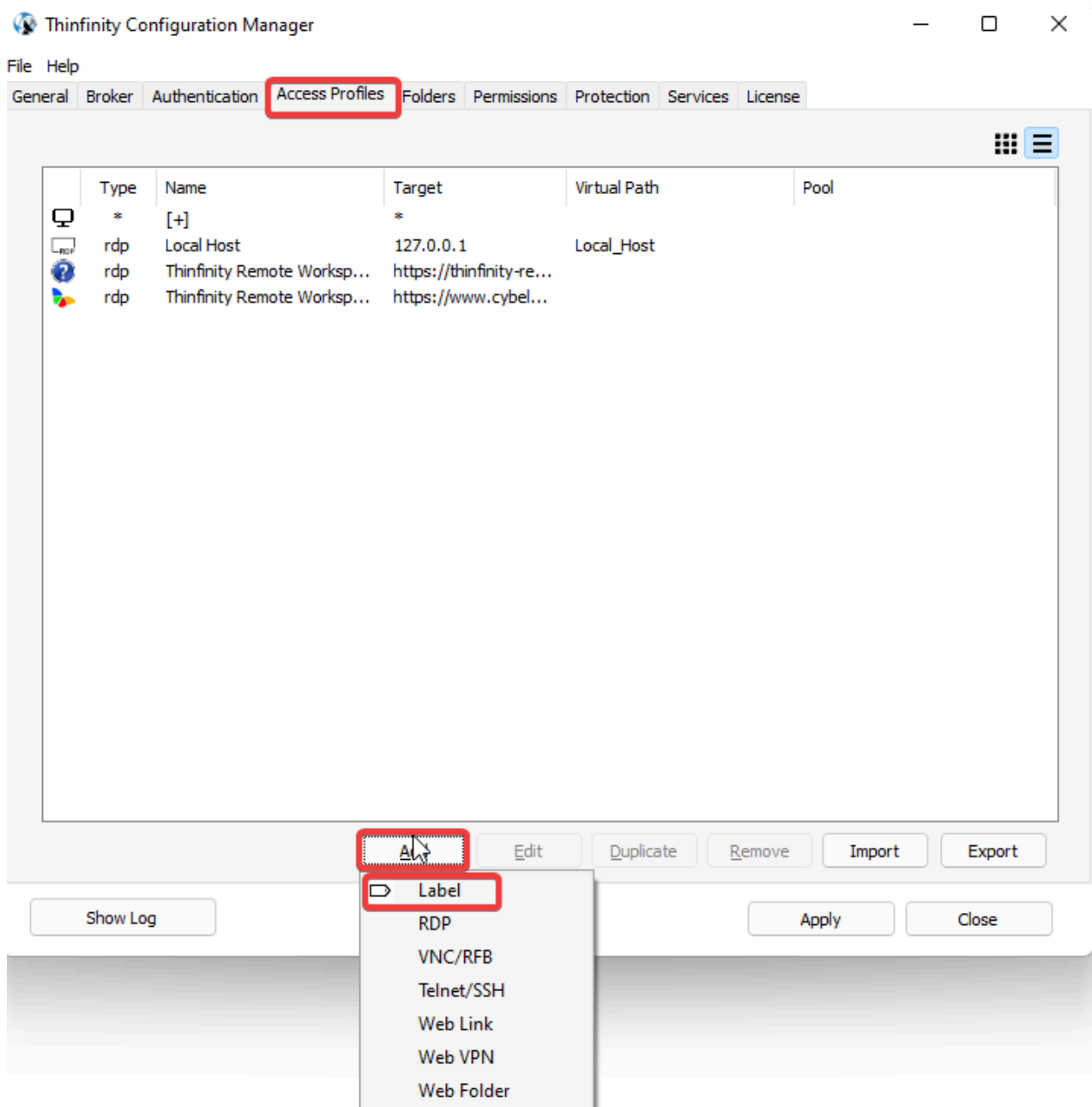
Removing a Label Access Profile

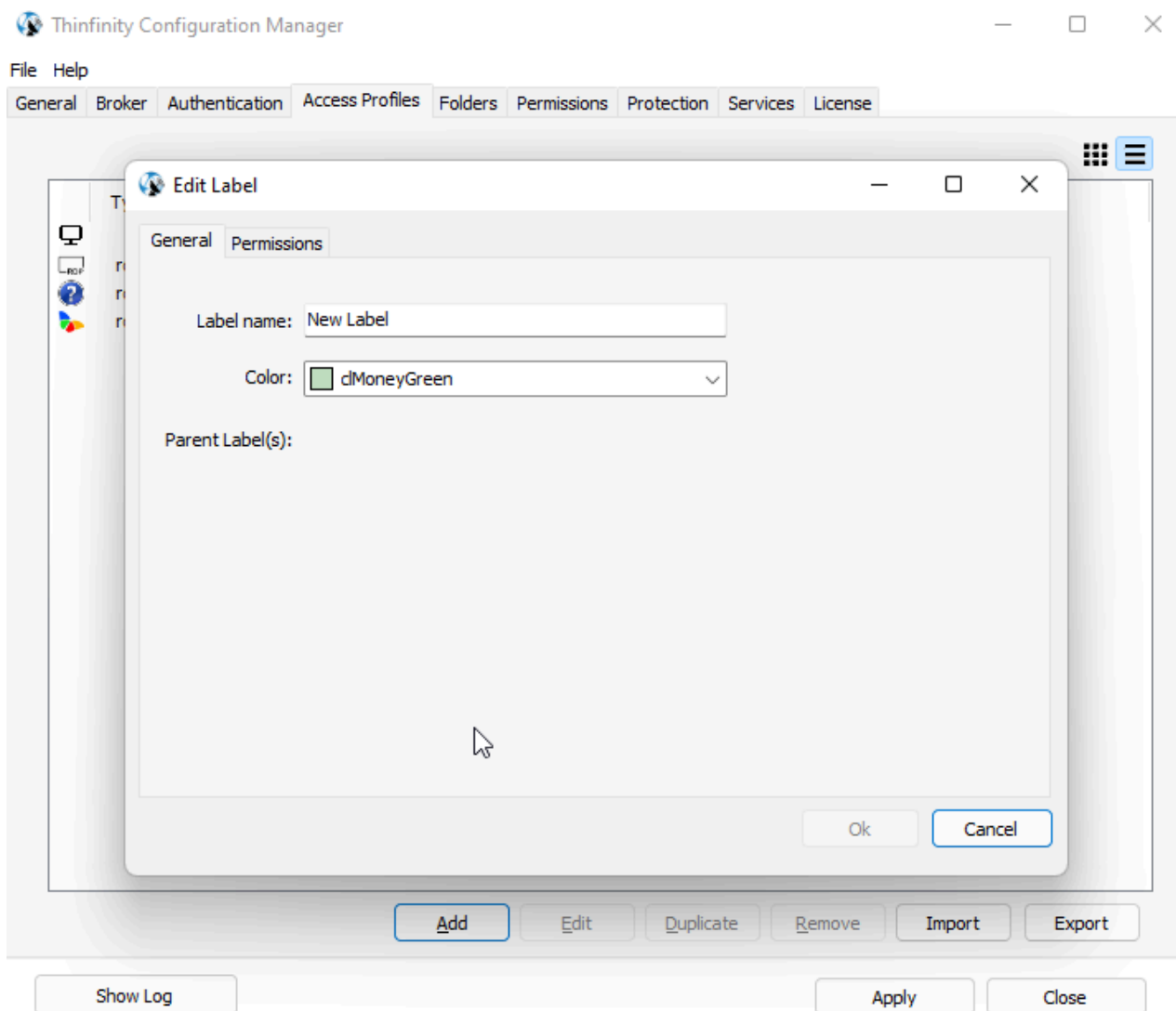
Thinfinity® Remote Workspace



Creating a Label Access Profile

- Go to the Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Add' > 'Label' to create a new profile and the following window will be presented:





OPTION	DESCRIPTION
Label name	Use this field to change the profile name. The profile name is shown to users to identify the Label.
Color	Specify the color of the Label for ease of access.
Parent Label(s)	If you're creating a Label within an existing Label, the latter will be shown here.

- Read the next topic '[Editing a Label Access Profile ↗](#)' to learn how to configure this profile.

Editing a Label Access Profile

Configuring a Label Access Profile properly will allow you to take advantage of all its features and create an access scheme that would suit your company's needs best.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab.
- Press 'Edit' to configure the Label and go to the 'Permissions' tab and the following window will be presented:

The screenshot shows a window titled 'Edit Label' with a close button (X) in the top right corner. It has two tabs: 'General' and 'Permissions', with 'Permissions' currently selected. Inside the 'Permissions' tab, there are two checkboxes: 'Inherit label access permissions' (checked) and 'Allow anonymous access' (unchecked). Below these is a table with two columns: 'Name' and 'Rights Access'. The table is currently empty. At the bottom of the table area, there is an unchecked checkbox for 'Admin permissions' and two buttons: 'Add' and 'Remove'. Below the table area, there is a text box containing the message: 'Access permissions will be applied to children objects without specific permissions. Edit permissions apply to label and all children objects.' Below this text box is an unchecked checkbox for 'Reset all child object permissions entries'. At the bottom right of the window are 'Ok' and 'Cancel' buttons.

OPTION	DESCRIPTION
Inherit label access permissions	
Allow anonymous access	Use this option, if you want this profile to be available for everyone. This means that everybody accessing Thinfinity® Remote

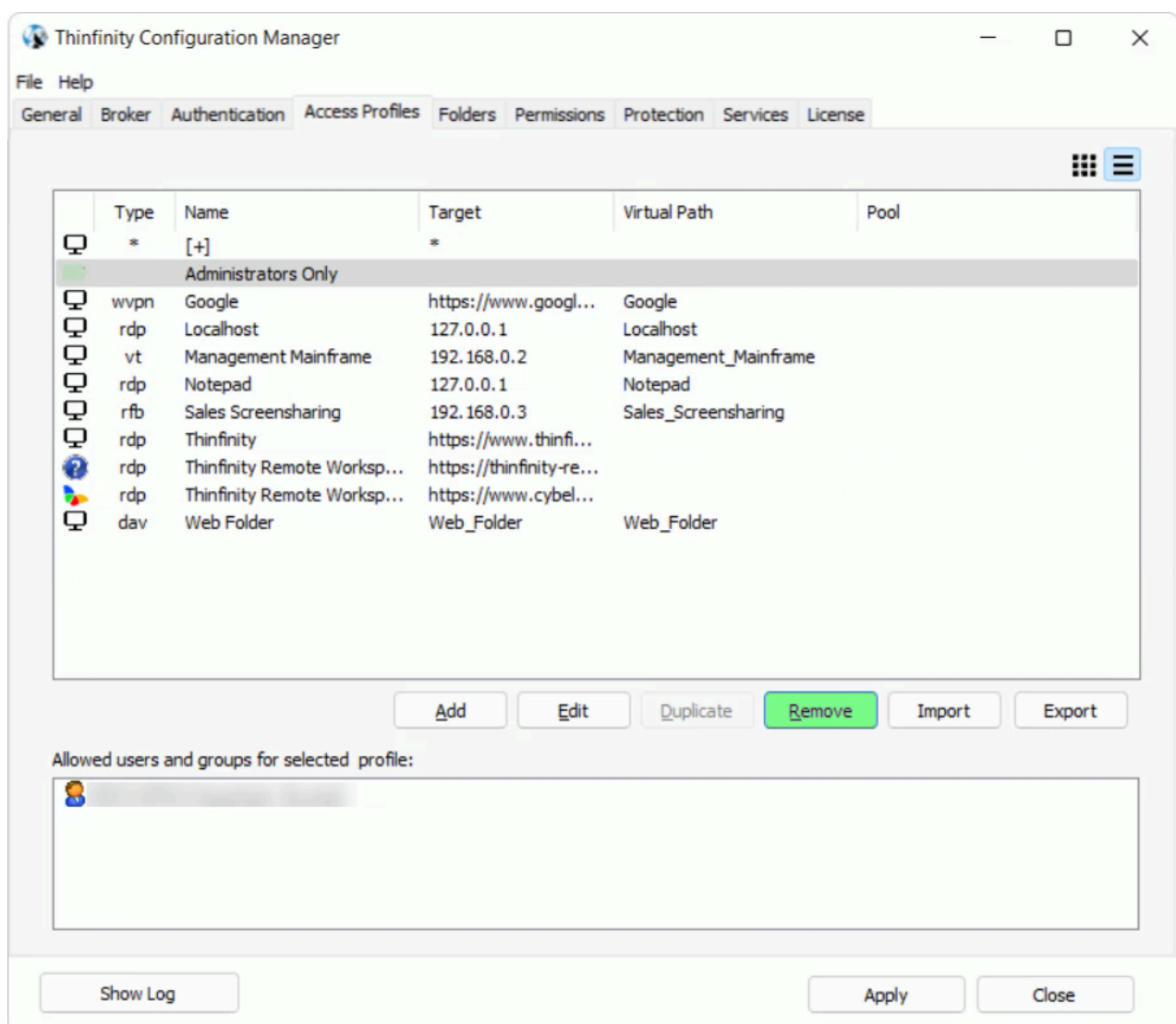
Admin permissions	Workspace will see this profile. Checking this option will disable the user. .
Reset all child object permission entries	

- When you are done, press '*Ok*'.

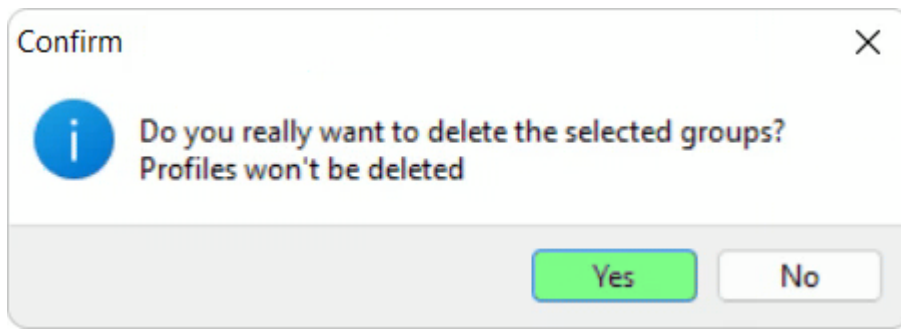
Removing a Label Access Profile

Remember that once you remove a Label Access Profile, you won't be able to recover it.

- Go to Thinfinity® Remote Workspace Configuration Manager's 'Access Profiles' tab. If it is not there, read the topic [Access Profiles](#) first.
- Select the profile you want to remove.
- Press the 'Remove' button:



- Press 'Yes' on the confirmation message:



- Press '*Apply*' to save the changes.

The '[+]' Access Profile

The '[+]' profile is the default profile for Thinfinity® Remote Workspace.

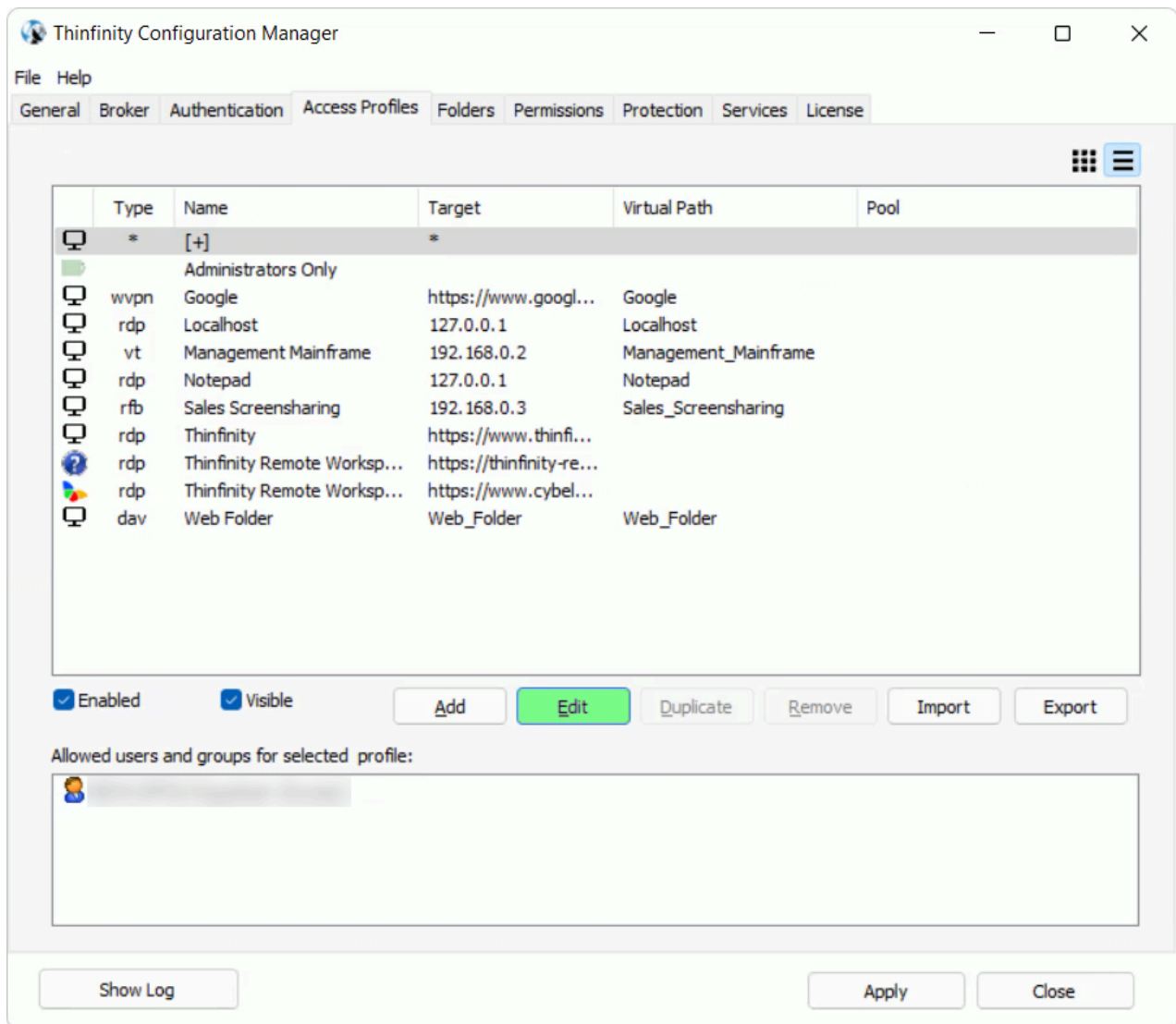
It has two special behaviors:

- Allows access to all computers
- Let users choose freely their own settings at the moment of connection

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:

- Select the '[+]' profile
- Observe that the '*Remove*' option is still disabled. That's because this profile cannot be removed
- Click on the '*Edit*' option:



- Uncheck '*Allow anonymous access*'
- Click on '*Add*' to select the users who will be granted with the '[+]' profile:

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible

Permissions | Restrictions | Authentication Methods

☒ Inherit label access permissions

☐ Allow anonymous access

Group or user names:

RDP Profile Editor

The Profile Editor is the tool to create, configure and edit Thinfinity® Remote Workspace's Access Profiles.

This section details the RDP Profile Editor:

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

None

New Key

Select Label

☒ Visible

☐ Default profile

☒ RDP

☐ RDS Web Feed

General

Display

Resources

Program

Experience

Advanced

Printer

Permissions

Restrictions

Access Hours

Auth

Computer:

Broker Pool:

☐ Connect to a Hyper-V Virtual Machine

Session Limit: Minutes

☐ Connect to a Virtual Desktop on an RDS Collection

☐ Enable Wake-on-LAN (WoL)

Credentials:

☒ Use the authenticated credentials

☐ Ask for new credentials

☐ Use these credentials: ☐ Create if it doesn't exist

User name:

Password:

Ok

Cancel

These are the profile properties you can edit:

OPTION	DESCRIPTION
Name	Use this field to change the profile name. The profile name is shown to users to

	<p>identify the connection.</p> <p>The Virtual Path will create a unique URL address for this connection. The complete path will consist of: http(s)://ThinfinityDomain:port/VirtualPath/. The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Workspace web interface.</p>
Virtual Path	
Access Key	Used in combination with Thinfinity® Remote Workspace 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.
Select Label	Prompts you to select an existing Label for this specific profile.
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.
Visible	If checked, the Access Profile will be visible on the Thinfinity® Remote Workspace landing page.
Default profile	If checked, the Thinfinity® Remote Workspace landing page will be skipped and connect directly to this profile.
RDP/RDS Web Feed	Select the 'RDP' option to have a regular profile that connects to a remote machine or application through RDP. Select the 'RDS Web Feed' option to pull the Microsoft RD Web Access connections into the web interface.

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

General

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'General' tab is selected. The form contains the following fields and options:

- Name:** Localhost
- Virtual Path:** Localhost
- Access Key:** tiYlfmYqip8tN2Va3WSkrK1vGNfvTLby
- Label(s):** \
- Buttons:** None, New Key, Select Label
- Checkboxes:**
 - ☒ Visible
 - ☐ Default profile
 - ☒ RDP
 - ☐ RDS Web Feed
- Tabs:** General, Display, Resources, Program, Experience, Advanced, Printer, Permissions, Restrictions, Access Hours, Auth
- Computer:** 127.0.0.1
- Broker Pool:** (empty)
- Session Limit:** 0 Minutes
- Connect to a Hyper-V Virtual Machine:** ☐
- Connect to a Virtual Desktop on an RDS Collection:** ☐
- Enable Wake-on-LAN (WoL):** ☐
- Credentials:**
 - ☒ Use the authenticated credentials
 - ☐ Ask for new credentials
 - ☐ Use these credentials:
 - ☐ Create if it doesn't exist
 - User name:** (empty)
 - Password:** (empty)
- Buttons:** Ok, Cancel

You can find the following options on the RDP Profile Editor's '*General*' tab:

OPTION	DESCRIPTION
Computer	Specify the computer that this profile will connect to. Enter the internal IP or computer name.
Connect to a Hyper-V Virtual Machine	Check this option if you want to connect to a Hyper-V Virtual Machine through its machine ID or GUID. Learn in details how to set up a Hyper-V profile .

	If you are able to connect to the Virtual Machine through its IP address or computer name, you can use a regular profile set up, and this option might not be necessary.
Connect to a Virtual Desktop on an RDS Collection	Check this option if you want to connect to a Virtual Machine located within an RDS Collection. Learn in details how to set up a RDS Collection profile .
Enable Wake-on-LAN (WoL)	Check this option if you want to allow a computer to be turned on or awakened by a network message.
Broker Pool	Specify which broker pool this profile belongs to.
Session Limit	Set up a session time limit for this profile.

Credentials

Choose the credentials for logging into the specified computer:

Use the authenticated credentials	<p>Use the same credentials entered in the browser for Thinfinity® Remote Workspace (specified in the "Permissions" tab).</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 Workspace if this is the only profile for their credentials.</p>
Ask for new credentials	Prompt the user for new credentials to access the computer.
Use these credentials	<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 Workspace if this is the only profile for their credentials.</p>

Setting up a Hyper-V Profile

The screenshot shows the 'General' tab of a configuration window for a Hyper-V profile. The window has a title bar with standard OS controls and a tabbed interface. The 'General' tab is active, showing fields for 'Computer' (a dropdown), 'Broker Pool' (a text field), and 'Session Limit' (a spinner set to 0 minutes). Below these are three checkboxes: 'Connect to a Hyper-V Virtual Machine' (checked), 'Connect to a Virtual Desktop on an RDS Collection' (unchecked), and 'Enable Wake-on-LAN (WoL)' (unchecked). The 'Credentials' section has three radio buttons: 'Use the authenticated credentials' (selected), 'Ask for new credentials' (unselected), and 'Use these credentials' (unselected). The 'Use these credentials' option is disabled, and there is a 'Create if it doesn't exist' checkbox. Below the radio buttons are 'User name' and 'Password' text fields. At the bottom, there is a 'Virtual machine id' text field and a 'Browse...' button. The 'Ok' and 'Cancel' buttons are at the bottom right.

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:

- Add a new profile.
- On the '*Computer*' field, inform the Hyper-V Server name or IP address.
- Check the option '*Connect to a Hyper-V Virtual Machine*'.
- Complete the '*Credentials*' necessary to authenticate against the Hyper-V Virtual Machine.
- If you know the Virtual Machine ID (GUID), you can inform it on the field '*Virtual machine*' and skip the next step.
- If you don't know the Virtual Machine GUID, click on the '*Browse*' button and a search dialog will be presented:

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

Select Hyper-V Virtual Machine

Hyper-V Server:

☐ Use these credentials:

User name:

Password:

Connect

Virtual Machines

Name	VMID
------	------

Ok Cancel

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

c. Once the Collection is selected you can double-click on it or click on 'Ok'.

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

- The other profile settings should be configured like any regular profile (Display, Resources, Program, Experience, Advanced, Printer, Permissions, Restrictions, Access Hours, Authentication Methods)
- Once you are done configuring the profile, press 'Ok' and then 'Apply'.

Setting up an RDS Collection Profile

The screenshot shows the 'General' tab of the RDS Collection Profile configuration window. The 'Computer' dropdown is highlighted in green. Below it, the 'Connect to a Virtual Desktop on an RDS Collection' checkbox is checked and highlighted in green. The 'Credentials' section has three radio buttons: 'Use the authenticated credentials' (selected), 'Ask for new credentials', and 'Use these credentials:'. The 'Use these credentials' option has a 'Create if it doesn't exist' checkbox. Below this are 'User name:' and 'Password:' text boxes. At the bottom, the 'TSV URL:' field is highlighted in green, with the text 'TSC://VMResource.1RD_Collection-Sa' entered. A 'Browse...' button is next to it. The 'Ok' and 'Cancel' buttons are at the bottom right.

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:

- Add a new profile.
- On the Profile Editor, inform the RDS server name or IP address.
- Check the option '*Connect to a Virtual Desktop on an RDS Collection*'.
- Complete the '*Credentials*' fields to authenticate against the virtual machine.
- 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.
- If you don't know the TSV URL, click on the '*Browse*' button and the following search dialog will be presented:

Select RDS Collection

Connection Broker Server:

☐ Use a Personal Virtual Desktop Collection

☒ Use a Pooled Virtual Desktop Collection

☐ Use a Session Collection

☐ Use these credentials:

User name:

Password:

Connect

RDS Collections

Farm Name

Ok Cancel

- a. Select whether you want to search for Personal or Pooled Virtual Desktop Collections.
 - b. Click on the Connect button. If necessary, inform the credentials to authenticate against the RDS Server.
 - c. The Collections found on the server will be presented on the bottom list. Select the one you want to create a profile for.
 - d. Once the Collection is selected you can double-click on it or click on the OK button.
 - e. The TSV URL will be set on the correspondent field.
- The other profile settings should be configured like any regular profile (Display, Resources, Program, Experience, Advanced, Printer, Permissions, Restrictions,

Access Hours, Authentication Methods).

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

Display

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General **Display** Resources Program Experience Advanced Printer Permissions Restrictions Access Hours Auth

Color Depth:

Resolution:

Image Quality:

☒ Update session resolution on resize

You can find the following options on the RDP Profile Editor's '*Display*' tab:

OPTION	DESCRIPTION
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	<p>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.</p>
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>

Resources

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General | Display | **Resources** | Program | Experience | Advanced | Printer | Permissions | Restrictions | Access Hours | Auth

☒ Enable Clipboard

☒ Enable Intermediate Disk

Disk name:

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

☒ Automatically download any newly-added file

☐ Disable these file extensions:

☒ Enable Sound

Sound quality:

You can find the following options on the RDP Profile Editor's '*Resources*' tab:

OPTION	DESCRIPTION
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 Workspace 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.
	Determines the quality that Thinfinity® Remote Workspace will use to reproduce

The settings.ini configuration file can be found on this path:

C:\ProgramData\Cybele Software\Thinfinity\Workspace\DB\settings.ini

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 Workspace 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].*$
```

Program

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Program' tab is selected, showing the 'On Connection' dropdown menu set to 'Do Nothing'. The window includes fields for Name, Virtual Path, Access Key, and Label(s), as well as checkboxes for Visible, Default profile, RDP, and RDS Web Feed. The 'On Connection' dropdown is located in the main area of the 'Program' tab.

Thinfinity Configuration Manager - Profile Editor

Name: Localhost

Virtual Path: Localhost

Access Key: tiYlfmYqjp8tN2Va3WSkrK1vGNfvTLby

Label(s): \

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General | Display | Resources | **Program** | Experience | Advanced | Printer | Permissions | Restrictions | Access Hours | Auth

On Connection: Do Nothing

Ok Cancel

On the '*Program*' 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.

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 | Restrictions | Access Hours | Auth...

On Connection: Start a Program ▼

Program path and file name:
C:\Windows\notepad.exe

Arguments:

Start in the following folder:
C:\Windows\notepad.exe

Ok Cancel

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

OPTION	DESCRIPTION
Program path and file name	Specify the complete path to give access the application you want to start with the connection. Right after the path you should also inform the application arguments, if they exist.
Arguments	Applications arguments.
Start in the following folder	Inform a context directory for the program set on the field "Program path and file name".

Launch RemoteApp:

The RemoteApp is a Terminal Services feature that allows Windows®-based application publishing. You can connect to an application using RemoteApp through

Thinfinity® Remote Workspace by selecting the '*Execute as RemoteApp*' on the '*Program*' tab.

This feature is only available within Windows Server versions.

The screenshot shows the 'Program' tab of the Thinfinity Remote Workspace configuration window. The 'On Connection' dropdown is set to 'Execute as RemoteApp'. Below it, the 'Program path and file name' field contains 'C:\Windows\notepad.exe'. The 'Arguments' field is empty. The 'Start in the following folder' field also contains 'C:\Windows\notepad.exe'. At the bottom, the checkbox 'Show Windows Login and Logout Screen' is checked. The 'Ok' and 'Cancel' buttons are at the bottom right.

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

OPTION	DESCRIPTION
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.

Experience

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General | Display | Resources | Program | **Experience** | Advanced | Printer | Permissions | Restrictions | Access Hours | Auth

Browser: ☒ Smart sizing

Input: ☐ Multitouch redirection

Graphics: ☐ Remote FX ☐ H264

☐ Desktop background

☒ Visual styles

☐ Menu and window animation

☒ Font smoothing

☐ Show window contents while dragging

☐ Desktop Composition

You can find the following options on the RDP Profile Editor's '*Experience*' tab:

OPTION	DESCRIPTION
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	<p>Check this option to configure the DWM to redirected the desktop drawing to off-screen surfaces in video memory.</p> <p>Also, the desktop will present many visual</p>

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

Advanced

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General | Display | Resources | Program | Experience | **Advanced** | Printer | Permissions | Restrictions | Access Hours | Auth

☒ Unicode keyboard

Keyboard layout:

☐ Connect to console session

☐ Disable NLA login

TLS version:

☒ Websocket compression

☐ Record remote desktop session

Touch Behavior:

☒ Drag to relative mouse movements

Touch to hold delay: milliseconds

Minimum drag distance: pixels

You can find the following options on the RDP Profile Editor's '*Advanced*' tab:

OPTION	DESCRIPTION
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	<p>Check this option to enable the compression for the exchanged Websocket data and have the application performance improved.</p> <p>It only works in browsers which have the websockets compression implemented and enabled.</p>
Record Remote Desktop Session	<p>Enable to record the remote desktop session when connecting to this profile.</p> <p>Read more about the Save Session feature.</p>
Drag to relative mouse movement	<p>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.</p> <p>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.</p>
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.

Printer

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General | Display | Resources | Program | Experience | Advanced | **Printer** | Permissions | Restrictions | Access Hours | Auth...

☒ Enable a Remote Printer

Printer name:

PostScript printer driver:

☒ Set as default printer

Ok Cancel

You can find the following options on the RDP Profile Editor's '*Printer*' tab:

OPTION	DESCRIPTION
Enable a Remote Printer	Uncheck this option to disable Thinfinity® Remote Workspace PDF printer.
Printer name	Specify the printer name that you want to be shown on the remote machine's printer list.
	This is the driver to be used by Thinfinity® Remote Workspace in order to print the

PostScript printer driver	<p>remote documents.</p> <p>The "<i>HP Color Laser Jet 2800 Series PS</i>" driver is compatible with 2008 Windows versions.</p> <p>The "<i>HP Color LaserJet 8500 PS</i>" driver is compatible with 2003 Windows versions.</p> <p>The "<i>Microsoft XPS Document Writer V4</i>" driver is compatible with Windows Server 2012 and Windows 8.</p> <p>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	<p>Mark this option to make Thinfinity® Remote Workspace printer the remote machine default printer.</p>

Permissions

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Permissions' tab is selected. The 'Access' section contains the following options:

- ☒ Inherit label access permissions
- ☐ Allow anonymous access
- Group or user names: (Empty text box)
- ☐ Booked access only
- Buttons: Add, Remove

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

You can find the following options on the RDP Profile Editor's '*Permissions*' tab:

Inherit label access permissions

Check this option if the Profile in question belongs to a Label with access permissions already configured on it.

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 Workspace will see this profile. Checking

	this option will disable the Add and Remove buttons.
Booked access only	Check this option if you wish for this profile to be access solely through booking.
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.

Restrictions

Thinfinitiy Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General | Display | Resources | Program | Experience | Advanced | Printer | Permissions | **Restrictions** | Access Hours | Auth

☒ No restrictions

☐ Allow only from these IPs

☐ Block connections from these IPs

If the list is empty, all IP addresses will be authorized

On the RDP Profile Editor's '*Restrictions*' tab, you can white list or black list the IP addresses which are allowed to connect to the configured application.

OPTION	DESCRIPTION
No restrictions	No restriction over which IP Addresses will be able to connect to the application.
Allow only from these IPs	Allow connections from the listed IP Addresses.

Block connections from these IPs	Block connections from the listed IP Addresses.
Add	Add an IP Address to the list

Access Hours

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

☒ RDP ☐ RDS Web Feed

General | Display | Resources | Program | Experience | Advanced | Printer | Permissions | Restrictions | **Access Hours** | Auth

All	0	2	4	6	8	10	12	2	4	6	8	10
Sunday	*	*	*	*	*	*	*	*	*	*	*	*
Monday	*	*	*	*	*	*	*	*	*	*	*	*
Tuesday	*	*	*	*	*	*	*	*	*	*	*	*
Wednesday	*	*	*	*	*	*	*	*	*	*	*	*
Thursday	*	*	*	*	*	*	*	*	*	*	*	*
Friday	*	*	*	*	*	*	*	*	*	*	*	*
Saturday	*	*	*	*	*	*	*	*	*	*	*	*

☒ Access Allowed ☐ Access Denied

☐ Allow access only within this period:

to

Ok Cancel

On the RDP Profile Editor's '*Access Hours*' tab, you can define the day and time your application will be available to your users.

OPTION	DESCRIPTION
Access Permitted	Define which day and hour the application will be available.
Access Denied	Define which day and hour the application will be disabled.



Authentication Methods

Thinfinity Configuration Manager - Profile Editor

Name: Localhost

Virtual Path: Localhost

Access Key: tiYlfmYqjp8tN2Va3WSkrK1vGNfvTLby

Label(s): \

Visible ☒ Default profile ☐

RDP ☒ RDS Web Feed ☐

Program | Experience | Advanced | Printer | Permissions | Restrictions | Access Hours | **Authentication Methods**

☐ No restrictions

☒ Only users authenticated with these methods:

Name	Type
<input checked="" type="checkbox"/> Windows Logon	Built-in
<input checked="" type="checkbox"/> API Access	{0FF2D795-FD58-4E4A-94CD-CA68B...
<input checked="" type="checkbox"/> Radius	Built-in
<input checked="" type="checkbox"/> SAML	SAML
<input checked="" type="checkbox"/> Google	OAuth
<input checked="" type="checkbox"/> Facebook	OAuth
<input checked="" type="checkbox"/> LinkedIn	OAuth
<input checked="" type="checkbox"/> Dropbox	OAuth
<input checked="" type="checkbox"/> Azure	OAuth
<input checked="" type="checkbox"/> ForgeRock	OAuth
<input checked="" type="checkbox"/> Okta	OAuth
<input checked="" type="checkbox"/> OAuth	OAuth

Ok Cancel

On the RDP Profile Editor's '*Authentication Methods*' tab, you can define which application will be available after authenticating to Thinfinity® Remote Workspace.

The Authentication Methods available in the list are those configured in the '*Authentication*' tab of the Thinfinity® Configuration Manager.

OPTION	DESCRIPTION
No restrictions	No restriction on the authentication method used.

Only users authenticated with these
.. ..

Only the users authenticated with the
selected methods will be able to see and

VNC/RFB Profile Editor

The Profile Editor is the tool to create, configure and edit Thinfinity® Remote Workspace's Access Profiles.

This section details the VNC/RFB Profile Editor:

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

None

New Key

Select Label

☒ Visible

☐ Default profile

General

Display

Permissions

Restrictions

Access Hours

Authentication Methods

Computer:

Port:

Broker Pool:

Session Limit: Minutes

Password:

☐ Enable Wake-on-LAN (WoL)

Ok

Cancel

These are the profile properties you can edit:

OPTION	DESCRIPTION
Name	Use this field to change the profile name. The profile name is shown to users to

Virtual Path	<p>identify the connection.</p> <p>The Virtual Path will create a unique URL address for this connection. The complete path will consist of:</p> <p>http(s)://ThinfinityDomain:port/VirtualPath/.</p> <p>The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Workspace web interface.</p>
Access Key	Used in combination with Thinfinity® Remote Workspace 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.
Select Label	Prompts you to select an existing Label for this specific profile.
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.
Visible	If checked, the Access Profile will be visible on the Thinfinity® Remote Workspace landing page.
Default profile	If checked, the Thinfinity® Remote Workspace landing page will be skipped and connect directly to this profile.

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

General

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'General' tab is selected, showing fields for Name, Virtual Path, Access Key, Label(s), Visible checkbox, and Default profile checkbox. Below these are tabs for Display, Permissions, Restrictions, Access Hours, and Authentication Methods. The 'General' tab content includes fields for Computer, Port, Password, Broker Pool, Session Limit, and an 'Enable Wake-on-LAN (WoL)' checkbox. At the bottom are 'Ok' and 'Cancel' buttons.

Thinfinity Configuration Manager - Profile Editor

Name: Sales Screensharing

Virtual Path: Sales_Screensharing

Access Key: tiae9PR.\$GVI7N7Vq39apacm\$znuBbz\$X

Label(s): \

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Display | Permissions | Restrictions | Access Hours | Authentication Methods

Computer: 192.168.0.3

Port: 5900

Password:

Broker Pool:

Session Limit: 0 Minutes

☐ Enable Wake-on-LAN (WoL)

Ok Cancel

You can find the following options on the VNC/RFB Profile Editor's '*General*' tab:

OPTION	DESCRIPTION
Computer	Use this field to change the profile name. The profile name is shown to users to identify the connection.
Port	Port used by the VNC/RFB server installed on the destination machine.

Password	Password configured in the VNC/RFB server installed on the destination machine
Broker Pool	Specify which broker pool this profile belongs to

Display

Thinfinity Configuration Manager - Profile Editor

Name: Sales Screensharing

Virtual Path: Sales_Screensharing

Access Key: tiae9PR.\$GVI7N7Vq39apacm\$znuBbz\$X

Label(s): \

☒ Visible ☐ Default profile

General | **Display** | Permissions | Restrictions | Access Hours | Authentication Methods

Color Depth: True Color

Encoding: ZRLE

Custom Compression Level: 6

Jpeg Compression Level: 6

Image Quality: Optimum

☒ Allow CopyRect encoding

☐ Show wallpaper

☒ Smart scaling

☐ Cursor shape updates

Ok Cancel

You can find the following options on the VNC/RFB Profile Editor's '*Display*' tab:

OPTION	DESCRIPTION
Color Depth	Choose the color depth for the remote computer view.
Encoding	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.

Custom Compression Level	Sets the level of image compression.
Jpeg Compression Level	Sets the level of JPEG compression.
Image Quality	Sets the quality level of the screen
Allow CopyRect encoding	Useful when moving windows in the remote session.
Show Wallpaper	Display the remote session wallpaper.
Smart Scaling	Enables Smart Scaling.

Permissions

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Permissions' tab is selected. The 'Access' section contains the following options:

- ☒ Inherit label access permissions
- ☐ Allow anonymous access
- Group or user names: (Empty text box)
- ☐ Booked access only

Buttons at the bottom right of the 'Access' section: Add, Remove. Buttons at the bottom of the window: Ok, Cancel.

You can find the following options on the VNC/RFB Profile Editor's '*Permissions*' tab:

Inherit label access permissions

Check this option if the Profile in question belongs to a Label with access permissions already configured on it.

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®

	Workspace 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.

Restrictions

The screenshot shows the 'Thinfinitiy Configuration Manager - Profile Editor' window. The 'Restrictions' tab is selected. The form contains the following fields and options:

- Name:** Sales Screensharing
- Virtual Path:** Sales_Screensharing
- Access Key:** tia9PR.\$GVI7N7Vq39apacm\$znuBbz\$X
- Label(s):** \
- Buttons:** None, New Key, Select Label
- Checkboxes:** ☒ Visible, ☐ Default profile
- Tabs:** General | Display | Permissions | **Restrictions** | Access Hours | Authentication Methods
- Restrictions Options:**
 - ☒ No restrictions
 - ☐ Allow only from these IPs
 - ☐ Block connections from these IPs
- IP List:** A large empty rectangular box for listing IP addresses.
- Text:** If the list is empty, all IP addresses will be authorized
- Buttons:** Add, Remove, Ok, Cancel

On the VNC/RFB Profile Editor's '*Restrictions*' tab, you can white list or black list the IP addresses which are allowed to connect to the configured application.

OPTION	DESCRIPTION
No restrictions	No restriction over which IP Addresses will be able to connect to the application.
Allow only from these IPs	Allow connections from the listed IP Addresses.

Block connections from these IPs	Block connections from the listed IP Addresses.
Add	Add an IP Address to the list

Access Hours

Thinfinity Configuration Manager - Profile Editor

Name: Sales Screensharing

Virtual Path: Sales_Screensharing

Access Key: tia9PR\$GVI7N7Vq39apacm\$znuBbz\$X

Label(s): \

☒ Visible ☐ Default profile

General | Display | Permissions | Restrictions | **Access Hours** | Authentication Methods

All	0	2	4	6	8	10	12	2	4	6	8	10
Sunday	*	*	*	*	*	*	*	*	*	*	*	*
Monday	*	*	*	*	*	*	*	*	*	*	*	*
Tuesday	*	*	*	*	*	*	*	*	*	*	*	*
Wednesday	*	*	*	*	*	*	*	*	*	*	*	*
Thursday	*	*	*	*	*	*	*	*	*	*	*	*
Friday	*	*	*	*	*	*	*	*	*	*	*	*
Saturday	*	*	*	*	*	*	*	*	*	*	*	*

☒ Access Allowed ☐ Access Denied

☐ Allow access only within this period:

8/ 8/2022 to 8/ 8/2022

Ok Cancel

On the VNC/RFB Profile Editor's '*Access Hours*' tab, you can define the day and time your application will be available to your users.

OPTION	DESCRIPTION
Access Permitted	Define which day and hour the application will be available.
Access Denied	Define which day and hour the application will be disabled.



Authentication Methods

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Authentication Methods' tab is selected. The 'Name' field is 'Sales Screensharing', 'Virtual Path' is 'Sales_Screensharing', and 'Access Key' is 'tia9PR\$GVI7N7Vq39apacm\$znuBbz\$X'. The 'Label(s)' field is empty. The 'Visible' checkbox is checked, and the 'Default profile' checkbox is unchecked. The 'Authentication Methods' section has two radio buttons: 'No restrictions' (unchecked) and 'Only users authenticated with these methods:' (checked). Below this is a list of authentication methods with checkboxes and their types:

Name	Type
<input checked="" type="checkbox"/> Windows Logon	Built-in
<input checked="" type="checkbox"/> API Access	{16D8D9B1-991A-477D-BEAC-5BAF1.
<input checked="" type="checkbox"/> Radius	Built-in
<input checked="" type="checkbox"/> SAML	SAML
<input checked="" type="checkbox"/> Google	OAuth
<input checked="" type="checkbox"/> Facebook	OAuth
<input checked="" type="checkbox"/> LinkedIn	OAuth
<input checked="" type="checkbox"/> Dropbox	OAuth
<input checked="" type="checkbox"/> Azure	OAuth
<input checked="" type="checkbox"/> ForgeRock	OAuth

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

On the VNC/RFB Profile Editor's '*Authentication Methods*' tab, you can define which application will be available after authenticating to Thinfinity® Remote Workspace.

The Authentication Methods available in the list are those configured in the '*Authentication*' tab of the Thinfinity® Configuration Manager.

OPTION	DESCRIPTION
No restrictions	No restriction on the authentication method used.

Only users authenticated with these methods

Only the users authenticated with the selected methods will be able to see and connect to the configured application.

Telnet/SSH Profile Editor

The Profile Editor is the tool to create, configure and edit Thinfinity® Remote Workspace's Access Profiles.

This section details the Telnet/SSH Profile Editor:

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

None

New Key

Select Label

☒ Visible

☐ Default profile

General

Display

Options

Permissions

Restrictions

Access Hours

Authentication Methods

Address:

Port:

☐ Enable Keep Alive

☐ Disable Telnet Protocol Negotiation

☐ Disable Server Echo

☐ SSL

☐ SSH

Character Set:

Keyboard Name:

Broker Pool:

Session Limit: Minutes

Ok

Cancel

These are the profile properties you can edit:

OPTION	DESCRIPTION
Name	Use this field to change the profile name. The profile name is shown to users to

Virtual Path	<p>identify the connection.</p> <p>The Virtual Path will create a unique URL address for this connection. The complete path will consist of:</p> <p>http(s)://ThinfinityDomain:port/VirtualPath/.</p> <p>The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Workspace web interface.</p>
Access Key	Used in combination with Thinfinity® Remote Workspace 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.
Select Label	Prompts you to select an existing Label for this specific profile.
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.
Visible	If checked, the Access Profile will be visible on the Thinfinity® Remote Workspace landing page.
Default profile	If checked, the Thinfinity® Remote Workspace landing page will be skipped and connect directly to this profile.

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

General

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'General' tab is selected. The form contains the following fields and options:

- Name:** Management Mainframe
- Virtual Path:** Management_Mainframe
- Access Key:** foa24WkiGpIENDV1xrKBadMh9-Td@p9W
- Label(s):** \
- Buttons:** None, New Key, Select Label
- Checkboxes:** ☒ Visible, ☐ Default profile
- Tabs:** General (selected), Display, Options, Permissions, Restrictions, Access Hours, Authentication Methods
- Address:** 192.168.0.2
- Port:** 23
- Enable Keep Alive:** ☐
- Disable Telnet Protocol Negotiation:** ☐
- Disable Server Echo:** ☐
- SSL:** ☐
- SSH:** ☐
- Character Set:** MsDos USA
- Keyboard Name:** [Standard]
- Broker Pool:**
- Session Limit:** 0 Minutes
- Buttons:** Ok, Cancel

You can find the following options on the Telnet/SSH Profile Editor's '*General*' tab:

OPTION	DESCRIPTION
Address	Specify the URL/resource you want to connect to.
Port	Specify the port for the connection.
Enable Keep Alive	Enables keep-alive mechanism, needed for some Telnet servers to prevent disconnections.

Disable Telnet Protocol Negotiation	Check this option if you want to omit the protocol negotiation when connecting.
Disable Server Echo	Check this option if you don't want the server to echo every character it receives.
SSL	Enables the SSL (Secure Sockets Layer) protocol for the host.
SSH	Enables the SSH protocol for the host.
Character Set	Select the character set that better suits your language needs.
Keyboard Name	Select a keyboard setup.
Broker Pool	Specify which broker pool this profile belongs to.
Session Limit	Set up a session time limit for this profile.

SSL

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'General' tab is selected, and the 'SSL' sub-tab is active. The configuration fields are as follows:

- Name:** Management Mainframe
- Virtual Path:** Management_Mainframe
- Access Key:** foa24WkiGpIENDV1xrKBadMh9-Td@p9W
- Label(s):** \
- Visible:** ☒ Visible
- Default profile:** ☐ Default profile

Below these fields are buttons for 'New Key' and 'Select Label'. The 'SSL' sub-tab is selected, showing the following options:

- SSL Method:**
 - ☐ SSL 2/3
 - ☐ SSL 2.0
 - ☐ SSL 3.0
 - ☒ TLS 1.0
 - ☐ TLS 1.1
 - ☐ TLS 1.2
- Server Certificate:**
 - ☐ Accept expired certificates
 - ☐ Accept certificates not yet valid
 - ☐ Accept invalid CA certificates
 - ☐ Accept self signed certificates
 - ☐ Accept any invalid certificate

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

You can find the following options on the Telnet/SSH Profile Editor's 'SSL' tab:

OPTION	DESCRIPTION
SSL Method	Available methods: SSL 2/3, SSL 2.0, SSL 3.0, TLS 1.x.
Server Certificate	Specify what policy should the software adopt when dealing with certificates that do not meet certain security conditions.

SSH

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'SSH' tab is selected, displaying configuration options for the SSH protocol. The 'General' tab is also visible in the background.

General Tab Fields:

- Name: Management Mainframe
- Virtual Path: Management_Mainframe
- Access Key: foa24WkiGpIENDV1xrKBadMh9-Td@p9W
- Label(s): \
- ☒ Visible
- ☐ Default profile

SSH Tab Fields:

- Protocol Version:**
 - ☐ SSH 1 Only
 - ☒ SSH 2
- ☐ Enable Compression
- Authentication:**
 - ☐ Use Only Password Authentication
 - Username: [Text Field]
 - Password: [Text Field]
- Security:**
 - Key Exchange:** curve25519-sha256,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
 - Host Key:** ssh-rsa,ecdsa
 - Encryption:** aes256-ctr,aes192-ctr,aes128-ctr,blowfish-cbc,aes256-cbc,aes192-cbc,aes128-cbc,cast128-ctr,3des-ctr
 - Data Integrity:** hmac-sha2-256,hmac-sha2-512,hmac-sha1

Buttons: New Key, Select Label, Ok, Cancel.

You can find the following options on the Telnet/SSH Profile Editor's 'SSH' tab:

OPTION	DESCRIPTION
Protocol Version	Available versions: SSH 1 Only, SSH 2.
Enable Compression	Enables compression for the SSH protocol.
Use Only Password Authentication	Check this option set specific credentials.
Username	Username with access to the host via the SSH protocol.



Display

Thinfinity Configuration Manager - Profile Editor

Name: Management Mainframe

Virtual Path: Management_Mainframe

Access Key: foa24WkiGpIENDV1xrKBadMh9-Td@p9W

Label(s): \

☒ Visible ☐ Default profile

General | SSH | **Display** | Options | Permissions | Restrictions | Access Hours | Authentication Methods

Terminal

Type: ANSI

String: ANSI

☒ Automatic ☐ Use Computer Name

☒ Auto wrap

Screen Size

24 rows x 80 cols

☐ Custom

Rows: 24

Cols: 80

☐ Fixed Column Size

Scrollback lines: 1,000

Scrolling

☐ Smooth

☒ Jump

Jump speed: 2

Ok Cancel

You can find the following options on the Telnet/SSH Profile Editor's '*Display*' tab:

OPTION	DESCRIPTION
Type / String	Specify the type of terminal to emulate, which is not necessarily the same that is informed to the server. To inform the server a different type of terminal than the one emulated, use the 'String' field. To automatically detect the type of terminal, check the 'Automatic' option.

DEC Answerback	Here you can specify the DEC 'Transmit answerback message' control character.
Use Computer Name	Check this box to assign the computer's name to the DEC Answerback field.
Auto Wrap	Check this option if you want the text lines to be wrapped when the terminal is resized.
Screen Size	<p>Select any size from the options available in the drop-down list.</p> <p>Custom</p> <p>Check this option and type in specific numbers.</p>
Rows/Cols	Specify the number of rows and columns to be displayed. Choose from the options provided or check the 'Custom' option and type in the numbers.
Fixed Column Size	Check this option to display a horizontal scrollbar instead of resizing the font.
Scrollback Lines	Specify the number of rows to keep in the buffer so they can be scrolled with the vertical scrollbar.
Scrolling	<p>Smooth</p> <p>Sets a moderated jump speed.</p> <p>Jump</p> <p>Allows to specify the speed of the jumps</p>

Options

Thinfinity Configuration Manager - Profile Editor

Name: Management Mainframe

Virtual Path: Management_Mainframe

Access Key: foa24WkiGpIENDV1xrKBadMh9-Td@p9W

Label(s): \

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Display | **Options** | Permissions | Restrictions | Access Hours | Authentication Methods

Modes

☐ Local echo ☒ Auto repeat ☒ Break enabled

Receive Replacements

CR is: ☒ CR ☐ LF ☐ CR/LF

LF is: ☐ CR ☒ LF ☐ CR/LF

Send Replacements

Enter sends: ☐ CR ☒ CR/LF

Backspace sends: ☐ Delete ☒ Backspace

Cursor keys: ☒ Normal ☐ Application

Keypad: ☒ Numeric ☐ Application

LineMode

Mode: Never

Ok Cancel

You can find the following options on the Telnet/SSH Profile Editor's '*Options*' tab:

OPTION	DESCRIPTION
Local Echo	Allows local echoing of the characters when the server doesn't return echoes.
Auto Repeat	Enables the auto repeat feature for the keyboard.
Break Enabled	Enable to use the 'Break' command.

CR/LF is	Desired behaviour for the 'Carriage Return' (CR) and 'Line Feed' (LF) commands.
Enter/Backspace Sends	Desired behaviour for the 'Enter' and 'Backspace' keys.
Cursor/Keypad Keys	How the cursor and keypad keys are interpreted.
	Indicate when Line Mode will be activated

Permissions

The screenshot shows the 'Thinfinit Configuration Manager - Profile Editor' window. The 'Permissions' tab is selected. The form contains the following fields and options:

- Name:** Management Mainframe
- Virtual Path:** Management_Mainframe
- Access Key:** foa24WkiGpIENDV1xrKBadMh9-Td@p9W
- Label(s):** \
- ☒ Visible
- ☐ Default profile
- Buttons:** None, New Key, Select Label
- Tabs:** General, Display, Options, **Permissions**, Restrictions, Access Hours, Authentication Methods
- ☒ Inherit label access permissions
- ☐ Allow anonymous access
- Group or user names:** (Empty list box)
- Buttons:** Add, Remove
- Buttons:** Ok, Cancel

You can find the following options on the Telnet/SSH Profile Editor's '*Permissions*' tab:

Inherit label access permissions

Check this option if the Profile in question belongs to a Label with access permissions already configured on it. Inherit label access permissions

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 Workspace 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.

Restrictions

The screenshot shows the 'Thinfinitiy Configuration Manager - Profile Editor' window. The 'Restrictions' tab is selected. The form includes fields for Name, Virtual Path, Access Key, and Label(s). There are checkboxes for 'Visible' and 'Default profile'. Below the tabs, there are three radio button options: 'No restrictions' (selected), 'Allow only from these IPs', and 'Block connections from these IPs'. A large empty text area is provided for IP addresses. At the bottom of this area, it says 'If the list is empty, all IP addresses will be authorized'. There are 'Add' and 'Remove' buttons. At the very bottom of the window are 'Ok' and 'Cancel' buttons.

On the Telnet/SSH Profile Editor's '*Restrictions*' tab, you can white list or black list the IP addresses which are allowed to connect to the configured application.

OPTION	DESCRIPTION
No restrictions	No restriction over which IP Addresses will be able to connect to the application.
Allow only from these IPs	Allow connections from the listed IP Addresses.

Block connections from these IPs	Block connections from the listed IP Addresses.
Add	Add an IP Address to the list

Access Hours

Thinfinity Configuration Manager - Profile Editor

Name: Management Mainframe

Virtual Path: Management_Mainframe

Access Key: foa24W/kiGpIENDV1xrKBadMh9-Td@p9W

Label(s): \

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Display | Options | Permissions | Restrictions | Access Hours | Authentication Methods

All	0	2	4	6	8	10	12	2	4	6	8	10
Sunday	*	*	*	*	*	*	*	*	*	*	*	*
Monday	*	*	*	*	*	*	*	*	*	*	*	*
Tuesday	*	*	*	*	*	*	*	*	*	*	*	*
Wednesday	*	*	*	*	*	*	*	*	*	*	*	*
Thursday	*	*	*	*	*	*	*	*	*	*	*	*
Friday	*	*	*	*	*	*	*	*	*	*	*	*
Saturday	*	*	*	*	*	*	*	*	*	*	*	*

☒ Access Allowed ☐ Access Denied

☐ Allow access only within this period:

8/19/2022 to 8/19/2022

Ok Cancel

On the Telnet/SSH Profile Editor's 'Access Hours' tab, you can define the day and time your application will be available to your users.

OPTION	DESCRIPTION
Access Permitted	Define which day and hour the application will be available.
Access Denied	Define which day and hour the application will be disabled.



Authentication Methods

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Authentication Methods' tab is selected. The 'Name' field is 'Management Mainframe', 'Virtual Path' is 'Management_Mainframe', and 'Access Key' is 'foa24W/kiGpIENDV1xrKBadMh9-Td@p9W'. The 'Label(s)' field is empty. The 'Visible' checkbox is checked, and the 'Default profile' checkbox is unchecked. The 'Authentication Methods' section has two radio buttons: 'No restrictions' (selected) and 'Only users authenticated with these methods:'. Below this is a table with two columns: 'Name' and 'Type'.

Name	Type
<input type="checkbox"/> Windows Logon	Built-in
<input type="checkbox"/> API Access	{0FF2D795-FD58-4E4A-94CD-CA68B.
<input type="checkbox"/> Radius	Built-in
<input type="checkbox"/> SAML	SAML
<input type="checkbox"/> Google	OAuth
<input type="checkbox"/> Facebook	OAuth
<input type="checkbox"/> LinkedIn	OAuth
<input type="checkbox"/> Dropbox	OAuth
<input type="checkbox"/> Azure	OAuth
<input type="checkbox"/> ForgeRock	OAuth

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

On the Telnet/SSH Profile Editor's '*Authentication Methods*' tab, you can define which application will be available after authenticating to Thinfinity® Remote Workspace.

The Authentication Methods available in the list are those configured in the '*Authentication*' tab of the Thinfinity® Configuration Manager.

OPTION	DESCRIPTION
No restrictions	No restriction on the authentication method used.

Only users authenticated with these methods

Only the users authenticated with the selected methods will be able to see and connect to the configured application.

Web Link Profile Editor

The Profile Editor is the tool to create, configure and edit Thinfinity® Remote Workspace's Access Profiles.

This section details the Web Link Profile Editor:

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

☒ Visible

☐ Default profile

None

New Key

Select Label

GeneralPermissionsRestrictionsAccess HoursAuthentication Methods

Web URL

Get Icon

Ok

Cancel

These are the profile properties you can edit:

OPTION	DESCRIPTION
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 Workspace 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

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

General

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'General' tab is selected. The form contains the following fields and controls:

- Name:** Text field with value 'Thinfinity'.
- Virtual Path:** Empty text field.
- Access Key:** Text field with value 'cDbdGmaHYVmmNtGagHCQhFxKVA6SFp\$2'.
- Label(s):** Text field with value '\'. To the right are buttons for 'None', 'New Key', and 'Select Label'.
- Visible:** Checked checkbox.
- Default profile:** Unchecked checkbox.
- Web URL:** Text field with value 'https://www.thinfinity.com'. To the right is a 'Get Icon' button.

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

You can find the following options on the Web Link Profile Editor's '*General*' tab:

OPTION	DESCRIPTION
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 .

Permissions

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Permissions' tab is selected. The 'Name' field is 'Thinfinity', 'Virtual Path' is empty, 'Access Key' is 'cDbdGmaHYVmmNtGagHCQhFxKVA6SFp\$2', and 'Label(s)' is '\'. There are buttons for 'None', 'New Key', and 'Select Label'. The 'Visible' checkbox is checked, and 'Default profile' is unchecked. The 'Permissions' tab contains the following options:

- ☒ Inherit label access permissions
- ☐ Allow anonymous access
- Group or user names: (empty list box)
- Buttons: Add, Remove
- Buttons: Ok, Cancel

You can find the following options on the Web Link Profile Editor's '*Permissions*' tab:

Inherit label access permissions

Check this option if the Profile in question belongs to a Label with access permissions already configured on it.

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

	Workspace 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.

Restrictions

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Restrictions' tab is selected. The 'Name' field is 'Thinfinity', 'Virtual Path' is empty, 'Access Key' is 'cDbdGmaHYVmmNtGagHCQhFxKVA6SFp\$2', and 'Label(s)' is '\'. The 'Visible' checkbox is checked, and 'Default profile' is unchecked. The 'Restrictions' section has three radio buttons: 'No restrictions' (selected), 'Allow only from these IPs', and 'Block connections from these IPs'. Below these is a large empty text area for IP addresses. At the bottom of this section are 'Add' and 'Remove' buttons. The main window has 'Ok' and 'Cancel' buttons at the bottom right.

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

General | Permissions | **Restrictions** | Access Hours | Authentication Methods

☒ No restrictions
☐ Allow only from these IPs
☐ Block connections from these IPs

If the list is empty, all IP addresses will be authorized

In the Thinfinity® Configuration Manager's Profile Editor on the 'Restrictions' tab, you can white list or black list the IP addresses which are allowed to connect to the configured application.

OPTION	DESCRIPTION
No restrictions	No restriction over which IP Addresses will be able to connect to the application.
Allow only from these IPs	Allow connections from the listed IP Addresses.

Block connections from these IPs	Block connections from the listed IP Addresses.
Add	Add an IP Address to the list

Access Hours

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Permissions | Restrictions | **Access Hours** | Authentication Methods

All	0	2	4	6	8	10	12	2	4	6	8	10
Sunday	*	*	*	*	*	*	*	*	*	*	*	*
Monday	*	*	*	*	*	*	*	*	*	*	*	*
Tuesday	*	*	*	*	*	*	*	*	*	*	*	*
Wednesday	*	*	*	*	*	*	*	*	*	*	*	*
Thursday	*	*	*	*	*	*	*	*	*	*	*	*
Friday	*	*	*	*	*	*	*	*	*	*	*	*
Saturday	*	*	*	*	*	*	*	*	*	*	*	*

☒ Access Allowed ☐ Access Denied

☐ Allow access only within this period:

8/19/2022 to 8/19/2022

Ok Cancel

On the Web Link Profile Editor's '*Access Hours*' tab, you can define the day and time your application will be available to your users.

OPTION	DESCRIPTION
Access Permitted	Define which day and hour the application will be available.
Access Denied	Define which day and hour the application will be disabled.



Authentication Methods

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

General | Permissions | Restrictions | Access Hours | **Authentication Methods**

☐ No restrictions

☒ Only users authenticated with these methods:

Name	Type
<input checked="" type="checkbox"/> Windows Logon	Built-in
<input checked="" type="checkbox"/> API Access	{0FF2D795-FD58-4E4A-94CD-CA68B.
<input checked="" type="checkbox"/> Radius	Built-in
<input checked="" type="checkbox"/> SAML	SAML
<input checked="" type="checkbox"/> Google	OAuth
<input checked="" type="checkbox"/> Facebook	OAuth
<input checked="" type="checkbox"/> LinkedIn	OAuth
<input checked="" type="checkbox"/> Dropbox	OAuth
<input checked="" type="checkbox"/> Azure	OAuth
<input checked="" type="checkbox"/> ForgeRock	OAuth

On the Web Link Profile Editor's '*Authentication Methods*' tab, you can define which application will be available after authenticating to Thinfinity® Remote Workspace.

The Authentication Methods available in the list are those configured in the '*Authentication*' tab of the Thinfinity® Configuration Manager.

OPTION	DESCRIPTION
No restrictions	No restriction on the authentication method used.

Only users authenticated with these

Only the users authenticated with the
selected methods will be able to see and

Web VPN Profile Editor

The Profile Editor is the tool to create, configure and edit Thinfinity® Remote Workspace's Access Profiles.

This section details the Web VPN Profile Editor:

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s): \

None

New Key

Select Label

☒ Visible

☐ Default profile

GeneralPermissionsRestrictionsAccess HoursAuthentication Methods

Main entry point:

☐ Rewrite urls to "/" (Optimize for SPA)

☒ Sanitize input (Prevent XSS)

Custom Headers

Valid domains:

Broker Pool:

Ok

Cancel

OPTION	DESCRIPTION
Name	Use this field to change the profile name. The profile name is shown to users to identify the connection.

Virtual Path	<p>The Virtual Path will create a unique URL address for this connection. The complete path will consist of: http(s)://ThinfinityDomain:port/VirtualPath/. The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Workspace web interface.</p>
Access Key	<p>Used in combination with Thinfinity® Remote Workspace SDK to access this profile.</p>
New Key	<p>Change the Access Key to disable access through the current key and provide access through a new one.</p>
Select Label	<p>Prompts you to select an existing Label for this specific profile.</p>
Icon	<p>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</p>

General

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'General' tab is selected. The form contains the following fields and options:

- Name:** Google
- Virtual Path:** Google
- Access Key:** fqsmBaW40f0vNff5gE2atbLQ4Nfd\$uU4
- Label(s):** \
- Buttons:** None, New Key, Select Label
- Checkboxes:** ☒ Visible, ☐ Default profile
- Tabs:** General (selected), Permissions, Restrictions, Access Hours, Authentication Methods
- Main entry point:** https://www.google.com
- Options:**
 - ☐ Rewrite urls to "/" (Optimize for SPA)
 - ☒ Sanitize input (Prevent XSS)
 - Custom Headers** (button)
- Valid domains:** (empty text area)
- Broker Pool:** (empty text field)
- Buttons:** Ok, Cancel

You can find the following options on the Web VPN Profile Editor's '*General*' tab:

OPTION	DESCRIPTION
Main Entry Point	Add the URL you wish to access via Web VPN from outside your network.
Optimize for SPA	Optimizes the connection to better work with Single Page Application, masking the Virtual Path to avoid routing incompatibilities on heavy dependent JavaScript web applications. E.g.: Web

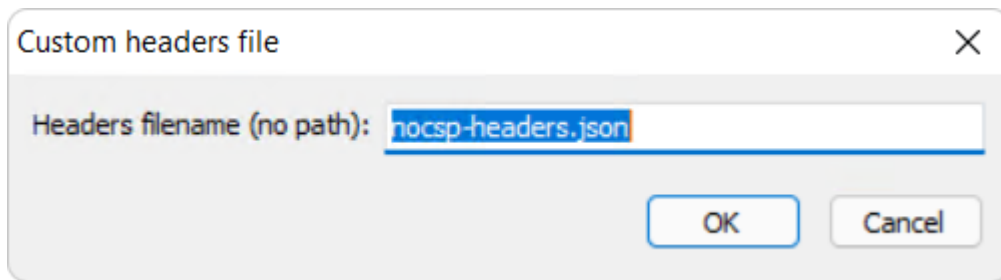
Sanitize Input (Prevent XSS)	Applications made with Angular, React and Vue which use routing plugins. Applies cross site scripting (XSS) sanitization to every request made to the server to avoid possible XSS issues or attacks. E.g.: This setting will help prevent malicious JavaScript injection in your web application.
Valid Domains	<p>Additional list of domains (Comma separated) that will go through the WebVPN if requested or utilized by the main entry point. By default, every subdomain of the main entry point is also a valid domain. These domains can also be specified as masks, E.g.:</p> <ol style="list-style-type: none"> 1) * 2) *.domain.com 3) fonts.domain.com 4) mydomain-*.com <ol style="list-style-type: none"> 1) Allow all domains 2) Allow every subdomain included under domain.com 3) Allow specifically fonts.domain.com 4) Allow every domain which starts with mydomain-

Custom Headers

Configure a json file that specifies how CSP (Content Security Policy) headers will be overridden for every request that goes through the WebVPN.

You can use this configuration to prevent unexpected CSP problems when using the WebVPN.

- Hit the Custom Headers button available on the General Tab.



- A pop-up window will be displayed with the default .json file. Assign the value or file you wish to use instead.

```
{
  "templates": {
    "nocsp": {
      "default": true,
      "headers": {
        "Content-Security-Policy": "",
        "cross-origin-opener-policy-report-only": "",
        "cross-origin-embedder-policy": "",
        "cross-origin-resource-policy": ""
      }
    }
  }
}
```

Permissions

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Name' field is 'Google', 'Virtual Path' is 'Google', and 'Access Key' is 'fqsmBaW40f0vNff5gE2atbLQ4Nfd\$uU4'. The 'Label(s)' field is empty. There are checkboxes for 'Visible' (checked) and 'Default profile' (unchecked). The 'Permissions' tab is selected, showing options to 'Inherit label access permissions' (checked) and 'Allow anonymous access' (unchecked). Below these is a list box for 'Group or user names' which is currently empty. At the bottom of the list box are 'Add' and 'Remove' buttons. At the bottom of the window are 'Ok' and 'Cancel' buttons.

You can find the following options on the Telnet/SSH Profile Editor's '*Permissions*' tab:

Inherit label access permissions

Check this option if the Profile in question belongs to a Label with access permissions already configured on it.

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

	Workspace 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.

Restrictions

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Restrictions' tab is selected, showing three radio button options: 'No restrictions' (selected), 'Allow only from these IPs', and 'Block connections from these IPs'. Below these options is a large empty text area for listing IP addresses. At the bottom of this area, it says 'If the list is empty, all IP addresses will be authorized'. There are 'Add' and 'Remove' buttons to the right of the text area. The top of the window has fields for 'Name' (Google), 'Virtual Path' (Google), 'Access Key' (fqsmBaW40f0vNff5gE2atbLQ4Nfd\$uU4), and 'Label(s)' (\). There are also checkboxes for 'Visible' (checked) and 'Default profile' (unchecked). Buttons for 'New Key' and 'Select Label' are on the right. The bottom of the window has 'Ok' and 'Cancel' buttons.

Thinfinity Configuration Manager - Profile Editor

Name: Google

Virtual Path: Google

Access Key: fqsmBaW40f0vNff5gE2atbLQ4Nfd\$uU4

Label(s): \

☒ Visible ☐ Default profile

General | Permissions | **Restrictions** | Access Hours | Authentication Methods

☒ No restrictions
☐ Allow only from these IPs
☐ Block connections from these IPs

If the list is empty, all IP addresses will be authorized

Add Remove

Ok Cancel

On the Web VPN Profile Editor's '*Restrictions*' tab, you can white list or black list the IP addresses which are allowed to connect to the configured application.

OPTION	DESCRIPTION
No restrictions	No restriction over which IP Addresses will be able to connect to the application.
Allow only from these IPs	Allow connections from the listed IP Addresses.

Add	Add an IP Address to the list
Remove	Remove an IP Address from the list

Access Hours

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Permissions | Restrictions | **Access Hours** | Authentication Methods

All	0	2	4	6	8	10	12	2	4	6	8	10
Sunday	*	*	*	*	*	*	*	*	*	*	*	*
Monday	*	*	*	*	*	*	*	*	*	*	*	*
Tuesday	*	*	*	*	*	*	*	*	*	*	*	*
Wednesday	*	*	*	*	*	*	*	*	*	*	*	*
Thursday	*	*	*	*	*	*	*	*	*	*	*	*
Friday	*	*	*	*	*	*	*	*	*	*	*	*
Saturday	*	*	*	*	*	*	*	*	*	*	*	*

☒ Access Allowed ☐ Access Denied

☐ Allow access only within this period:

8/19/2022 to 8/19/2022

Ok Cancel

On the Access Hours Profile Editor's '*Access Hours*' tab, you can define the day and time your application will be available to your users.

OPTION	DESCRIPTION
Access Permitted	Define which day and hour the application will be available.
Access Denied	Define which day and hour the application will be disabled.



Authentication Methods

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

General | Permissions | Restrictions | Access Hours | **Authentication Methods**

☐ No restrictions

☒ Only users authenticated with these methods:

Name	Type
<input checked="" type="checkbox"/> Windows Logon	Built-in
<input checked="" type="checkbox"/> API Access	{0FF2D795-FD58-4E4A-94CD-CA68B.
<input checked="" type="checkbox"/> Radius	Built-in
<input checked="" type="checkbox"/> SAML	SAML
<input checked="" type="checkbox"/> Google	OAuth
<input checked="" type="checkbox"/> Facebook	OAuth
<input checked="" type="checkbox"/> LinkedIn	OAuth
<input checked="" type="checkbox"/> Dropbox	OAuth
<input checked="" type="checkbox"/> Azure	OAuth
<input checked="" type="checkbox"/> ForgeRock	OAuth

On the Web VPN Profile Editor's '*Authentication Methods*' tab, you can define which application will be available after authenticating to Thinfinity® Remote Workspace.

The Authentication Methods available in the list are those configured in the '*Authentication*' tab of the Thinfinity® Configuration Manager.

OPTION	DESCRIPTION
No restrictions	No restriction on the authentication method used.

Only users authenticated with these methods

Only the users authenticated with the selected methods will be able to see and connect to the configured application.

Web Folder Profile Editor

The Profile Editor is the tool to create, configure and edit Thinfinity® Remote Workspace's Access Profiles.

This section details the Web Folder Editor:

These are the profile properties you can edit:

OPTION	DESCRIPTION
Name	Use this field to change the profile name. The profile name is shown to users to

Virtual Path	<p>identify the connection.</p> <p>The Virtual Path will create a unique URL address for this connection. The complete path will consist of:</p> <p>http(s)://ThinfinityDomain:port/VirtualPath/.</p> <p>The users can then create a web shortcut to this connection in particular and bypass the Thinfinity® Remote Workspace web interface.</p>
Access Key	<p>Used in combination with Thinfinity® Remote Workspace SDK to access this profile.</p>
New Key	<p>Change the Access Key to disable access through the current key and provide access through a new one.</p>
Select Label	<p>Prompts you to select an existing Label for this specific profile.</p>
Icon	<p>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.</p>
Visible	<p>If checked, the Access Profile will be visible on the Thinfinity® Remote Workspace landing page.</p>
Default profile	<p>If checked, the Thinfinity® Remote Workspace landing page will be skipped and connect directly to this profile.</p>

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

General

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'General' tab is selected. The form contains the following fields and options:

- Name:** Web Folder
- Virtual Path:** Web_Folder
- Access Key:** cDd2BPoBGU8yNDQaHad44K1vkafS\$V5W
- Label(s):** \
- ☒ Visible
- ☐ Default profile
- Buttons:** None, New Key, Select Label
- Tabs:** General, Permissions, Restrictions, Access Hours, Authentication Methods
- ☒ Local server
- Server URL:** (empty field)
- Root Path:** C:\Users\Public\Downloads
- Authentication Options:**
 - ☒ Use the authenticated credentials
 - ☐ Ask for new credentials
 - ☐ Use these credentials:
 - User name:** (empty field)
 - Password:** (empty field)
- Buttons:** Ok, Cancel

You can find the following options on the Web Folder Profile Editor's '*General*' tab:

OPTION	DESCRIPTION
Local server	Check this option if you wish to share a folder from within the server where Thinfinity® Workspace is installed.
Server URL	Enter the URL of the server that has the folder you wish to share.

Permissions

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Permissions' tab is selected. The 'Name' field is 'Web Folder', 'Virtual Path' is 'Web_Folder', and 'Access Key' is 'cDd2BPoBGU8yNDQaHad44K1vkafS\$V5W'. The 'Label(s)' field is empty. There are checkboxes for 'Visible' (checked) and 'Default profile' (unchecked). Below the tabs, there are checkboxes for 'Inherit label access permissions' (checked) and 'Allow anonymous access' (unchecked). A text area for 'Group or user names' is empty. At the bottom right of the text area are 'Add' and 'Remove' buttons. At the bottom of the window are 'Ok' and 'Cancel' buttons.

You can find the following options on the Web Folder Profile Editor's '*Permissions*' tab:

Inherit label access permissions

Check this option if the Profile in question belongs to a Label with access permissions already configured on it.

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®

	Workspace 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.

Restrictions

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Restrictions' tab is selected. The 'Name' field is 'Web Folder', 'Virtual Path' is 'Web_Folder', and 'Access Key' is 'cDd2BPoBGU8yNDQaHad44K1vkafS\$V5W'. The 'Label(s)' field is empty. There are checkboxes for 'Visible' (checked) and 'Default profile' (unchecked). Below the tabs, there are three radio button options: 'No restrictions' (selected), 'Allow only from these IPs', and 'Block connections from these IPs'. A large empty text area is provided for IP addresses. At the bottom of this area, it says 'If the list is empty, all IP addresses will be authorized'. There are 'Add' and 'Remove' buttons. At the very bottom of the window are 'Ok' and 'Cancel' buttons.

On the Web Folder Profile Editor's '*Restrictions*' tab, you can white list or black list the IP addresses which are allowed to connect to the configured application.

OPTION	DESCRIPTION
No restrictions	No restriction over which IP Addresses will be able to connect to the application.
Allow only from these IPs	Allow connections from the listed IP Addresses.

Block connections from these IPs	Block connections from the listed IP Addresses.
Add	Add an IP Address to the list

Access Hours

Thinfinity Configuration Manager - Profile Editor

Name: Web Folder

Virtual Path: Web_Folder

Access Key: cDd2BPoBGU8yNDQaHad44K1vkafS\$V5W

Label(s): \

☒ Visible ☐ Default profile

None

New Key

Select Label

General | Permissions | Restrictions | **Access Hours** | Authentication Methods

All	0	2	4	6	8	10	12	2	4	6	8	10
Sunday	*	*	*	*	*	*	*	*	*	*	*	*
Monday	*	*	*	*	*	*	*	*	*	*	*	*
Tuesday	*	*	*	*	*	*	*	*	*	*	*	*
Wednesday	*	*	*	*	*	*	*	*	*	*	*	*
Thursday	*	*	*	*	*	*	*	*	*	*	*	*
Friday	*	*	*	*	*	*	*	*	*	*	*	*
Saturday	*	*	*	*	*	*	*	*	*	*	*	*

☒ Access Allowed ☐ Access Denied

☐ Allow access only within this period:

8/19/2022 to 8/19/2022

Ok Cancel

On the Web Folder Profile Editor's '*Access Hours*' tab, you can define the day and time your application will be available to your users.

OPTION	DESCRIPTION
Access Permitted	Define which day and hour the application will be available.
Access Denied	Define which day and hour the application will be disabled.



Authentication Methods

Thinfinity Configuration Manager - Profile Editor

Name:

Virtual Path:

Access Key:

Label(s):

☒ Visible ☐ Default profile

General | Permissions | Restrictions | Access Hours | **Authentication Methods**

☐ No restrictions

☒ Only users authenticated with these methods:

Name	Type
<input checked="" type="checkbox"/> Windows Logon	Built-in
<input checked="" type="checkbox"/> API Access	{0FF2D795-FD58-4E4A-94CD-CA68B.
<input checked="" type="checkbox"/> Radius	Built-in
<input checked="" type="checkbox"/> SAML	SAML
<input checked="" type="checkbox"/> Google	OAuth
<input checked="" type="checkbox"/> Facebook	OAuth
<input checked="" type="checkbox"/> LinkedIn	OAuth
<input checked="" type="checkbox"/> Dropbox	OAuth
<input checked="" type="checkbox"/> Azure	OAuth
<input checked="" type="checkbox"/> ForgeRock	OAuth

On the Web Folder Profile Editor's '*Authentication Methods*' tab, you can define which application will be available after authenticating to Thinfinity® Remote Workspace.

The Authentication Methods available in the list are those configured in the '*Authentication*' tab of the Thinfinity® Configuration Manager.

OPTION	DESCRIPTION
No restrictions	No restriction on the authentication method used.

Only users authenticated with these methods

Only the users authenticated with the selected methods will be able to see and connect to the configured application.

Multi Terminal

In the Thinfinity Workspace Manager, you can configure these parameters for Multiterminal:

Service:

Pool name:

VZSCOPE

Access code:

Zxq4cjauhk

Service mode:

Run under the interactive session

Run under the interactive session

Run under an independent Windows session

Show Log

Apply

Close

Pool Name [String]: This value identifies the name for the multiterminal access profile, this can be any alphanumeric string.**Access code** [String]: This is the service password for the multiterminal connection. This can be any alphanumeric string.**Service mode**: This changes how the session is created.Available Modes:

Option	Description
<i>Run under the interactive session</i>	Select this option to run the multiterminal connection in the same RDS Session as the interactive session.
<i>Run under an independent Windows Session</i>	Select this option to run the multiterminal connection on individual RDS Sessions. This improves performance but at a higher resource cost.

Folders

Thinfinity® Configuration Manager's '*Folders*' tab you will find the following options:

Thinfinity Configuration Manager

File Help

General Broker Authentication Access Profiles **Folders** Permissions Protection Services License

Temporary Folders

Root Path:
 ...

Credentials for network shares only:

User name:

Password:

Test

Shared Folders

Share Name	Network Path	User name
------------	--------------	-----------

Add Edit Remove

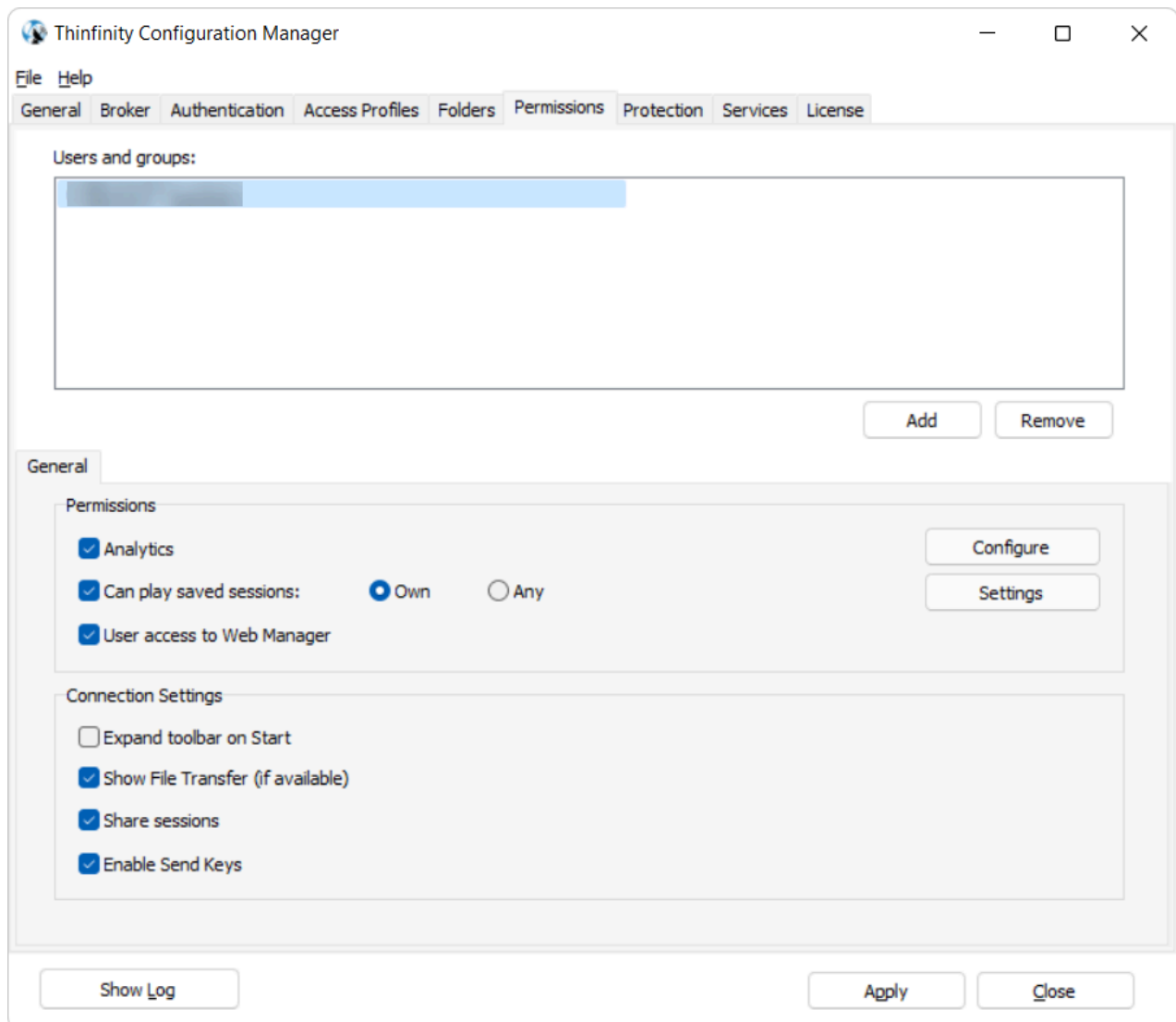
Show Log Apply Close

OPTION	DESCRIPTION
Temporary Folders (root path)	<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</p>

	<p>location in case you have intensive files exchange or also, if users start using the intermediate disks as their personal storage folder.</p>
Credentials for network shares only	<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>
Shared Folders	<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 Workspace 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>
Network User	<p>Sets a valid Windows Active Directory user for accessing the "Shared folders" being published.</p>

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

Permissions



In the Thinfinity® Configuration Manager's '*Permissions*' tab you will find the following options:

OPTION	DESCRIPTION
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 <u>connection toolbar</u> 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 Workspace toolbar.
Configure Analytics	Press this button to access the Analytics Database Options.
Saved session cleanup	Sets up a self-cleaning process for the stored Saved Sessions .

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

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

VirtualUI

- Click the "VirtualUI" tab to access the VirtualUI app session settings:

The screenshot shows the 'VirtualUI' configuration window in the Thinfinity Configuration Manager. The window has a title bar 'Thinfinity Configuration Manager' and standard window controls. Below the title bar is a menu bar with 'File' and 'Help'. A tabbed interface shows 'General', 'Broker', 'Authentication', 'Access Profiles', 'VirtualUI' (selected), 'Folders', 'Permissions', 'Protection', 'Services', and 'License'. The main content area contains the following text and controls:

VirtualUI requires at least one interactive Windows session. By default it uses the console session, sharing this session among all connected users.

You can configure VirtualUI to run under an alternate Windows session or, if you installed the Gateway, you can chose to balance memory usage/performance by configuring one session per user or distribute users evenly among a number of Windows sessions.

Mode: One Browser per Windows Session (dropdown menu)

☐ Allow running third-party applications

☒ Use these credentials:

Username:

Password: Test

☐ Create users on demand:

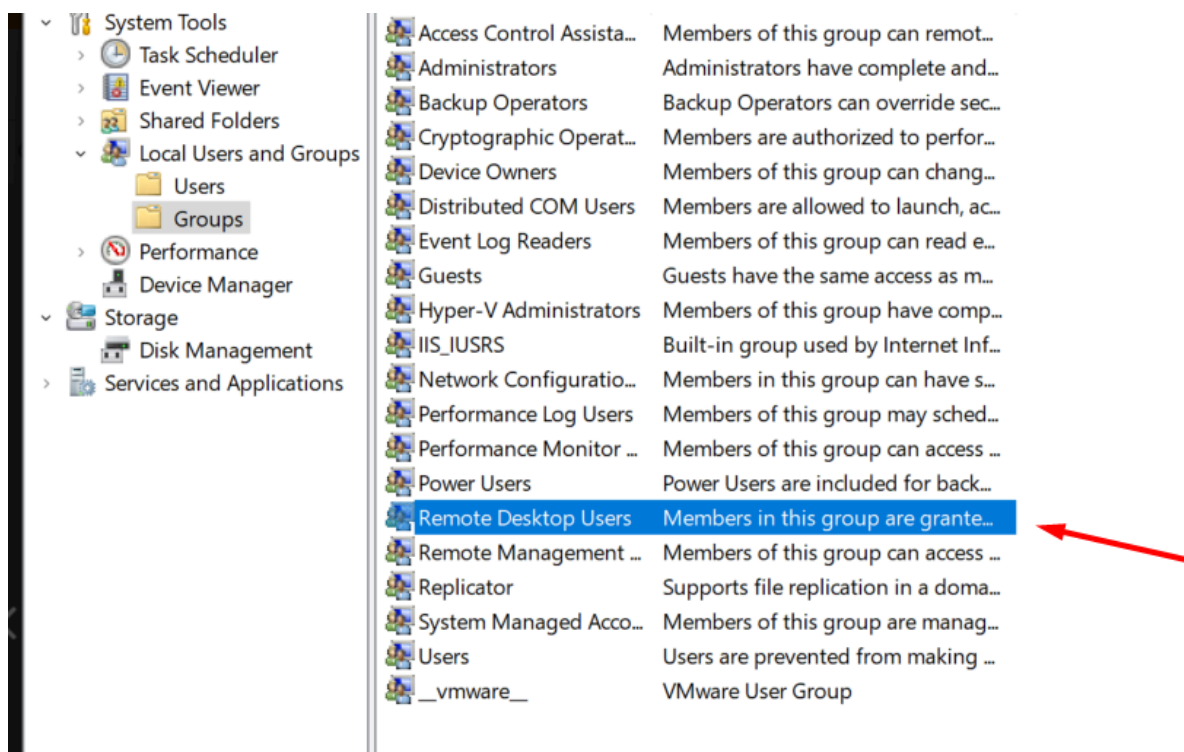
Username prefix: Add to group:

☐ Predefined users Configure

At the bottom of the window are three buttons: 'Show Log', 'Apply', and 'Close'.

In Desktop Manager we can only use the "One Browser per Windows Session" mode. We also need to declare credentials of a particular user for the app to be executed. Or have it create or predefine allowed users for it. Users need to be added to the "Remote Desktop Users" group in Computer Management:

One Browser per Session options



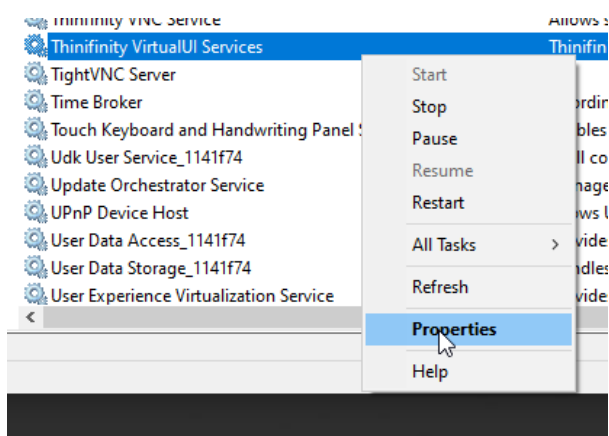
Options	Description
Allow running third-party applications	Check this option to enable Thinfinity VirtualUI to run directly under a Windows Interactive session.
Use these credentials	Check this option to enable Thinfinity VirtualUI to run under a specific Windows account.
User name	Enter the username for the Remote Desktop Services session you want Thinfinity VirtualUI to run applications under.
Password	Enter the password for the Remote Desktop Services session you want Thinfinity VirtualUI to run applications under.
Test	Test the credentials entered to verify that the username and password are correct and can access RDS.
Create Users on demand	This option lets VirtualUI create local users to run the applications, you can customize a prefix for these. IE: Prefix = Usertest , then VirtualUI creates Usertest1, Usertest2, etc.

Use predefined users

This option lets you define pre-created users instead (local or domain). Users need

Create users on-demand This option will let VirtualUI create the users. Each time VirtualUI requires to open a new session, it will create a user following the "Username prefix" you have established and it will make this user part of the group you specify in the box "Add to group":

If you set the prefix "TestUser". VirtualUI will create the user "TestUser", "TestUser2", "TestUser3, and so on. Bear in mind that if you need to use domain users along with this option, you will have to specify the domain in the prefix, for instance, "Domain\TestUser". You will also need to configure VirtualUI's service to logon as a domain user, this user must have permission to create domain users. To update the service's logon user, open the services panel (services.msc) and go to the properties of the Thinfinity VirtualUI's service:



☐ Use the current interactive session or console Autologon

☐ Use these credentials:

Username:

Password: Test

☒ Create users on-demand:

Username prefix: Add to group:

☐ Predefined users Configure

☐ Use VirtualUI's logged-in credentials

Once there, go to the tab 'Log on', and enter the information of the user:

Thinfinity VirtualUI Services Properties (Local Computer) ×

General Log On Recovery Dependencies

Log on as:

☐ Local System account
☐ Allow service to interact with desktop

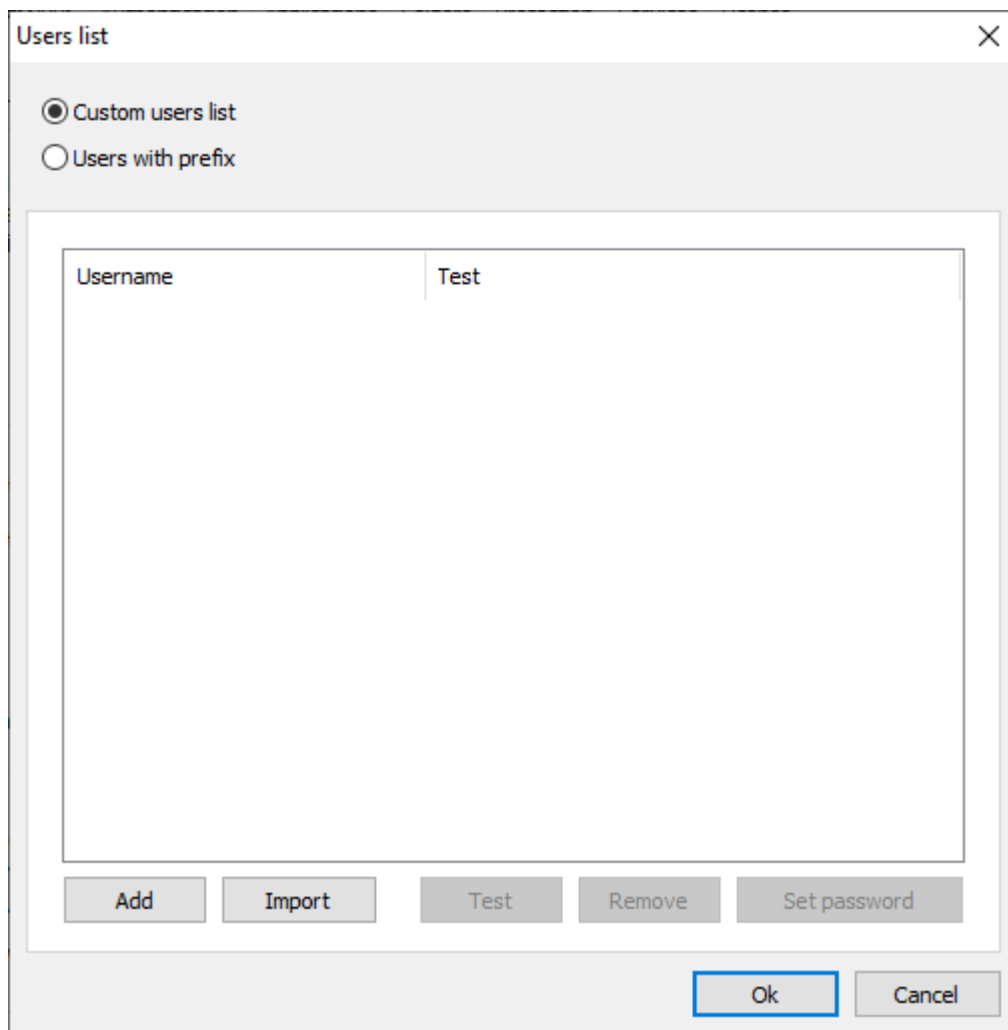
☒ This account: Browse...

Password:

Confirm password:

OK Cancel Apply

Predefined users The predefined user's option, will allow adding existing users of your domain or local server.



You can either add them from a ***custom list*** or ***users with a prefix***.

Custom List

In the custom list, you can add users individually by clicking on 'Add', or importing them from a list.

The list must be a txt file, following these formats:

For local users:

.\\user:password

Computer\\user:password

For domain users:

Domain\user:password

Users with prefix

This option is similar to "Create users on-demand" only that you must create the users upfront.

Bear in mind all the users must have the same password.

VirtualUI will start the first session using the number 1 and gradually increase based on the number of connections/users

For instance, if you configured the prefix "TestUser", the first session VirtualUI will attempt to start is "TestUser1".

Multi Terminal

In the Thinfinity Workspace Manager, you can configure these parameters for Multiterminal:

Service:

Pool name:

VZSCOPE

Access code:

Zxq4cjauhk

Service mode:

Run under the interactive session

Run under the interactive session

Run under an independent Windows session

Show Log

Apply

Close

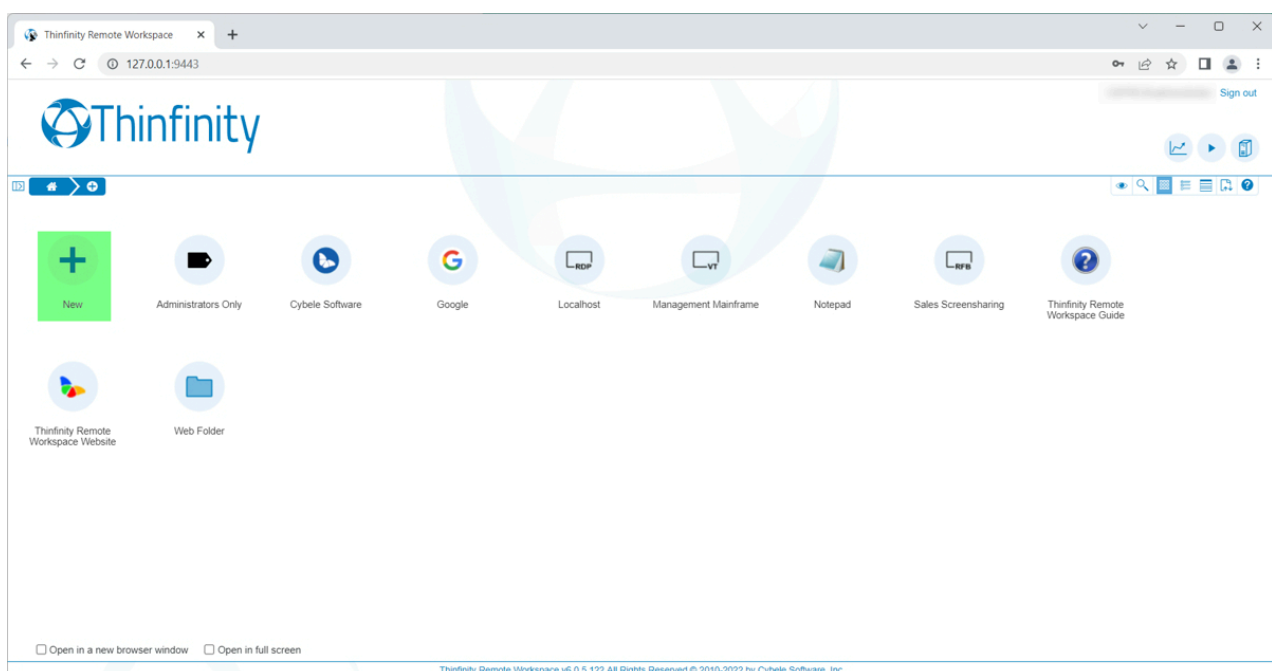
Pool Name [String]: This value identifies the name for the multiterminal access profile, this can be any alphanumeric string.**Access code** [String]: This is the service password for the multiterminal connection. This can be any alphanumeric string.**Service mode**: This changes how the session is created.Available Modes:

Option	Description
<i>Run under the interactive session</i>	Select this option to run the multiterminal connection in the same RDS Session as the interactive session.
<i>Run under an independent Windows Session</i>	Select this option to run the multiterminal connection on individual RDS Sessions. This improves performance but at a higher resource cost.

Thinfinity® Remote Workspace Admin User Interface

With Thinfinity® Remote Workspace, you are able to set up profiles to your desired connections entirely through the index page on the browser itself.

- To access the Thinfinity® Remote Workspace Wizard to be able to create this 'Web Profiles' you would need to click on the 'New' button with the '+' symbol as shown below:





- Afterwards, you'll find the Thinfinity® Remote Workspace Wizard where you'll find all types of connections available:


×


Welcome! Let's create a new connection.

This wizard will help you create a new access profile. Please choose the type of connection you want to create.


Desktop


Application


Web Folder


Terminal

Make this profile available to other users ☒

Next

You can find read our step-by-step guide to create Web Profiles with Thinfinity® Remote Workspace here:



How to create a Web Profile connection

Thinfinity® Remote Workspace



The Web Profiles available for Thinfinity® Remote Workspace are as follows:



Desktop

Thinfinity® Remote Workspace



Application

Thinfinity® Remote Workspace





Web Folder

Thinfinity® Remote Workspace



Terminal

Thinfinity® Remote Workspace



Additionally, you are able to create a '*Label*' that allows you to organize your Web Profiles of your Thinfinity® Remote Workspace landing page into subfolders for ease of access:



Label

Thinfinity® Remote Workspace

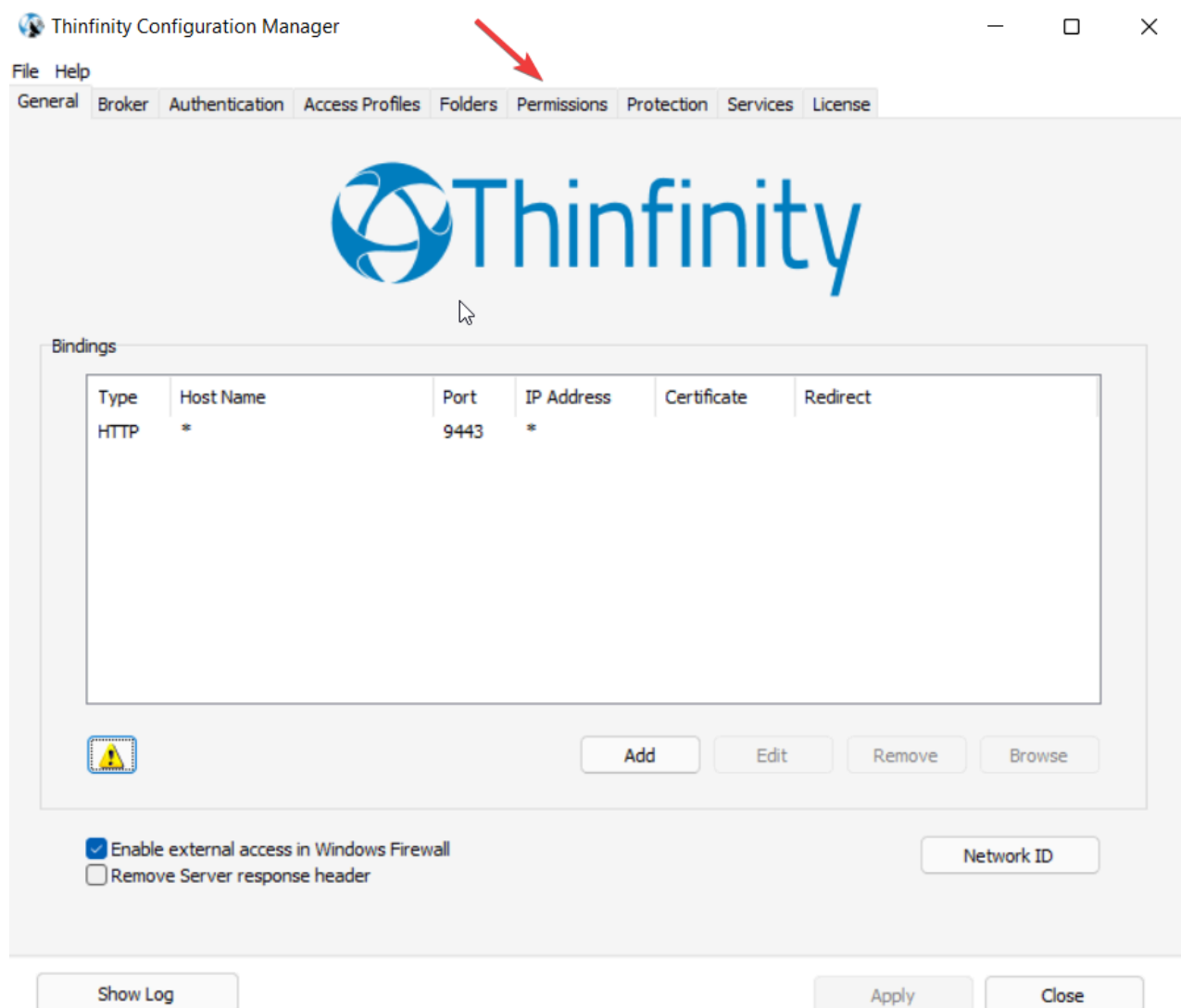


Web Manager

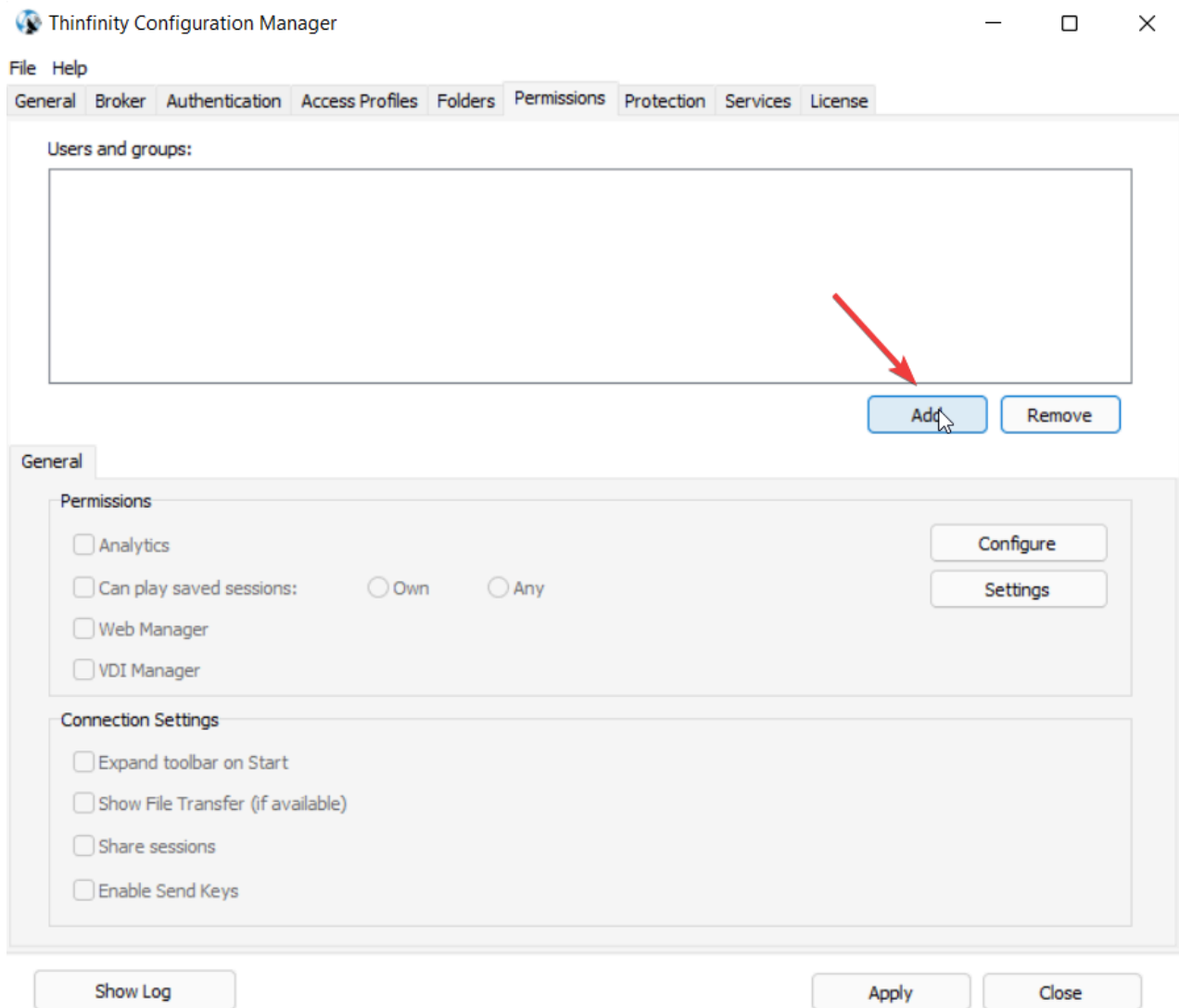
In order to edit public profiles in the Thinfinity Remote Workspace web interface, you will have to assign a Web Manager in Thinfinity Remote Workspace Configuration Manager.

Here is a "Step by step" on how to enable the Web Manager Permissions for a Domain or local user on Thinfinity Remote Workspace.

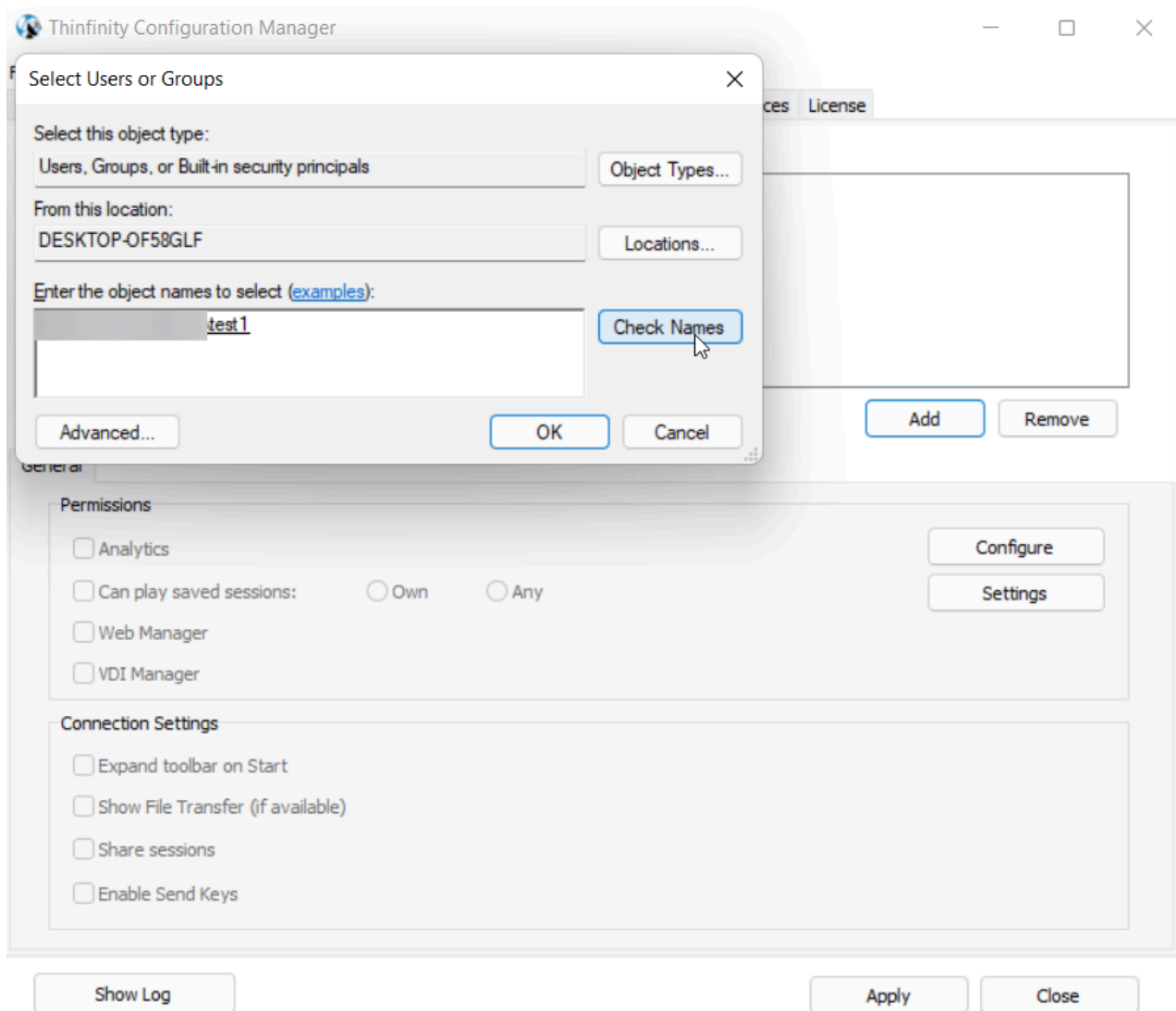
First, we need to open the Configuration Manager of Workspace and go to the tab Permissions



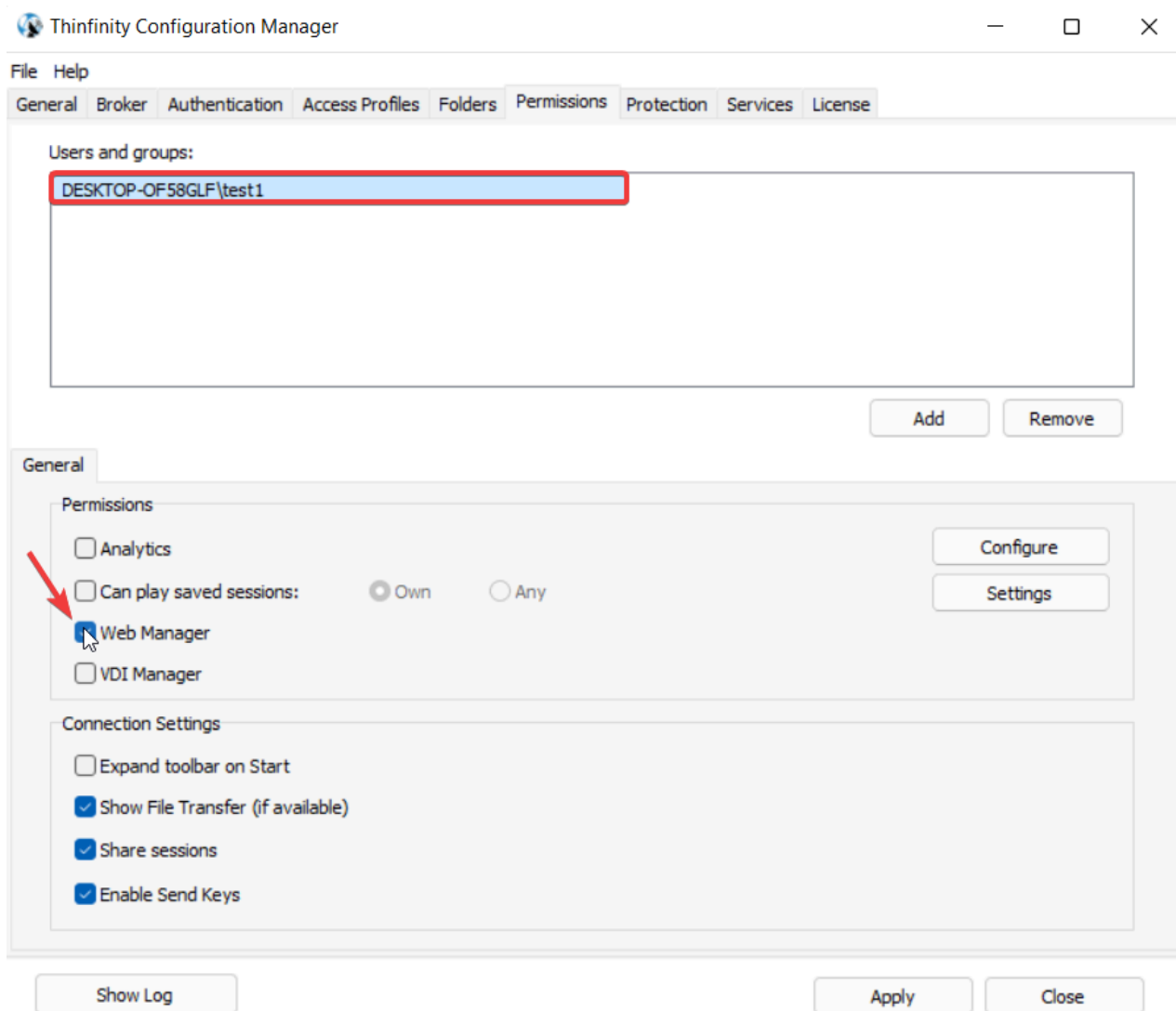
Once in the Permissions tab, we need to add a user to "Users and Groups" by Clicking "Add"



Then, type the name of the user you wish to add, click on check, and then on OK to confirm.

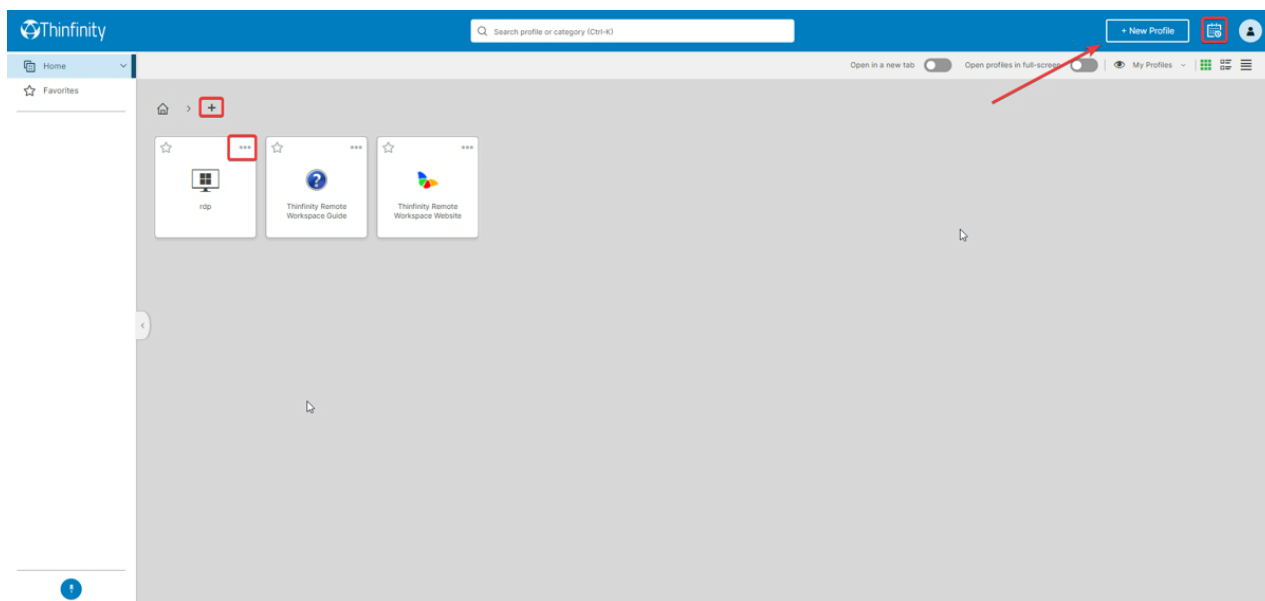


Once we've added the user to "Users and Groups", we need to grant them the "Web Manager" permissions by selecting the user (by clicking on it first), and then enabling the feature "Web Manager" option, as seen below



Once this is done, all that is left to do is click on "Apply", in the bottom right corner of the Configuration Manager to save the changes.

If we go now to the landing page of Thinfinity Remote Workspace, we will see, once we log on with this user, that we have access to new options.



These options will allow us to create new labels, and different types of connections for our users, as well as edit existing ones, without the necessity of accessing the Configuration Manager.

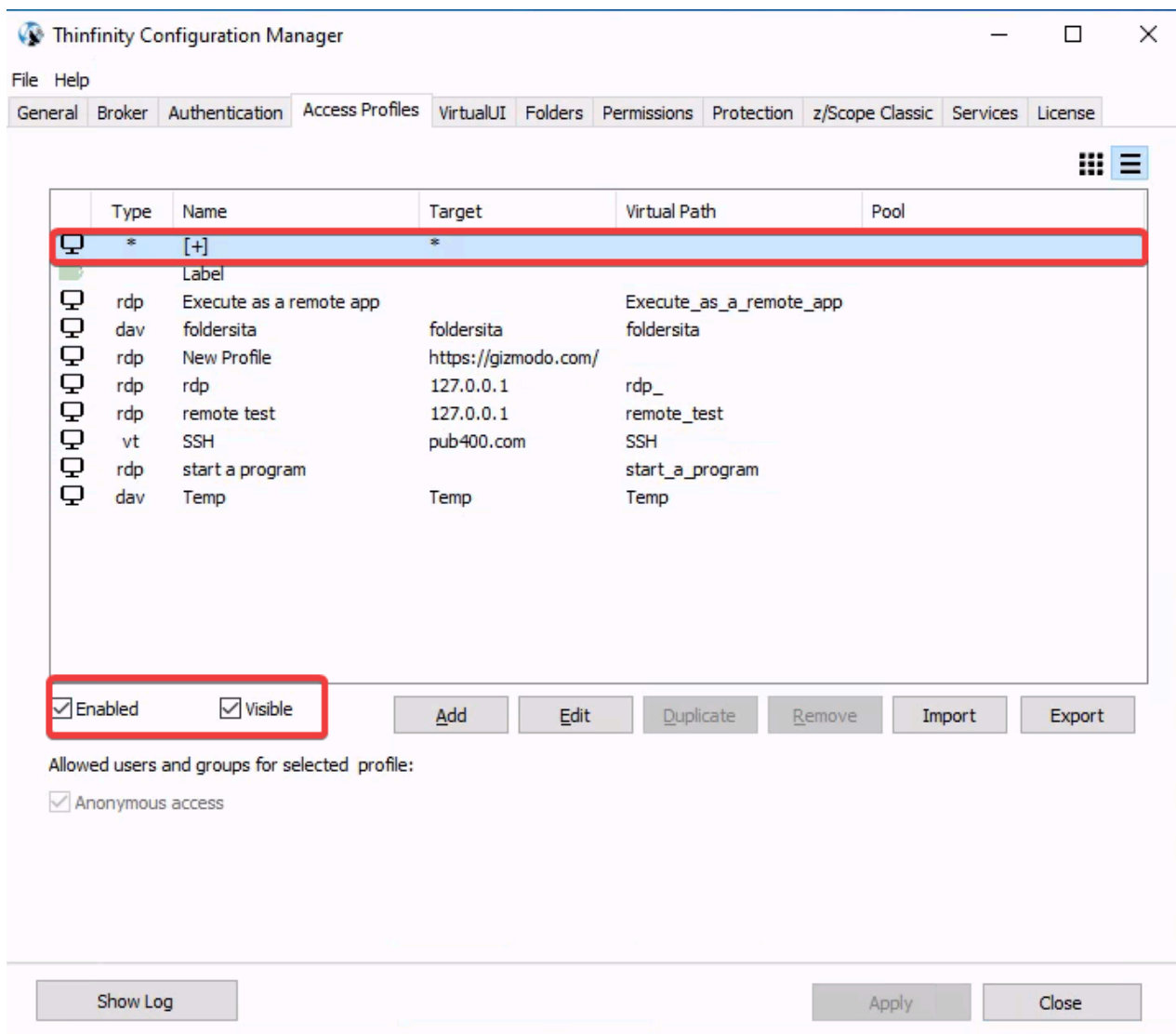
Web Interface

Web Profile Manager

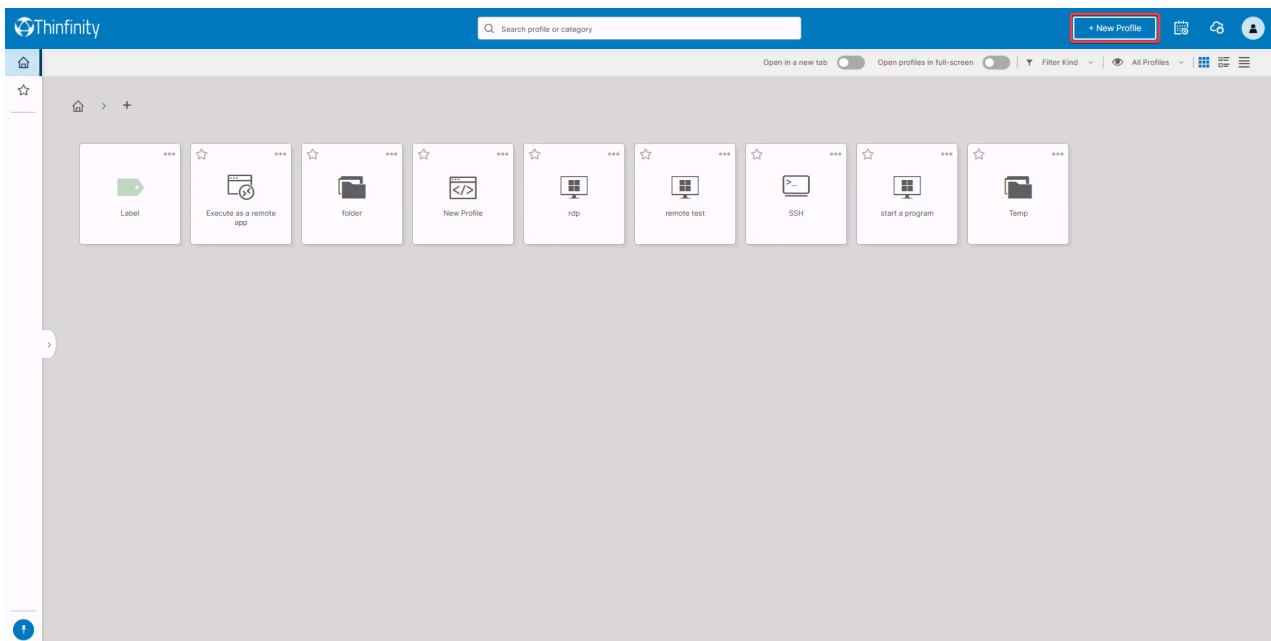
In here, you'll find the steps to create a new connection with Thinfinity® Workspace, via a completely revamped Web Profile Manager, in which you'll be able to configure all aspects of your Access Profiles from within the browser itself. Thinfinity® Workspace allows you to create connections such as the following:

- Remote Desktop
- VNC/RFB
- Terminal Connection
- Web Link
- Web VPN
- Labels
- Edit Web Profiles

By default, the option to create new connections on the Thinfinity® Workspace landing page is enabled and visible. This is seen as a "[+]" on the Thinfinity® Configuration Manager, on the Access Profiles tab, like so:



With the New button activated, you will be able to see if on the Thinfinity® Workspace landing page:





After clicking on the New button, you'll see the revamped New Access window that allows you to choose from all the Access types of profiles that Thinfinity® Workspace has to offer. Those being Remote Desktop, VNC/RFB, a Terminal connection, Web Link and Web VPN. You also have the Label feature that allows you to create subfolders to better organize your Thinfinity® Workspace landing page:


×


Welcome! Let's create a new connection.

This wizard will help you create a new access profile. Please choose the type of connection you want to create.


Desktop


Application


Web Folder

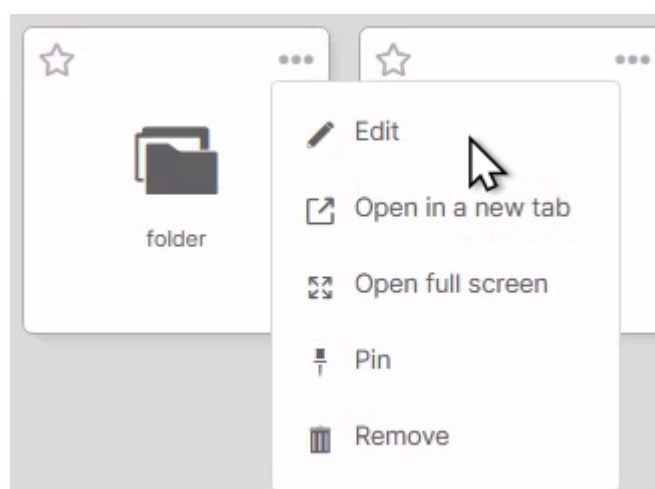

Terminal

Make this profile available to other users

☒

Next

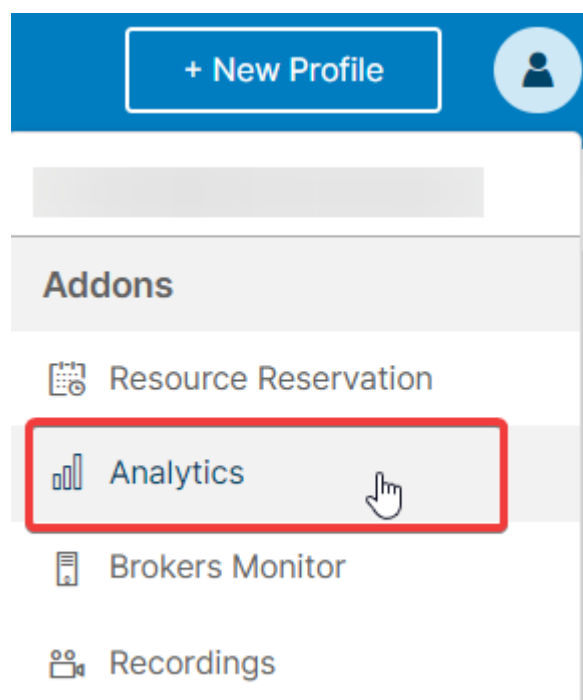
Another feature new to Thinfinity® Workspace is the ability to edit existing profiles in all aspects, same as on the client application. To be able to modify an existing connection, you would only need to click on the Edit button in the form of a pen, above the profile icon:



Analytics

The analytics feature allows assigned users to view historical data regarding Logins, Sessions and Connections established within Thinfinity® Remote Workspace 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® Configuration 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:

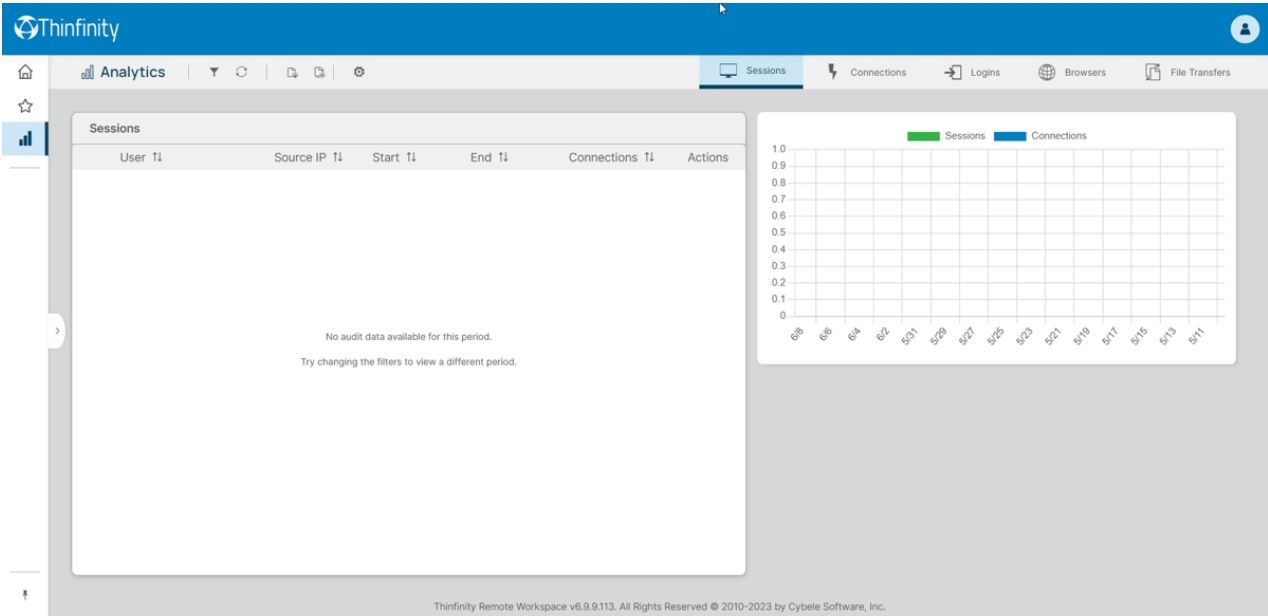


Click on the Analytics button to have the "Log & Statistics" window open on a new window and find inside the "Log & Statistics" window the available subsection tabs/options:

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](#).

Sessions

The Session View mode shows all the sessions created through the application within a determined period of time (default filter: Last hour).

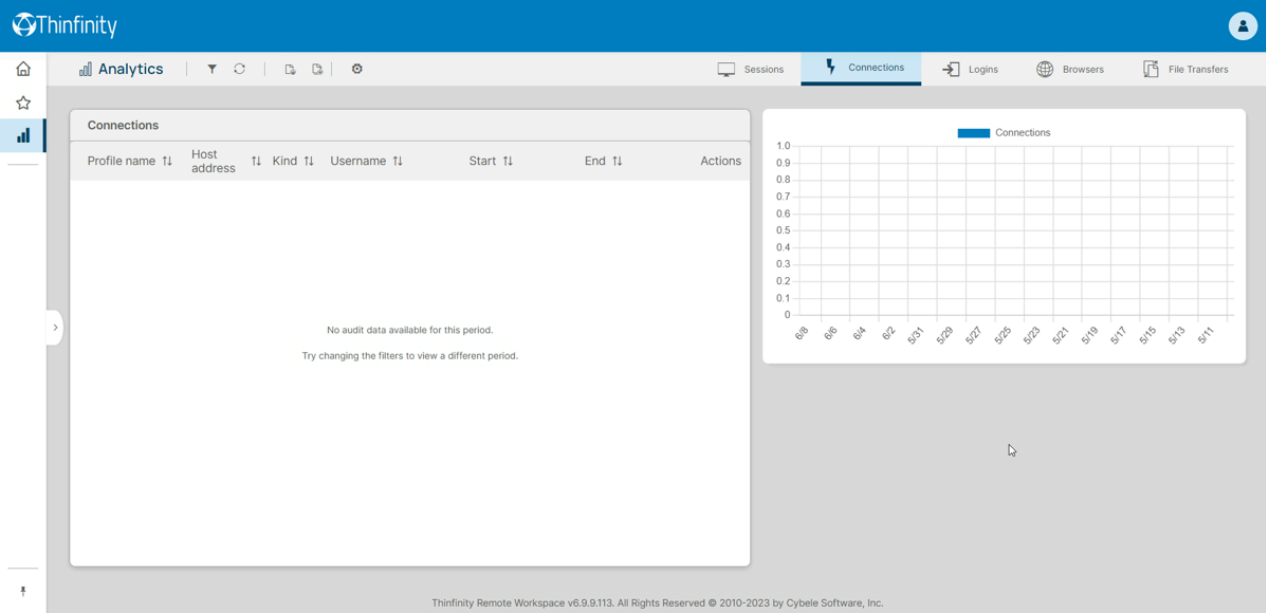


This is the information shown on the Sessions table:

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.

Connections

The Connection View mode shows all the connections established in a determined period of time (default filter: Last hour).

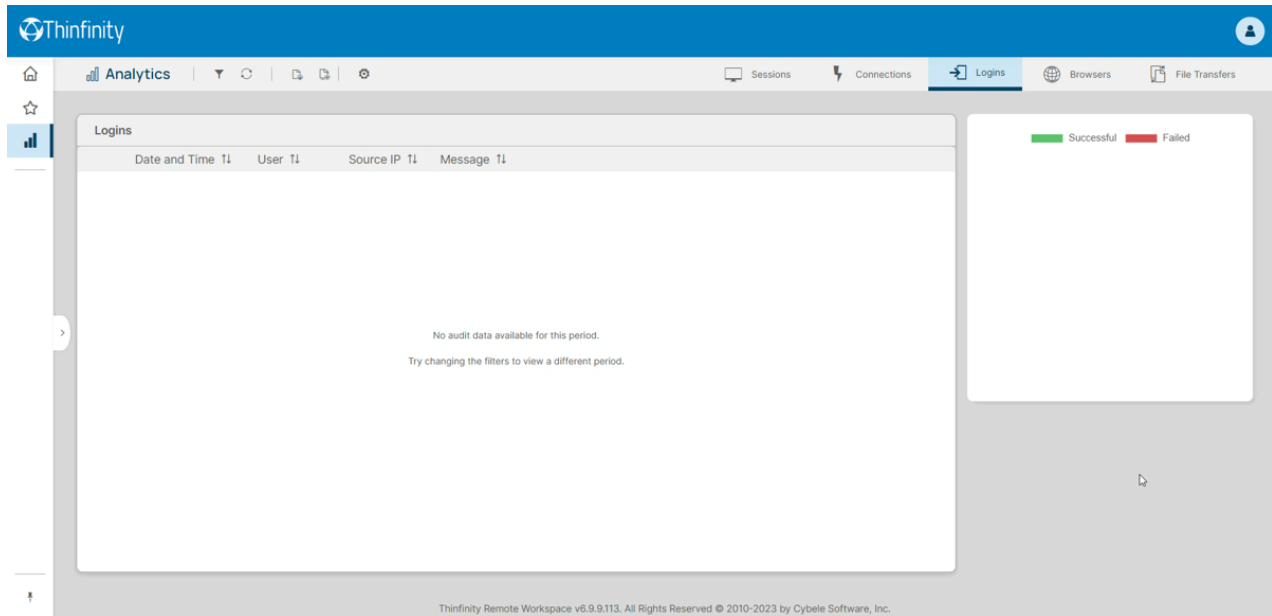


This is the information shown on the Connections table:

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

Logins

The Logins View mode shows all the logins performed through the application within a determined period of time (default filter: Last hour).

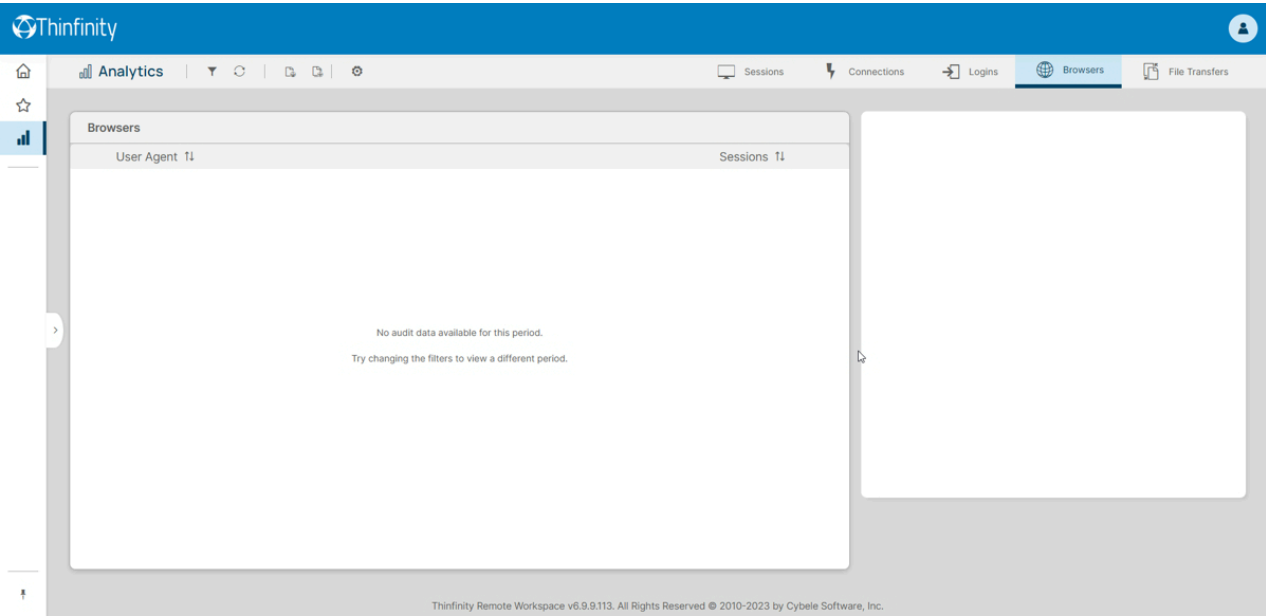


This is the information shown on the Logins table:

Start and End	Date and Time when the Login was performed.
User	User that logged in.
Source IP	IP Address from which the login was done.
Connections	Numbers of connections initiated by

Browsers

The Browsers View mode shows all the kinds of browsers used to access Thinfinity® Remote Workspace.



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.

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.

Host/IP

Users

Active Users Only

Range

Last 30 days

Apply

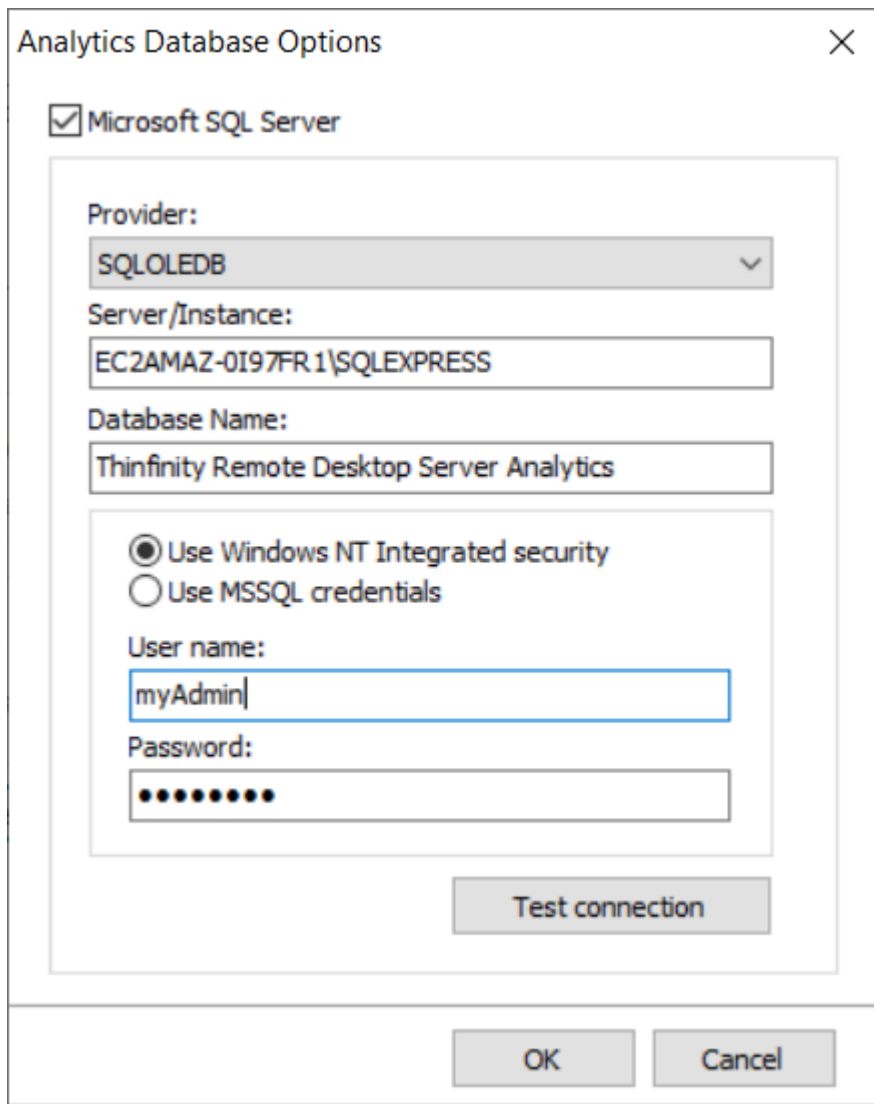
Users	Type in the usernames of the users you want filter, separated by commas.
Host	Type in a host name or IP Address.
Pick a date range from the list	Select one of the date range options, or select "Custom Range" to inform a custom period to filter the data.

Always remember to press "apply" in order to have the records filtered by the selected parameters.

Configuring MS SQL Server

These are the requisites for Thinfinity® Remote Workspace Analytics to use MS SQL Server:

1. An MS SQL Server 2005 (or higher) installation that is accessible from the machine running Thinfinity® Remote Workspace.
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® Configuration Manager, and press the 'Configure Analytics' button.
4. Access the Microsoft SQL Server Data Link Properties and configure the connection:



The image shows a dialog box titled "Analytics Database Options" with a close button (X) in the top right corner. Inside the dialog, there is a checked checkbox labeled "Microsoft SQL Server". Below this, there is a section for configuring the database connection. It includes a "Provider:" dropdown menu set to "SQLOLEDB". The "Server/Instance:" text box contains "EC2AMAZ-0I97FR1\SQLEXPRESS". The "Database Name:" text box contains "Thinfinity Remote Desktop Server Analytics". Below these, there are two radio buttons: "Use Windows NT Integrated security" (which is selected) and "Use MSSQL credentials". Under the selected radio button, there is a "User name:" text box containing "myAdmin" and a "Password:" text box filled with ten dots. A "Test connection" button is located below the password field. At the bottom of the dialog, there are "OK" and "Cancel" buttons.

Analytics Database Options

☒ Microsoft SQL Server

Provider:
SQLOLEDB

Server/Instance:
EC2AMAZ-0I97FR1\SQLEXPRESS

Database Name:
Thinfinity Remote Desktop Server Analytics

☒ Use Windows NT Integrated security
☐ Use MSSQL credentials

User name:
myAdmin

Password:
●●●●●●●●●●

Test connection

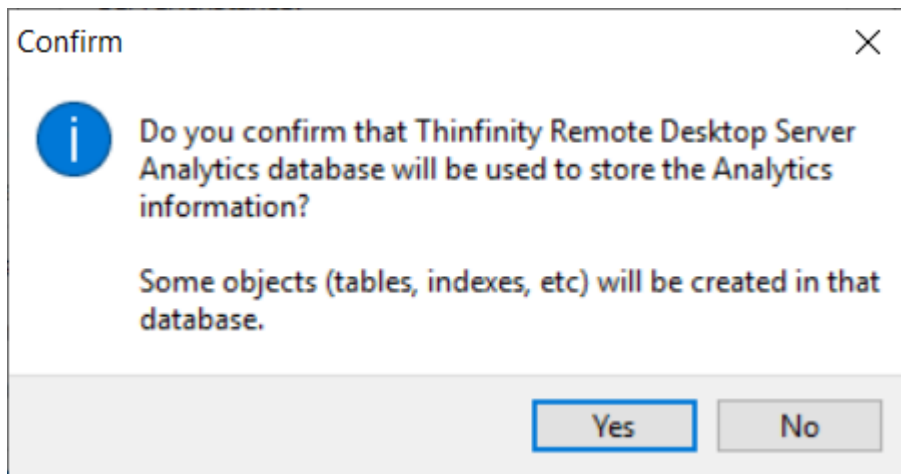
OK Cancel

4.1 Enter the server name and complete the information to log in to the server.

4.2 Select the database created in step 2.

4.3 Choose whether you want to use Windows NT credentials or MSSQL credentials.

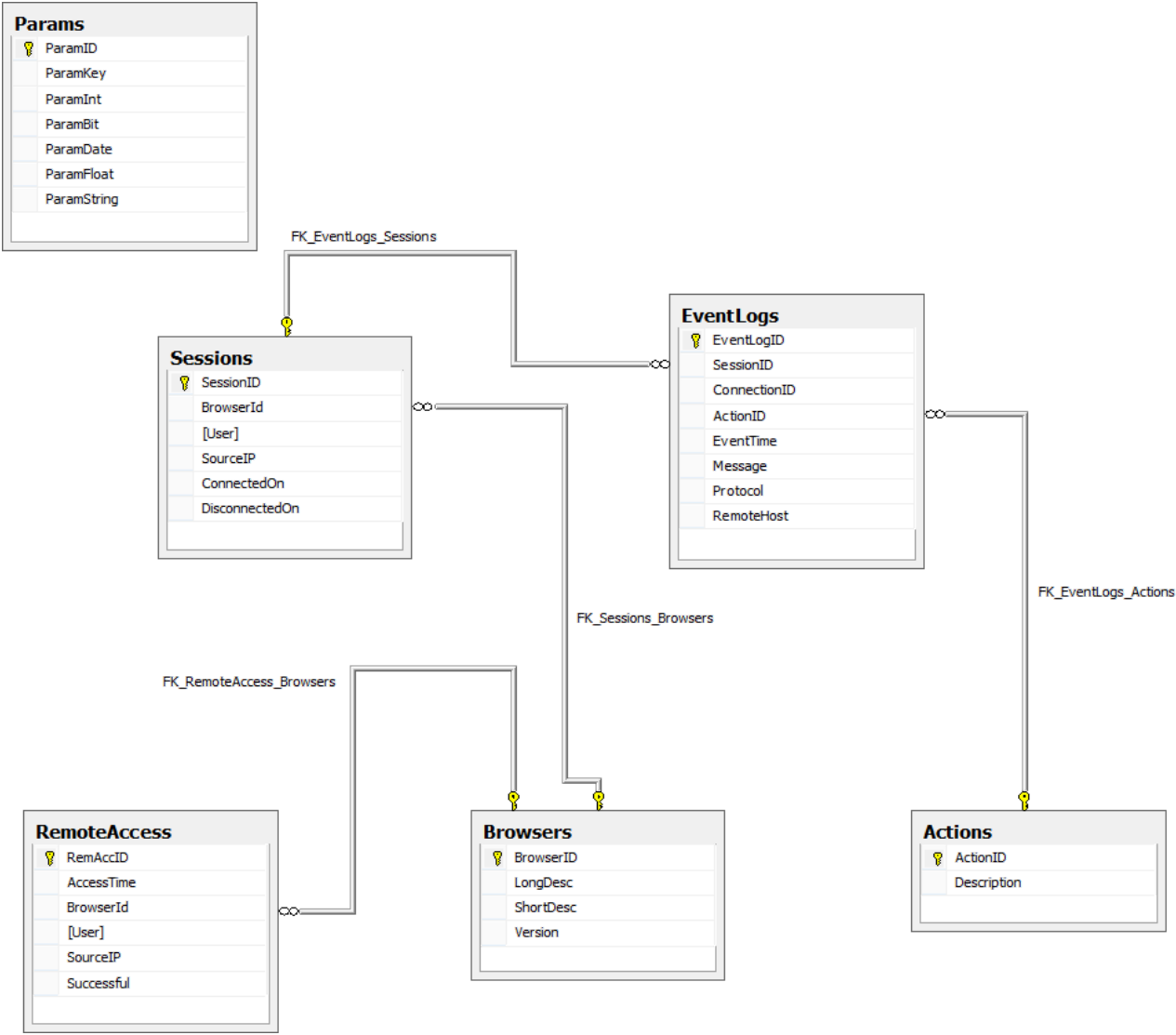
4.4 "Test connection" in order to verify the settings. You should see the following message :



4.5 Press "Yes"

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 Workspace user access.

Field	Description
-------	-------------

RemAccID	Auto increment field. Unique ID
AccessTime	The moment when the user accessed Thinfinity® Remote Workspace.
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.

Thinfinity® Remote Workspace session information

The Thinfinity® Remote Workspace 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 Workspace 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 Workspace 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 Workspace.
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 referenced 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.

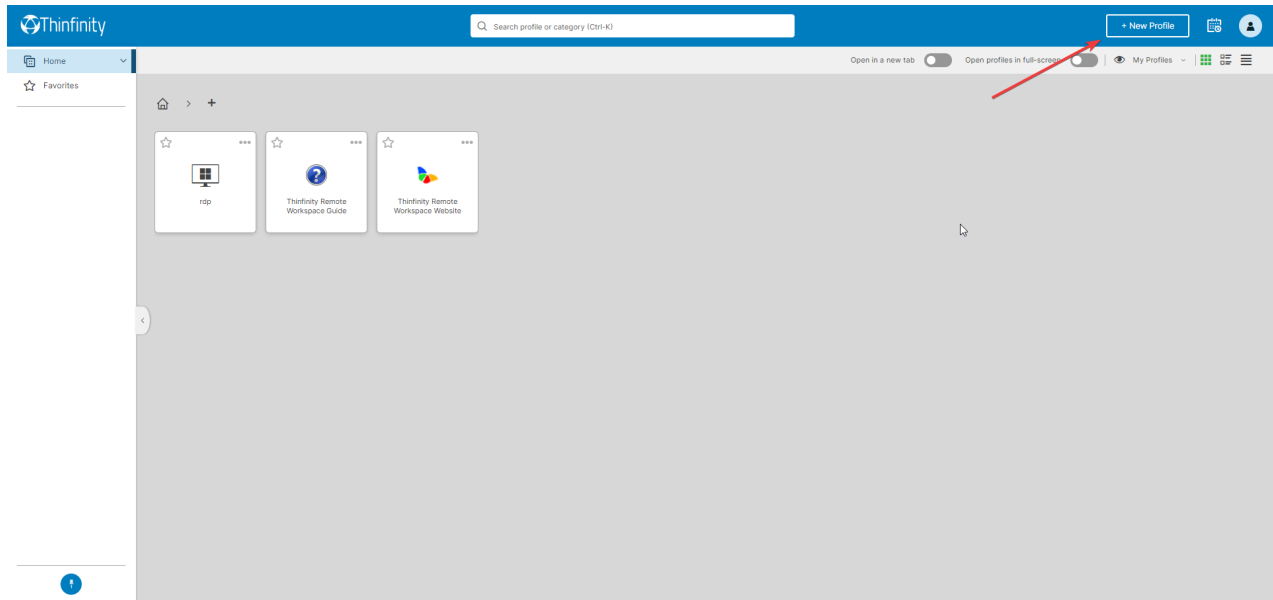
Version	Not used for the moment
---------	-------------------------

Connections

RDP

Connecting to an application

- First, you need to open the *landing page of Workspace* - *http(s)://ThinfinityURL:Port*
- Then click on the “New Profile” icon of the landing page

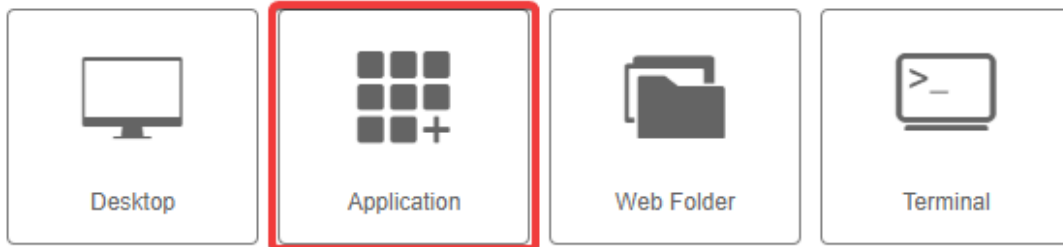


- Then select the “Application” type of connection, and click on next



Welcome! Let's create a new connection.

This wizard will help you create a new access profile. Please choose the type of connection you want to create.

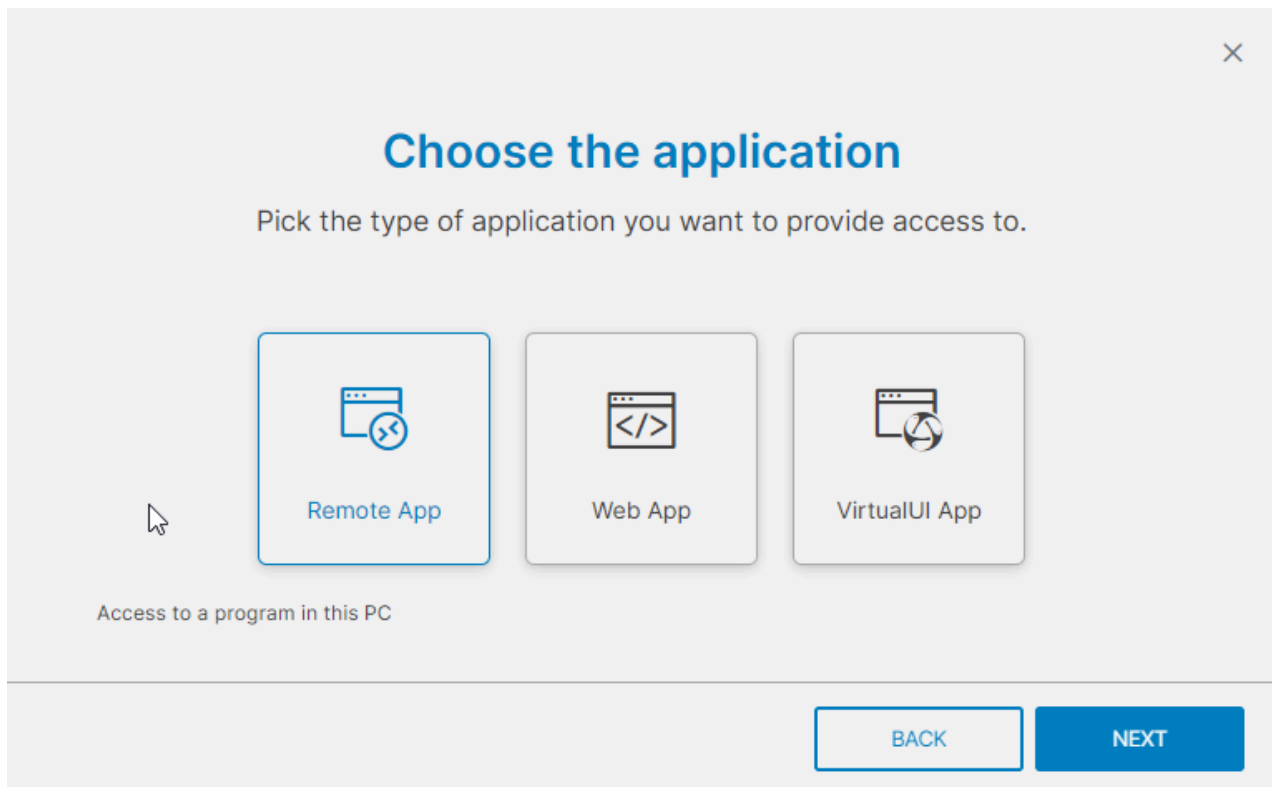


Make this profile available to other users

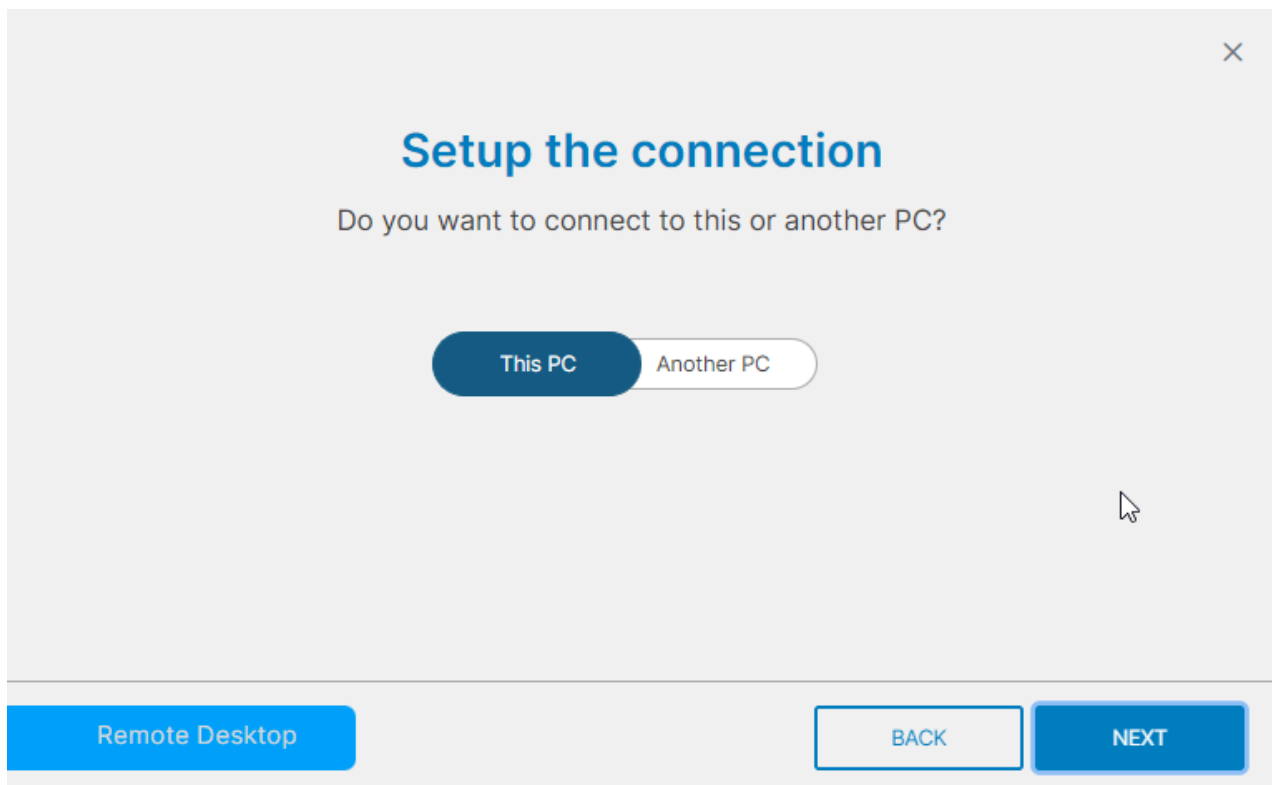


Next

- Select "RemoteApp"



- Now choose between making the connection to the current pc where you're working, or to another terminal



- After that we need to set the virtual path of the application you want to connect

×

Choose the application

Please specify the application parameters.

Program path and filename

notepad.exe

Remote Desktop

BACK

NEXT

- Now choose the authentication method

×

Authentication

Select how you want to handle the credentials to access this resource.

Credentials

Ask for new credentials ✓

Use the authenticated credentials

Ask for new credentials

Use these credentials

Remote Desktop

BACK

NEXT

- And at last, the name and the icon of the application you're going to use

×

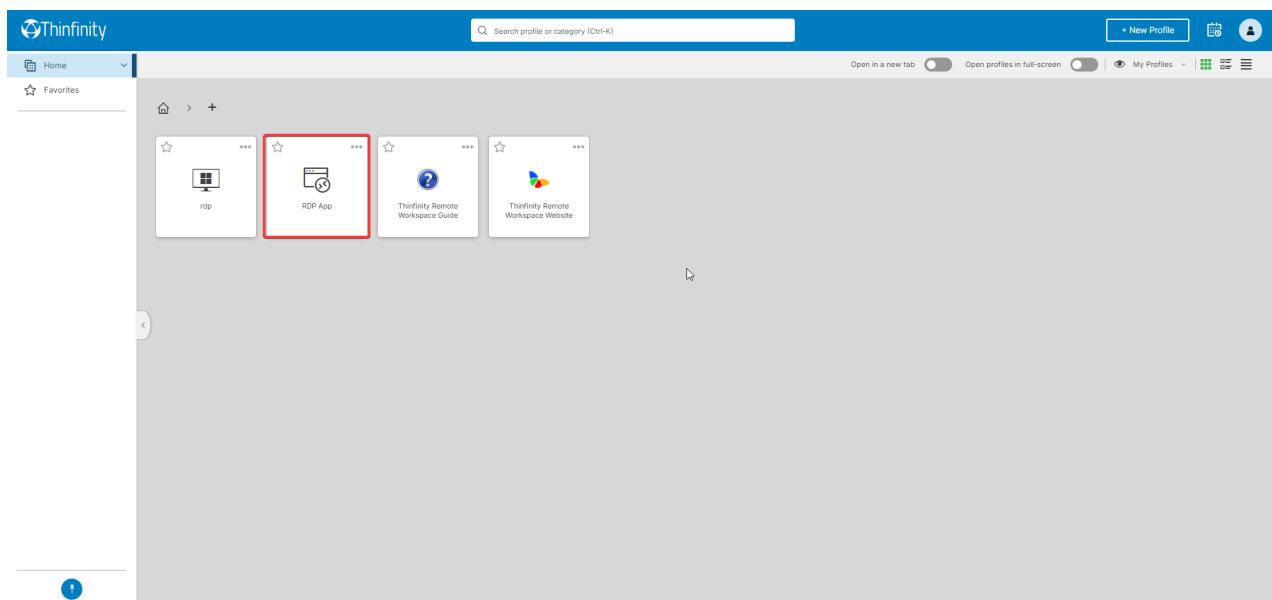
Profile Name

Enter a new name for this profile. This will be used as a friendly name for this connection.

Name

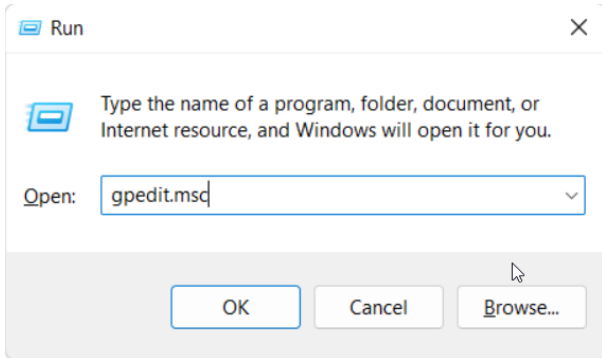
Remote DesktopBACKDONE

- You can now run the application by starting the newly created connection

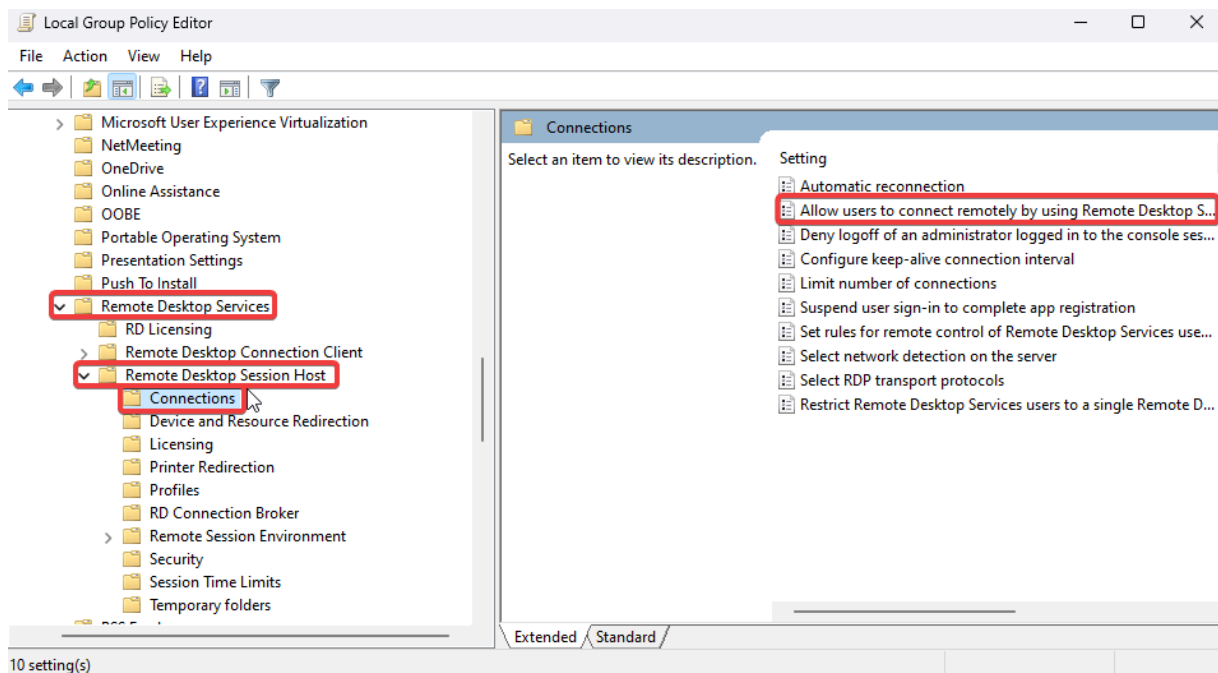


- If you start multiple RemoteApps, you'll find a dock menu at the bottom of the browser screen, this allows you to toggle between different applications of the same connection.
- You can also resize the App's windows and be able to see more than one at the same time.

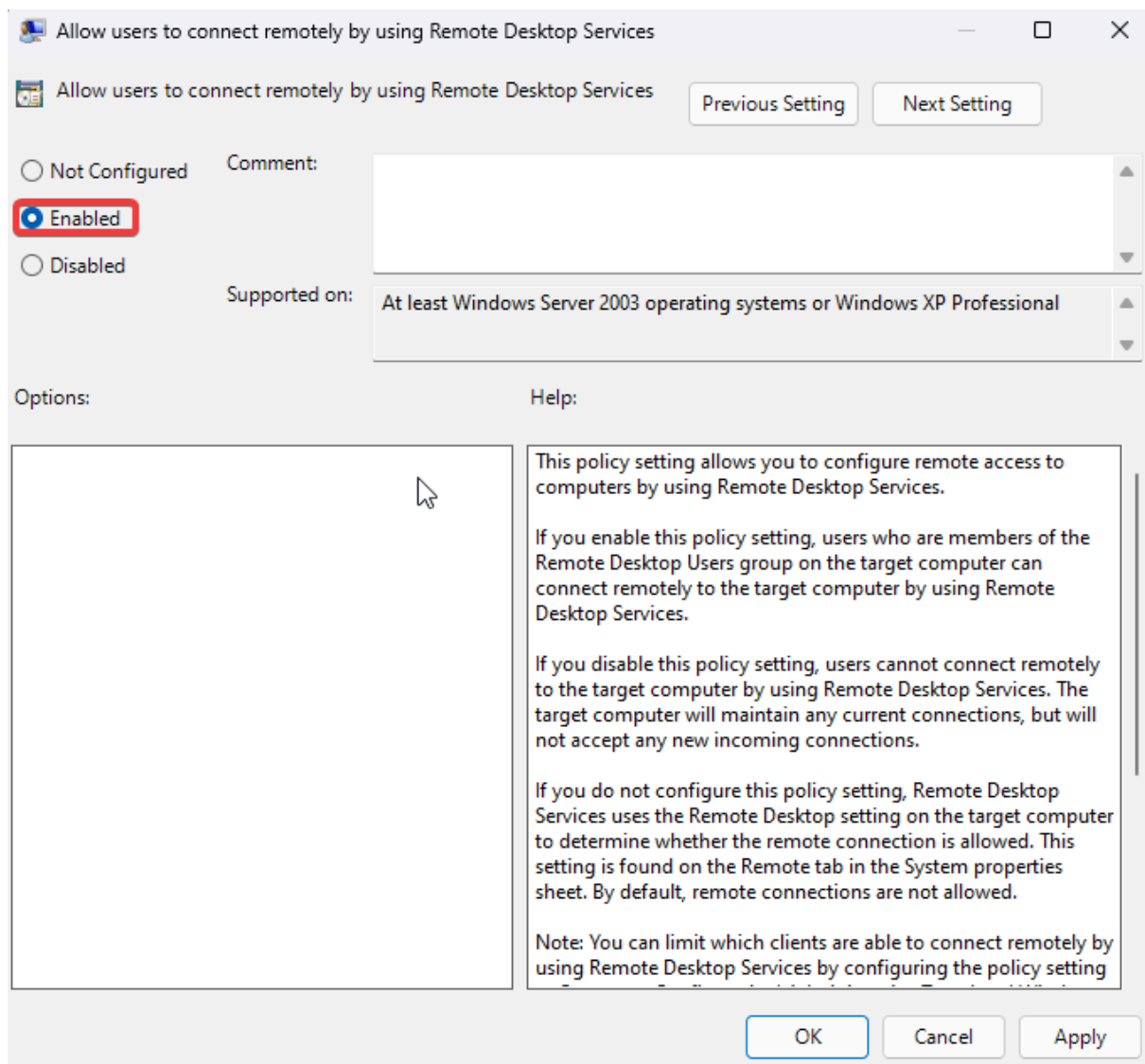
- You can also pin this menu to be always on top or unpin it to automatically hide it.
- If you get an access denied error, you would need to enable a group policy to allow unlisted programs to be started. To this end, open the '*Group Policy Editor*' by going to '*Start > Run > gpedit.msc*':



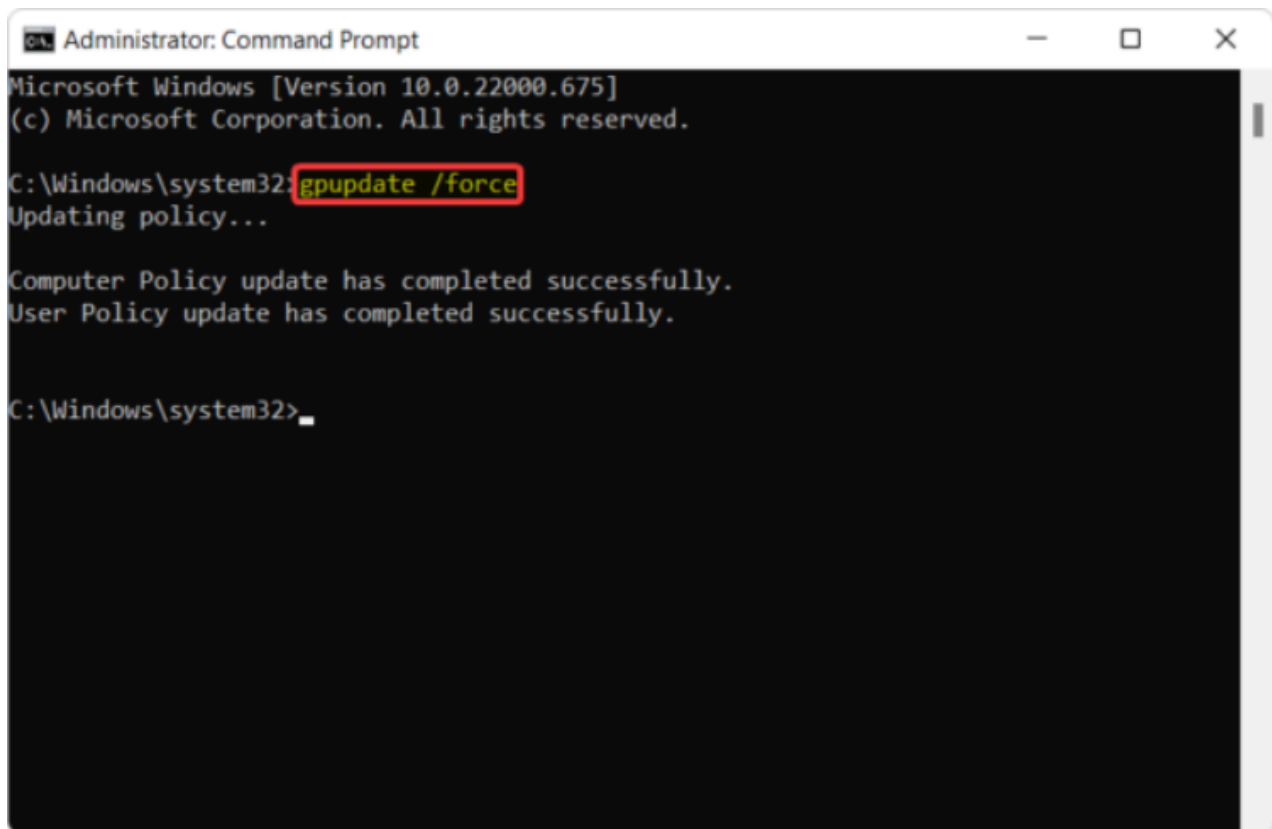
- On the '*Group Policy Editor*' navigate to:
- '*Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections > Allow users to connect remotely by using Remote Desktop Services*'



- Double click on this policy and then click on the check-box next to '*Enabled*':



- Afterwards, you'll have to update the group policies. In order to do this, call '*gpupdate /force*' from a '*Command Prompt*' window elevated as an Administrator:



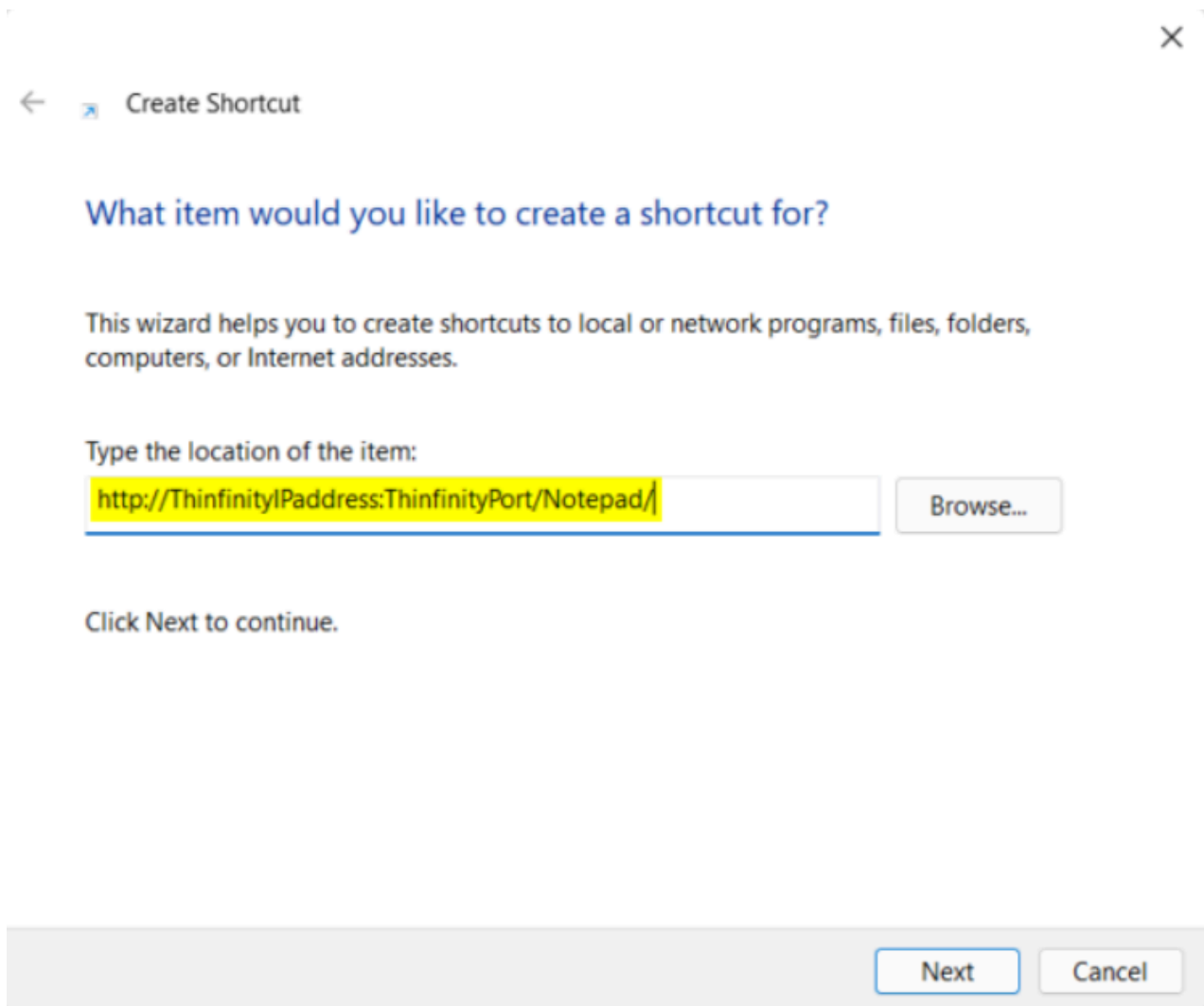
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Windows\system32>
```

- If you want to give your users quick access to your applications, you can create a desktop shortcut to the URL of VirtualUI with the Virtual Path of the application. Here's an example:



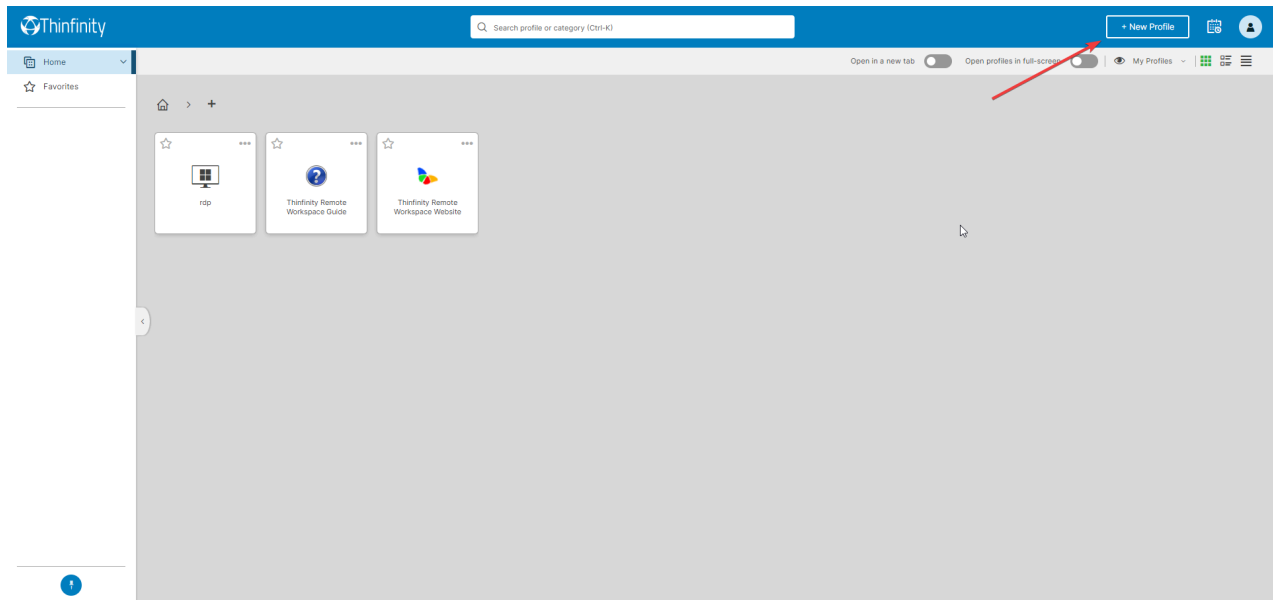
- To ensure these changes are applied, you can go to 'Start > Run > services.msc' and restart the 'Thinfinity Service Manager':

Services					
					Run new task Start Stop Restart ...
Name	PID	Description	Status	Group	
TapiSrv		Telephony	Stopped	NetworkServi...	
TeamViewer	6532	TeamViewer	Running		
TermService		Remote Desktop Services	Stopped	NetworkServi...	
TextInputManagementSe...	4888	Text Input Management Serv...	Running	LocalSystem...	
Themes	3528	Themes	Running	netsvcs	
ThinfinityRDToolsSvcMgr	6484	Thinfinity RDTools Service M...	Running		
ThinfinitySvcMgr	17320	Thinfinity Service Manager	Running		
ThinfinityVncSvc	6508	Thinfinity VNC Service	Running		
ThinfinityVUISvcMgr	6548	Thinfinity VirtualUI Services	Running		

- You can check our live demo and experience this feature yourself. You will be able to test this feature with the following Profiles:
 - Desktop
 - Notepad
 - Paint

Connecting to a Desktop

- With the New button activated, you will be able to see it on the Thinfinity® Remote Workspace landing page:





- After clicking on the button "New" , you'll see the Access window that allows you to choose from all the Access types of profiles that Thinfinity® has to offer. In this ocation, we will click on Desktop


×

Welcome! Let's create a new connection.

This wizard will help you create a new access profile. Please choose the type of connection you want to create.


Desktop


Application


Terminal

Access to a remote desktop or shared screen

Make this profile available to other users ☒


NEXT


Here we will choose RDP


×

Desktop Connection

Choose how you want to connect to the remote computer.


RDP

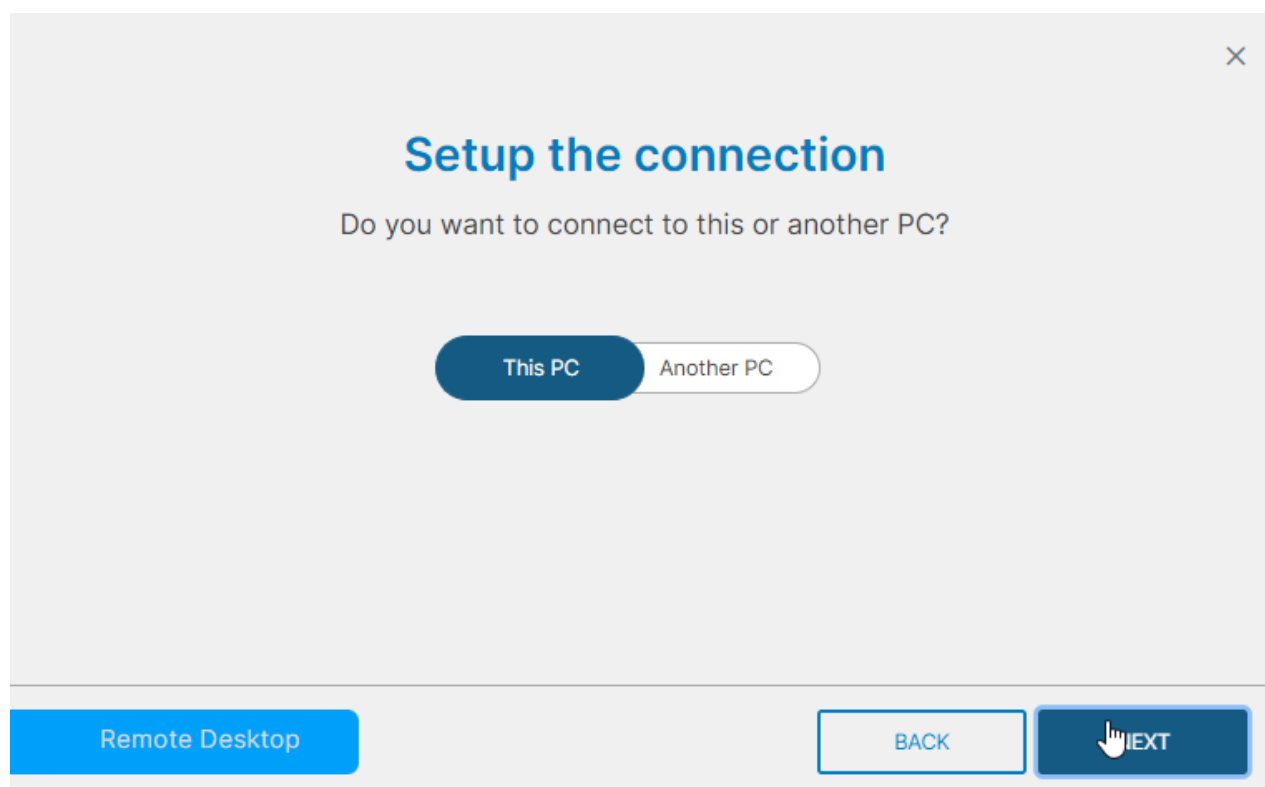

VNC/RFB


ThinVNC

Access to a remote desktop using RDP

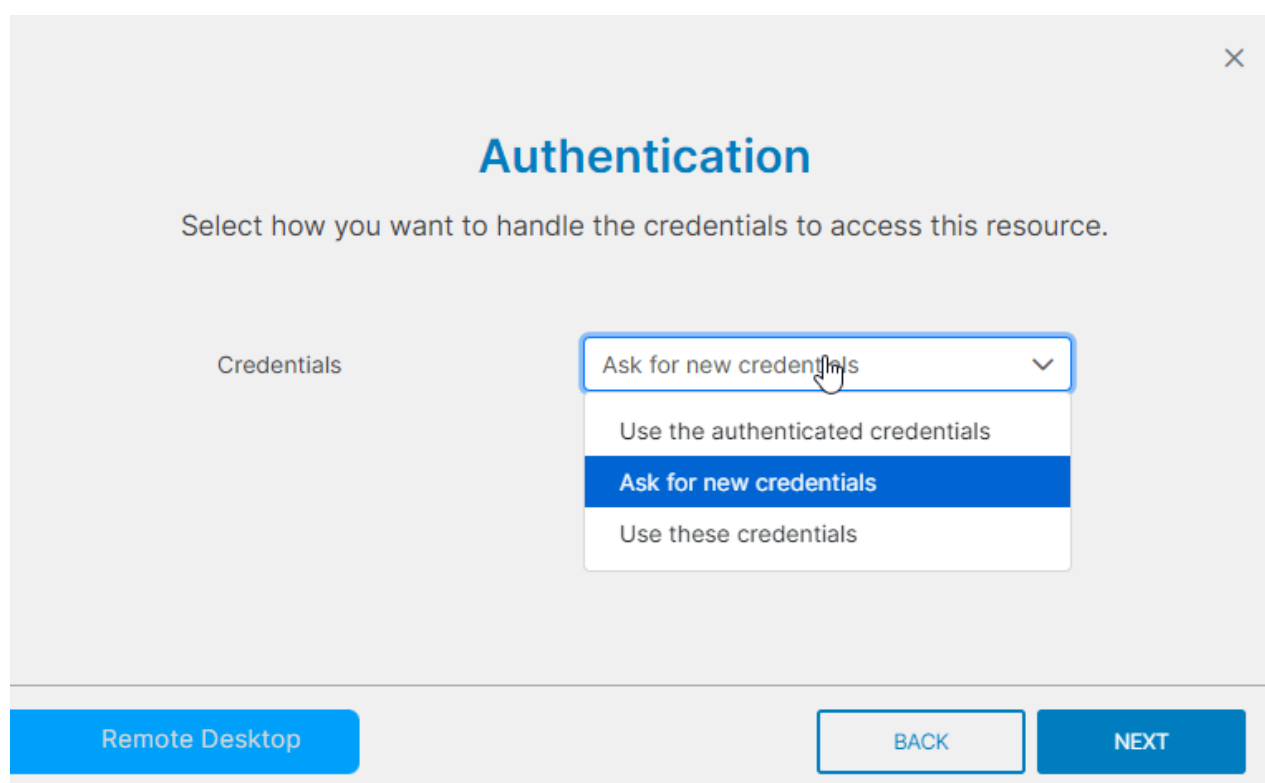
BACK NEXT

In the next window we get to choose if we want to create a connection to our current computer or another computer, for demonstration purposes we will choose "this computer" (both options work exactly the same from now on



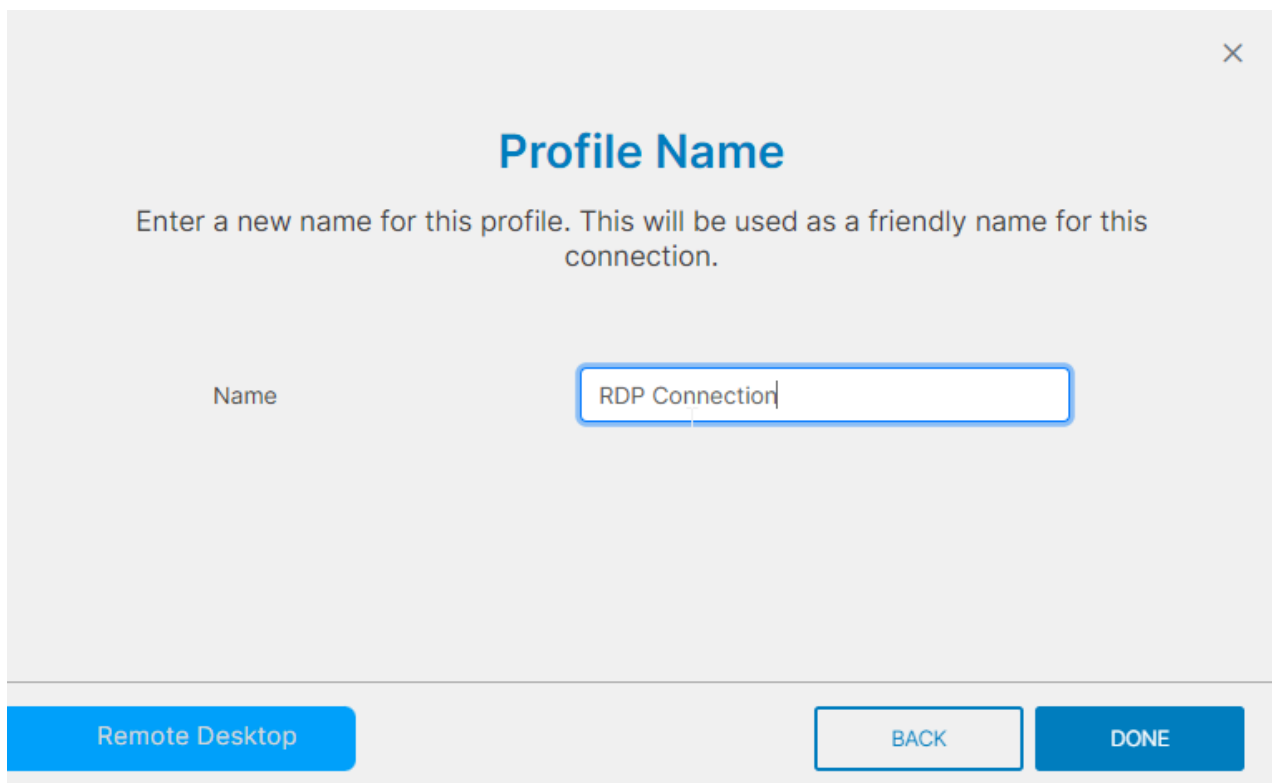
The screenshot shows a window titled "Setup the connection" with a close button (X) in the top right corner. Below the title is the question "Do you want to connect to this or another PC?". There are two buttons: "This PC" (highlighted in dark blue) and "Another PC" (white with a blue border). At the bottom, there is a blue "Remote Desktop" button on the left, and "BACK" and "NEXT" buttons on the right. A mouse cursor is pointing at the "NEXT" button.

Next, we choose the desired authentication method for this specific connection

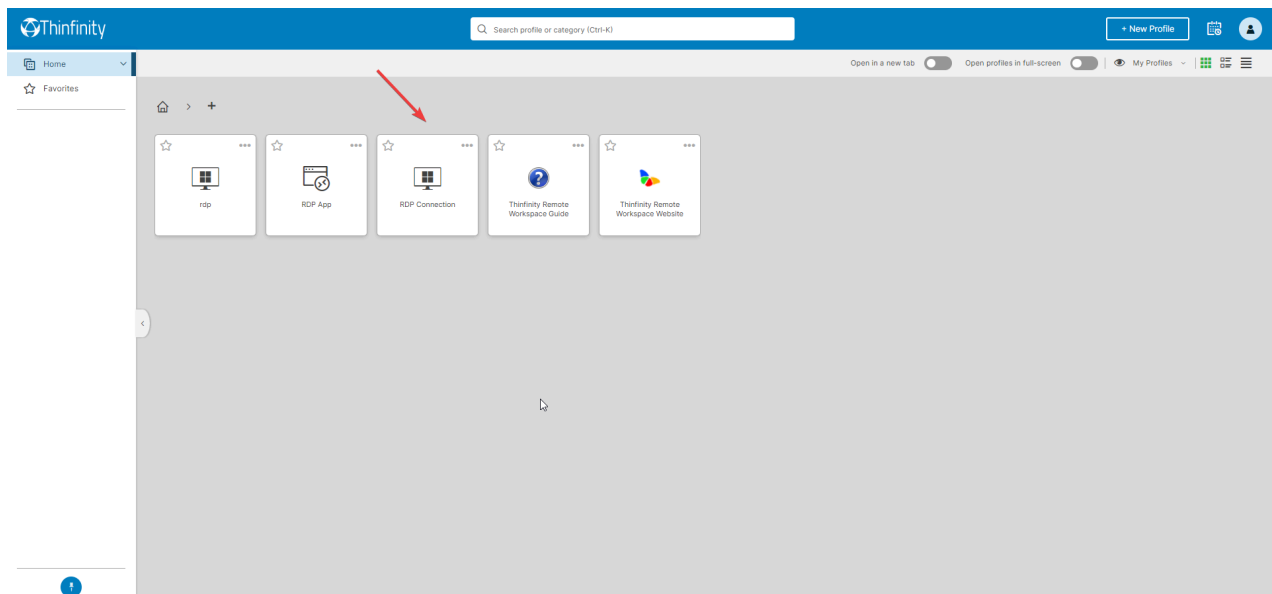


The screenshot shows a window titled "Authentication" with a close button (X) in the top right corner. Below the title is the instruction "Select how you want to handle the credentials to access this resource." There is a label "Credentials" on the left. A dropdown menu is open, showing four options: "Ask for new credentials" (selected and highlighted in blue), "Use the authenticated credentials", "Ask for new credentials" (highlighted in blue), and "Use these credentials". At the bottom, there is a blue "Remote Desktop" button on the left, and "BACK" and "NEXT" buttons on the right. A mouse cursor is pointing at the "Ask for new credentials" option in the dropdown menu.

Now we set the name of the connection

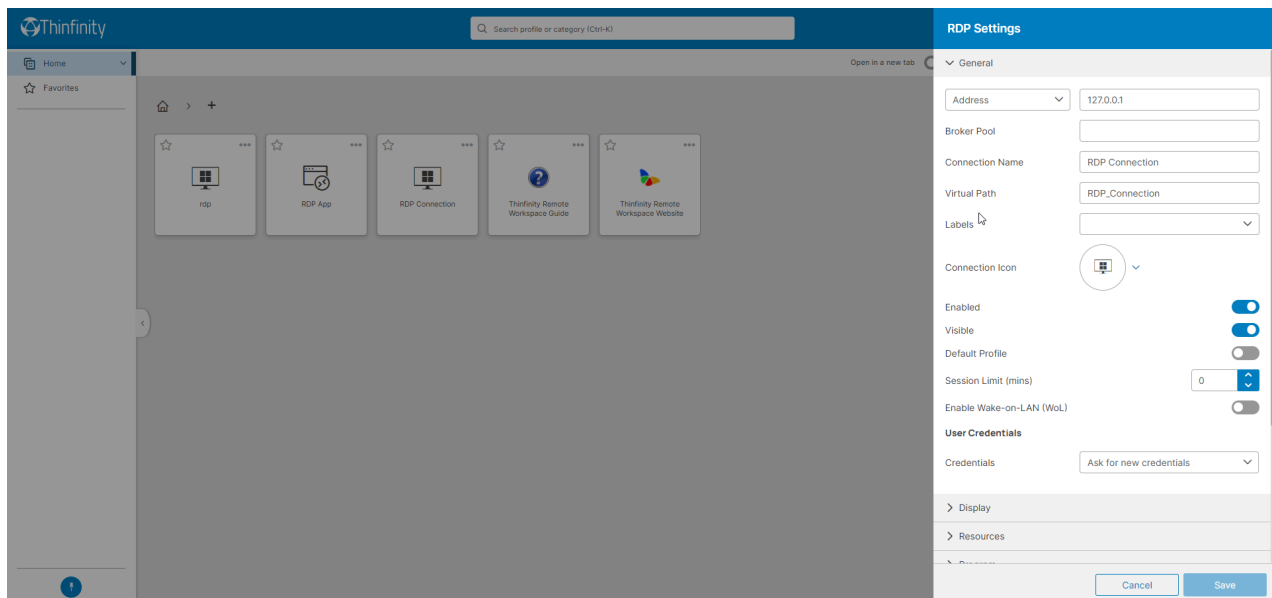
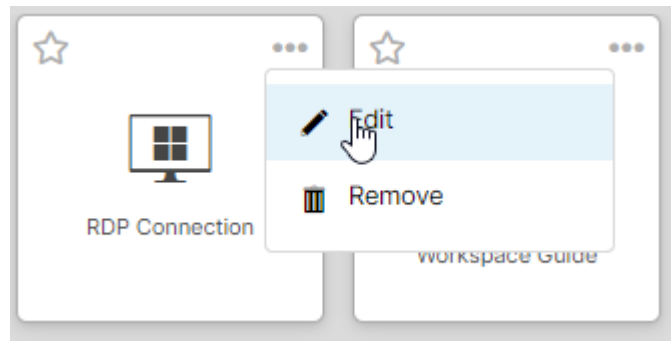


And after we click on done, our new connection will be ready to be used on the landing page



Another feature new to Thinfinity® Remote Workspace 6.0 is the ability to edit existing profiles in all aspects, same as on the client application. To be able to modify an existing connection, you would only need to click on the Edit button in

the form of a pen, above the profile icon: And lastly, you can also edit the configuration of the new connection by click on the "key" button:

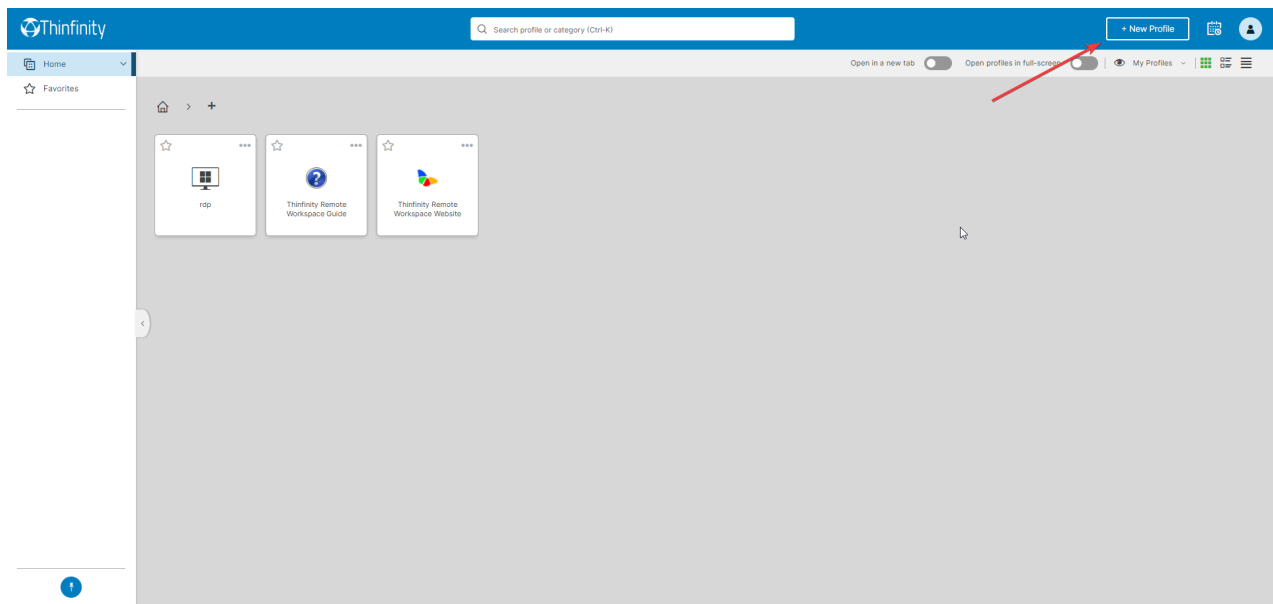


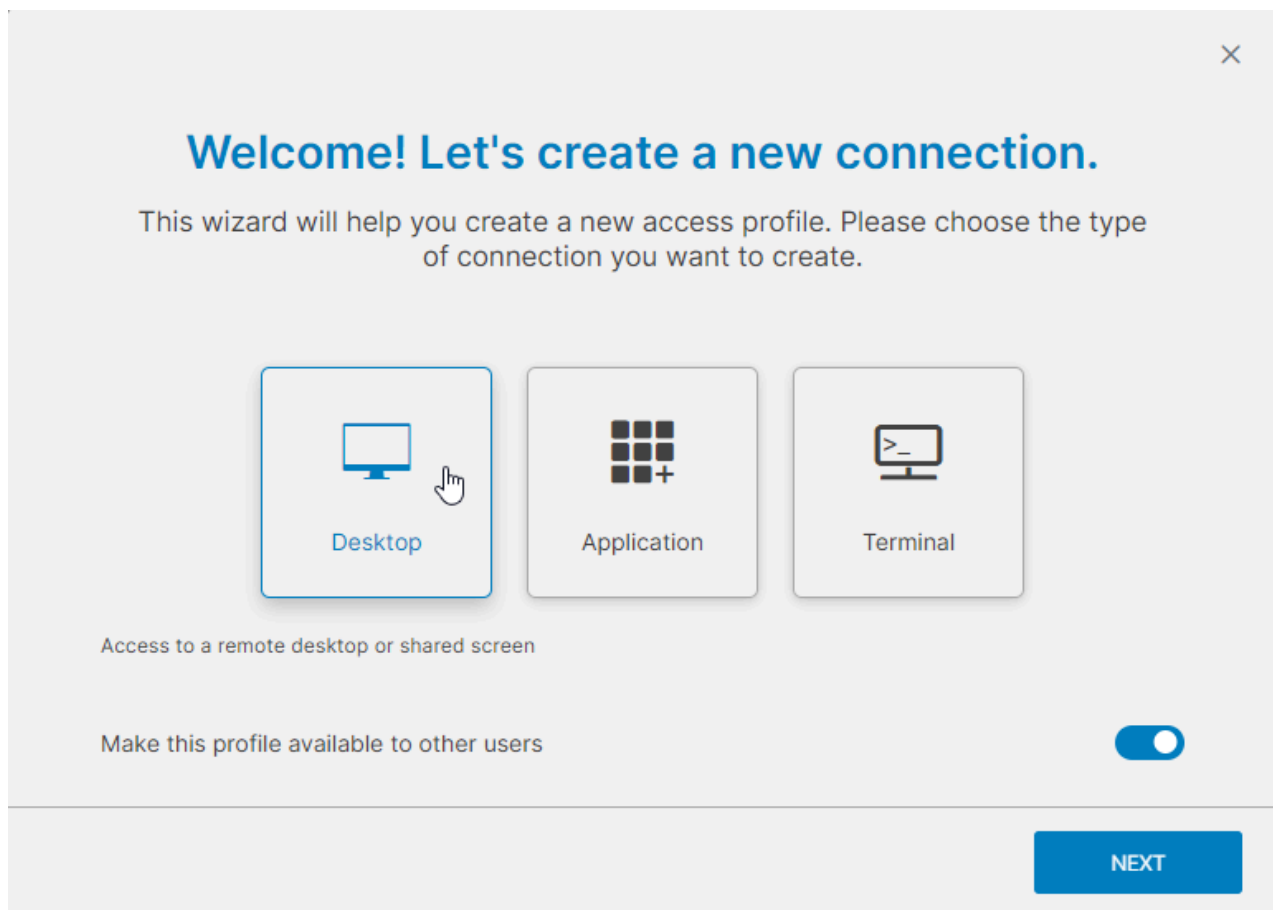
If you have any questions, feel free to email support@cybelesoft.com or leave a comment on this article.

How to create a VNC connection

1- Once your VNC server (in this case TightVNC) is installed, on the intended destination to which to connect via Thinfinity. You can leave all the settings as default. On the TightVNC Main manager, you can add for example a password for your new connection

2- Now you can go to your server and Enter the Thinfinity Remote Workspace Web Manager. Click on the "new" icon, select desktop, and click on next



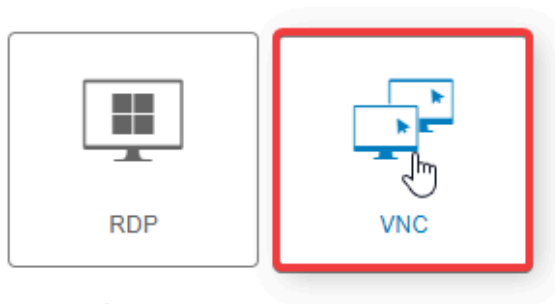


3- Now click on VNC



Desktop Connection

Choose how you want to connect to the remote computer.



Access to a remote shared screen using vnc

VNC / RFB

Back

Next

4- Choose the computer where you want to establish the connection



Setup the connection

Do you want to connect to this or another PC?



This PC

Another PC

Address



127.0.0.1

VNC / RFB

Back

Next

5- Set the credentials (if wanted), the name of the connection and click on "done"



Credentials

Select how you want to handle the credentials to access this resource.

Password:



VNC / RFB

Back

Next



Profile name

Enter a name for this new profile. This will be used as a friendly name for this connection.

Name

VNC Connection|



VNC / RFB

Back

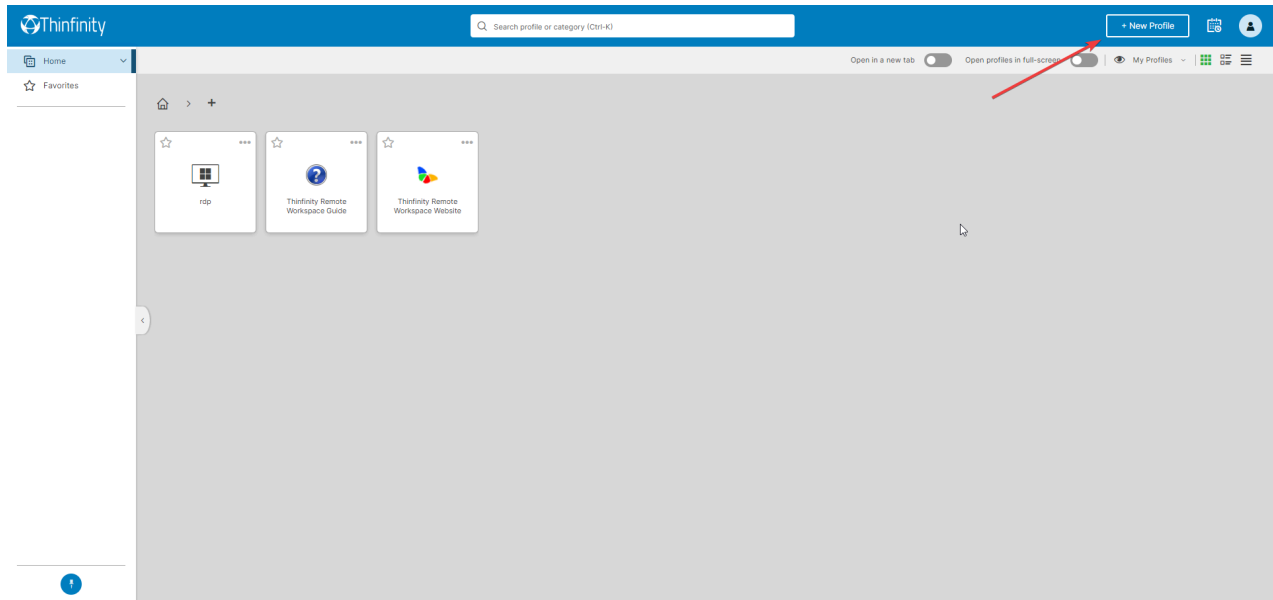
Done

And that's it, you are now able to connect to a VNC connection using Remote Workspace.

If you have any questions regarding this blog entry, you can leave a comment below or send us an email at support@cybelesoft.com ↗

How to SSH

To create a new SSH connection first we need to enter the landing page of Thinfinity Workspace, log in as a Web Manager user, and click on the "new profile" button





Then we click on the "Terminal" option


×

Welcome! Let's create a new connection.

This wizard will help you create a new access profile. Please choose the type of connection you want to create.


Desktop


Application


Terminal

Access to a telnet or ssh terminal

Make this profile available to other users ☒


NEXT


In the next screen we have to choose the address we are going to connect to, the port we are going to use and the desired protocol

×

Terminal Connection

Choose type of terminal Connection.


Telnet SSH


Multi Terminal

Access to Telnet SSH

BACK

NEXT

×

Setup a terminal connection

Specify the address and port to access the remote computer.

Address

Port

23

Auto ☒

SSH

☐

Terminal

BACK

NEXT

After that we get to configure the type of terminal we want to use

×

Terminal

Please specify the terminal type and display characteristics.

Terminal Type

ANSI

▼

Screen Size

24 rows x 80 cols

▼

Auto Wrap

☒

Send CRLF instead of CR

☐

Terminal

BACK

NEXT

Once that is set up, we have to choose a name for the connection and click on "done"

×

Profile Name

Enter a new name for this profile. This will be used as a friendly name for this connection.

Name

Terminal

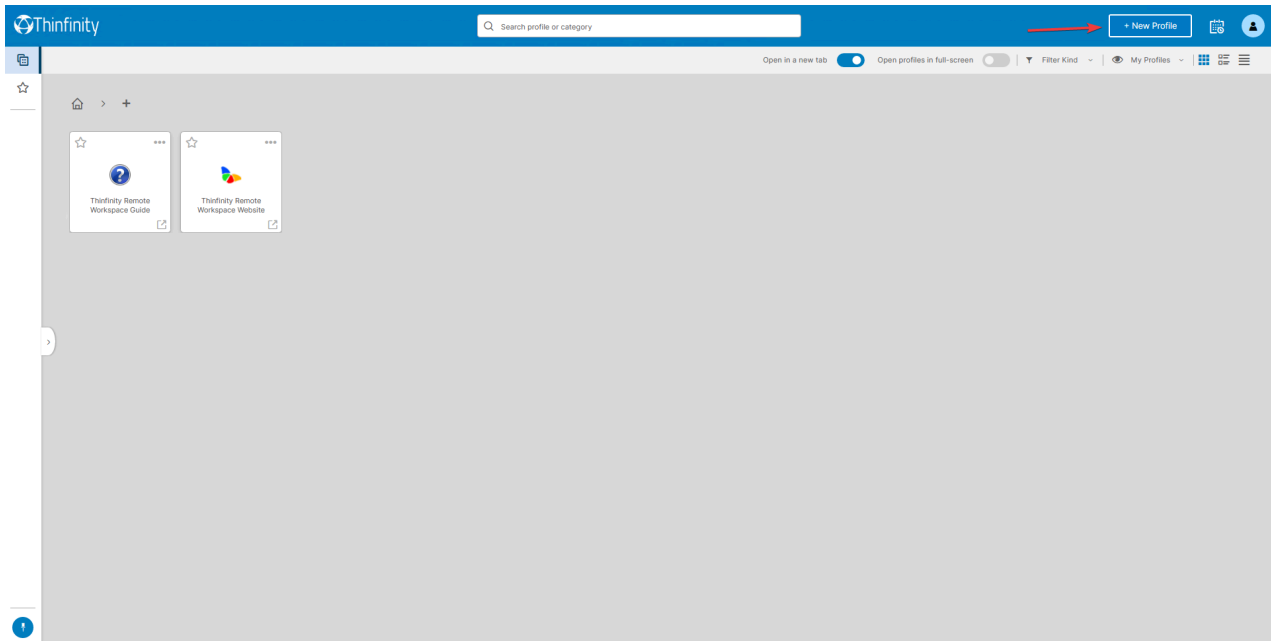
BACK

DONE

And the connection will be ready to use

Web Folder

The process of creating a Web Folder through the web manager is really simple. First, we need to be logged in the landing page as a Web Manager user, and click on the "new" button

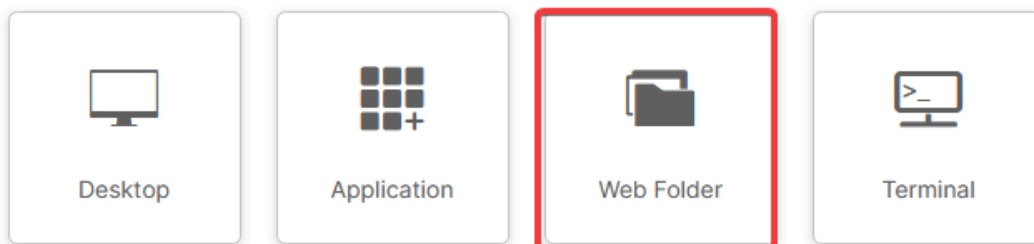


Then we choose the "web folder" option



Welcome! Let's create a new connection.

This wizard will help you create a new access profile. Please choose the type of connection you want to create.



Make this profile available to other users



NEXT

Now we have to choose the virtual path where the users are going to be connected



Setup a web folder

Add the path to a local folder you want to provide access to.

Path

C:\Temp

Web Folder

BACK

NEXT

Once that is done, we choose the name of the new folder, we click on "done" and the Web Folder will be ready to use

✕

Profile Name

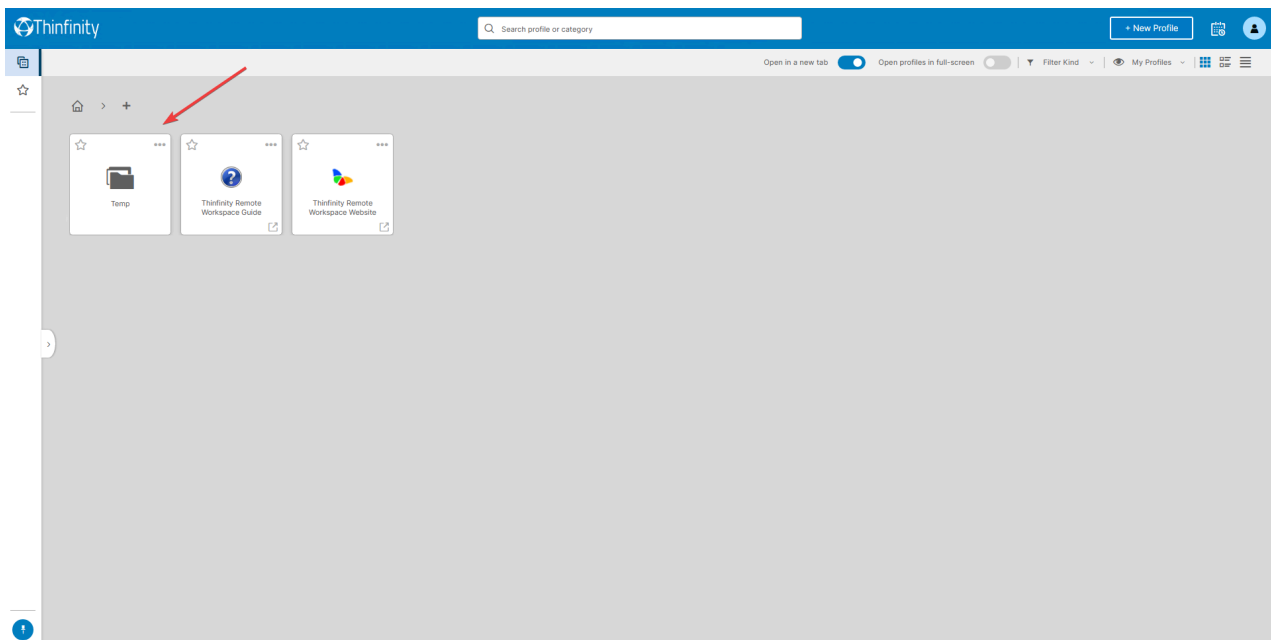
Enter a new name for this profile. This will be used as a friendly name for this connection.

Name

Web Folder

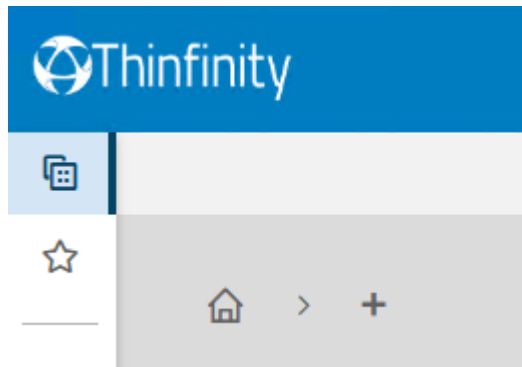
BACK

DONE

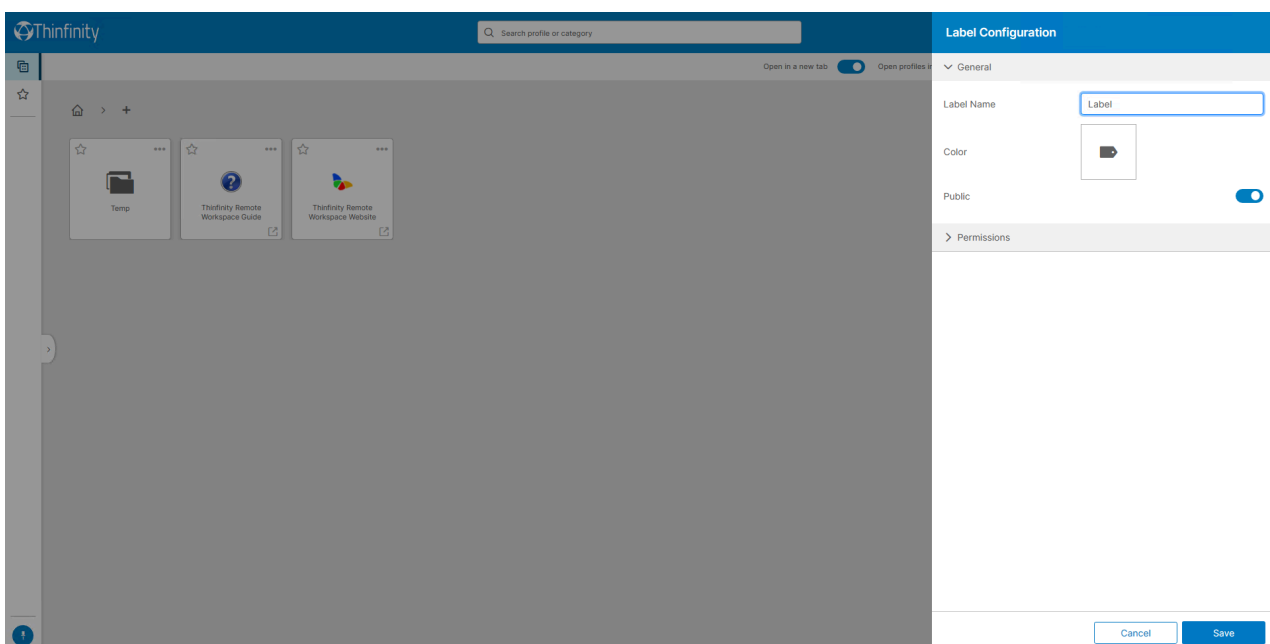


Labels

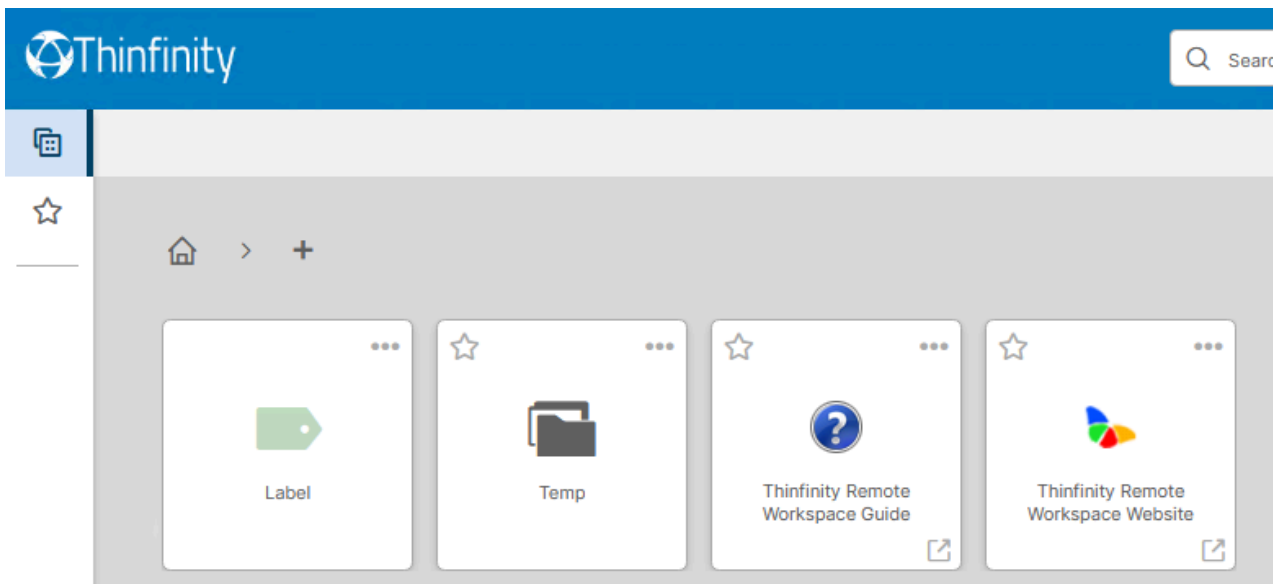
User-created Labels: You can also create labels from the Thinfinity Remote Workspace landing page: 1. Sign in 2. Click the “+” button



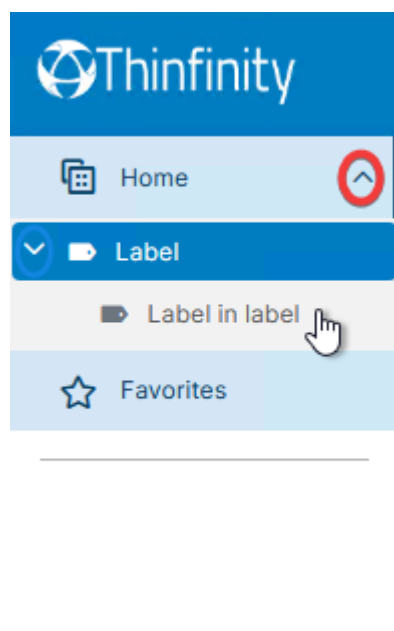
3. This will open the “Edit label” tab, where you can name the label and select a color for it.



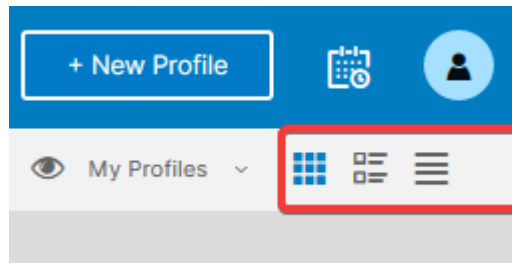
4. Once completed, the label will be added to the main menu. 5. By clicking on the label, you will be able to create RDP profiles and other labels, which can also have their own labels and profiles within.



6. There's a view option that you may find much more comfortable. It allows you to see the labels you have created and the labels within them. 7. Click on the button of the image below to access it.



8. There you will find the option "home" and when you click it, a list will open all the labels. Click on any label to expand the menu and see its child labels. To see the contents of a given label, just click on it.



9. The menu shows icons by default, but you can either display smaller icons or a list view, where you can see the name of the profile, the labels created and the connection type.

Edit Web Profiles

General

Here, you are able to edit the address of the Access Profile, its name, and virtual path, and you can choose to categorize it on a Label, as well as customize the icon, and enter credentials to log in. The Enabled button lets you decide whether the existing connection is active or not, whereas the Visible button lets you decide whether you wish for this connection to be accessible by users who aren't administrators.

General

Address

127.0.0.1

Broker Pool

Connection Name

Localhost


Virtual Path

Localhost

Labels

Select

Connection Icon



Enabled

☒

Visible

☒

User Credentials

Credentials

Use the authenticated credentials

Address	Enter the IP Address or domain name of the profile
Broker Pool	Enter the Broker Pool to which this profile belongs to
Connection Name	Enter the name of the profile for easy recognition
Virtual Path	Enter the virtual path of the profile. By default, it matches the Connection Name
Labels	You can place the profile as part of a Label, provided it's already created
Connection Icon	You can choose a specific icon for the profile or leave the one set up by default
Enabled	If Enabled is checked, this profile will be functioning on the landing page.
Visible	If Visible is checked, this profile will be visible to users on the landing page.
Credentials	You can specify to use the authenticated credentials; specific credentials that you can type here, or to be asked for credentials when you connect to the profile

Display

The Display section allows you to set up the color depth of the connection, ranging from 16bit to 32bit. It also lets you adjust the resolution of the session to fit to the browser window, fit to screen or specify the resolution. You can also change the quality of the image, ideal for low bandwidth scenarios, and whether to let Thinfinity® Workspace adjust the screen when the browser window is resized or not.

▼ Display

Color Depth

True Color (24bit)▼

Resolution

Fit to browser window▼

Image Quality

Optimum▼

Update session resolution on resize

Multi-monitor (GFX is required)

Color Depth	Choose the color depth for the remote computer view
Resolution	Choose from the available list of resolutions including "Fit to browser window" and "Fit to screen", ideal for hiding the browser and working on a full-screen mode
Image Quality	The connection image quality is related to the application's 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 at the other options below: Highest - Works only with PNG images and has no compression (0% compression) Optimal - Combines PNG and JPEG images (20%

	compression).Good - Works only with JPEG images (40% compression)Faster - Works only with JPEG images (50% compression)
Update session resolution on resize	With this option checked, the profile connection will adapt its resolution if the browser is resized
Multi-Monitor	With this option you can manually add multiple screens with the orientation you want

Resources

The Resources section lets you configure the features clipboard, virtual disk for file transfer operations, printer, and remote sound.

Resources

Enable Clipboard

Enable Intermediate Disk

Disk name

ThinDisk

Automatically download any newly-added file

Enable printer

Set As Default Printer

Printer Name

Thinfinity Remote Desktop Printer

PostScript Printer Driver

Microsoft XPS Document Writer V4

Enable Remote Sound

Enable Clipboard	Mark this option to enable the clipboard on the remote connection.
Enable Intermediate Disk	Check this option to have an intermediate disk available on the connections created through this profile.
Disk name	This is the name to identify the intermediate disk among the other remote desktop disks.
Automatically download any newly-added file	Enabling this option will download files as soon as they are added.

Enable printer	Uncheck this option to disable Thinfinity® Workspace PDF printer.
Set As Default Printer	Mark this option to make Thinfinity® Workspace printer the remote machine default 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® Workspace 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.
Enable Remote 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® Workspace will use to reproduce the remote sound. The highest quality, and the most

Program

The Program tab allows you to set up an app to start in the foreground of your connection, while the rest of the operating system is loaded in the background. You have two options to achieve this, Start a Program, which loads the selected application without any additional features, ideal for Windows 10 users. Or you can Execute it as a RemoteApp, for Windows Server users only. This creates an interface that lets you use more than one app instance at a time, while the rest of the server is hidden in the background.

Program

On Connection

Start a Program

Program path and file name

Arguments

Start in the following folder

On Connection	Select between Do Nothing (Normal desktop connection); Start a Program; Execute as RemoteApp
Program path and file name	Specify the complete path to give access to 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"

Experience

The Experience section has graphics features that you can choose from like RemoteFX, H264 support, and whether to have a desktop background visible or not, among other features.

The web interface "Experience" tab presents you with the following options:

▼ Experience

Graphics

Remote FX

GFX

H264 (requires a minimum resolution of 800 × 600)

Desktop Background

Visual Styles

Menu and Window Animation

Font Smoothing

Show window contents while dragging

Desktop Composition

Miscellaneous

Smart Sizing

Multitouch Redirection

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 ↗ .

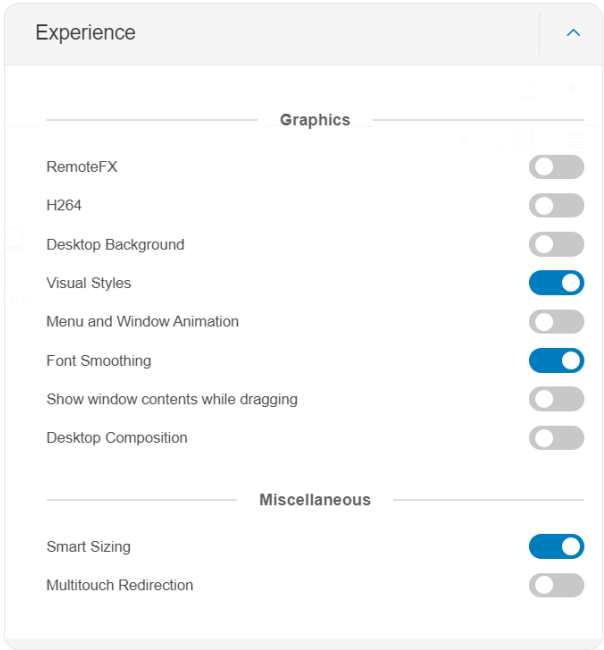
GFX	
H264	
RemoteFX	Check this option to enable RemoteFX. Read More about Remote FX ↗ . This option affects other settings.
Desktop Background	Check this option to show the desktop background.
Visual Styles	Check this option to show Windows Visual Styles: the appearance of common controls, colors, borders, 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.
On Connection	Select between Do Nothing (Normal desktop connection); Start a Program; Execute as RemoteApp
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"

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

Advanced

The Experience section has graphics features that you can choose from like RemoteFX, H264 support, and whether to have a desktop background visible or

not, among other features.



The web interface "Experience" tab presents you with 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.
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.
On Connection	Select between Do Nothing (Normal desktop connection); Start a Program; Execute as RemoteApp
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.
	Inform a context directory for the program

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

Access Hours

The Access Hours feature lets you choose a schedule for when your users are able to connect to this profile. You can choose the exact days and hours, and even specific dates. That way, the user won't be able to see the connection during off-hours.

Access Hours

All

0

2

4

6

8

10

12

14

16

18

20

22

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

*

☒ Access Allowed
 ☐ Access Denied

☐ Allow access only within this period:

01/30/2022 to 01/30/2022

OPTION	DESCRIPTION
Access Permitted	Define which day and hour the application will be available
Access Denied	Define which day and hour the application will be disabled
Allow Access only within this period	Define which days the application will be disabled or enabled

Permissions

The Permissions tab lets you choose whether the Access Profile is able to be seen by anyone, a specific user, or a group of users.

Permissions

Allow anonymous access

Users

Group or usernames:

+ Add

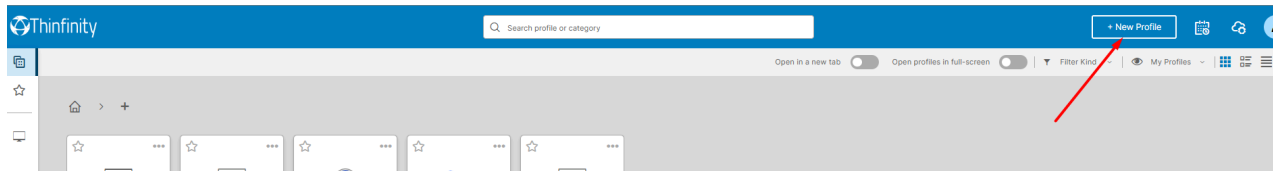
Name

Actions

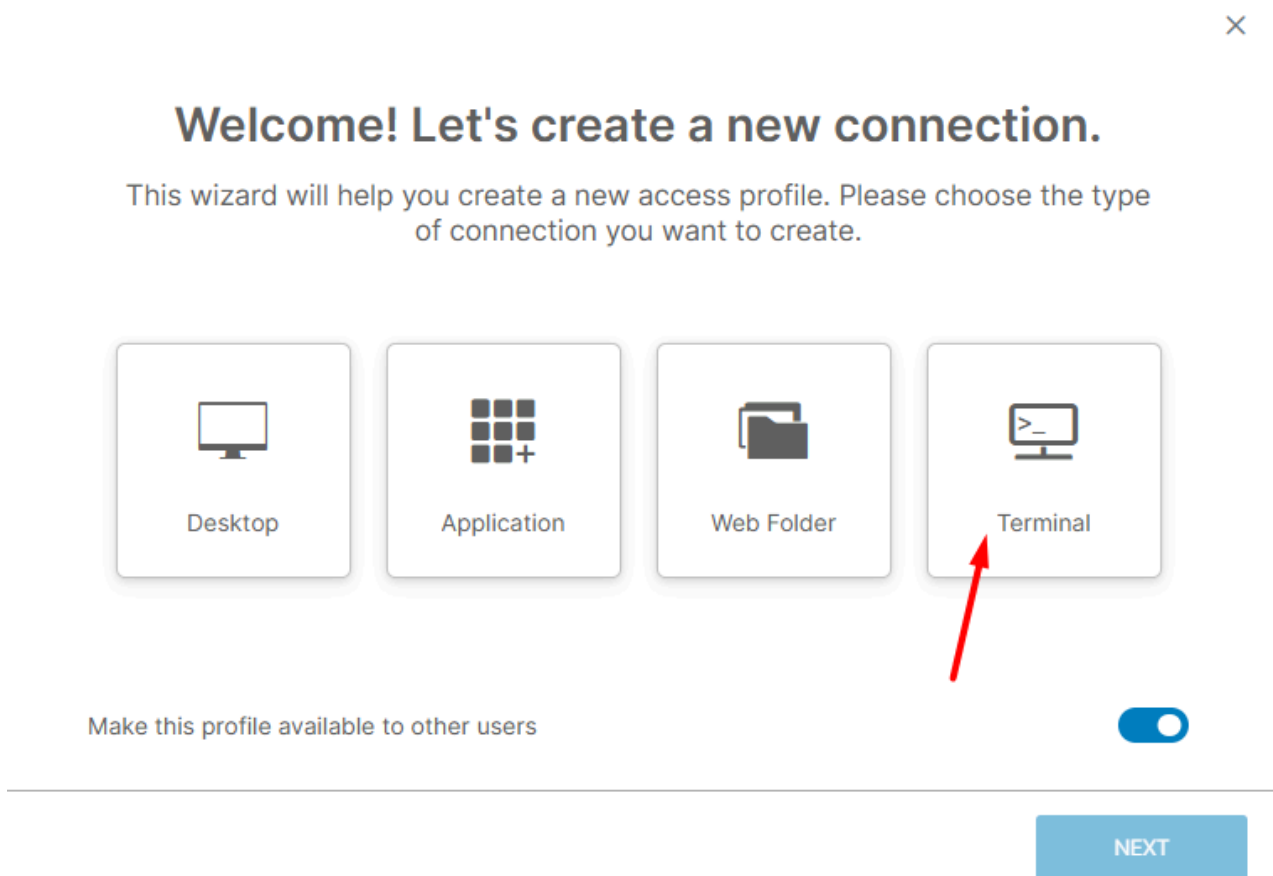
OPTION	DESCRIPTION
Allow anonymous access	Check this option to make this profile available without any authentication. Use this option, if you want this profile to be available for everyone. This means that everybody accessing Thinfinity® Workspace will see this profile. Checking this option will disable 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.

Multi Terminal

To create a connection through the Multi Terminal feature. Head to the landing page and click on "New Profile":



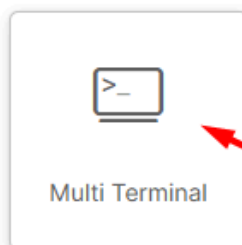
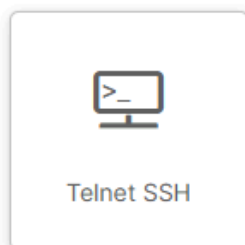
Afterwards, select Terminal and "Multi Terminal" after:





Terminal Connection

Choose type of terminal Connection.



BACK

NEXT

The following screen will pop up. Choose a name for your Multi Terminal profile:



Profile Name

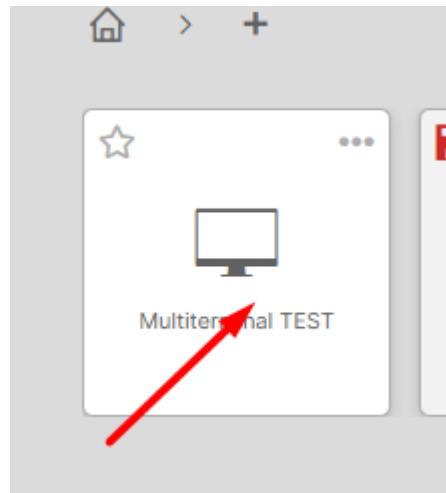
Enter a new name for this profile. This will be used as a friendly name for this connection.

Name

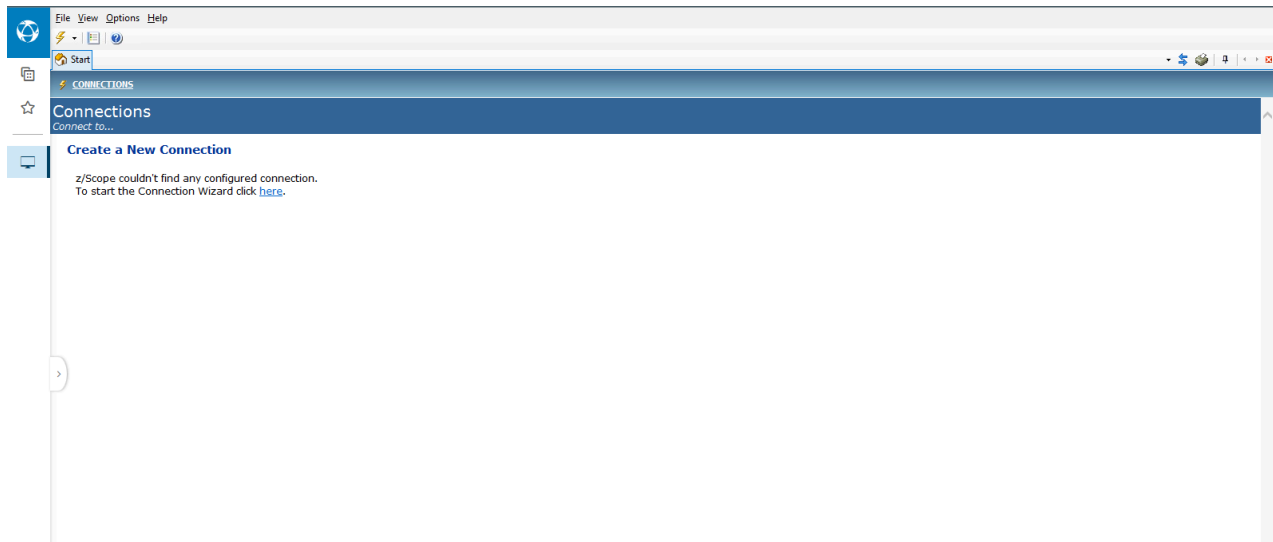
BACK

DONE

Afterwards, your profile will be successfully created and you can view it on the landing page like this:



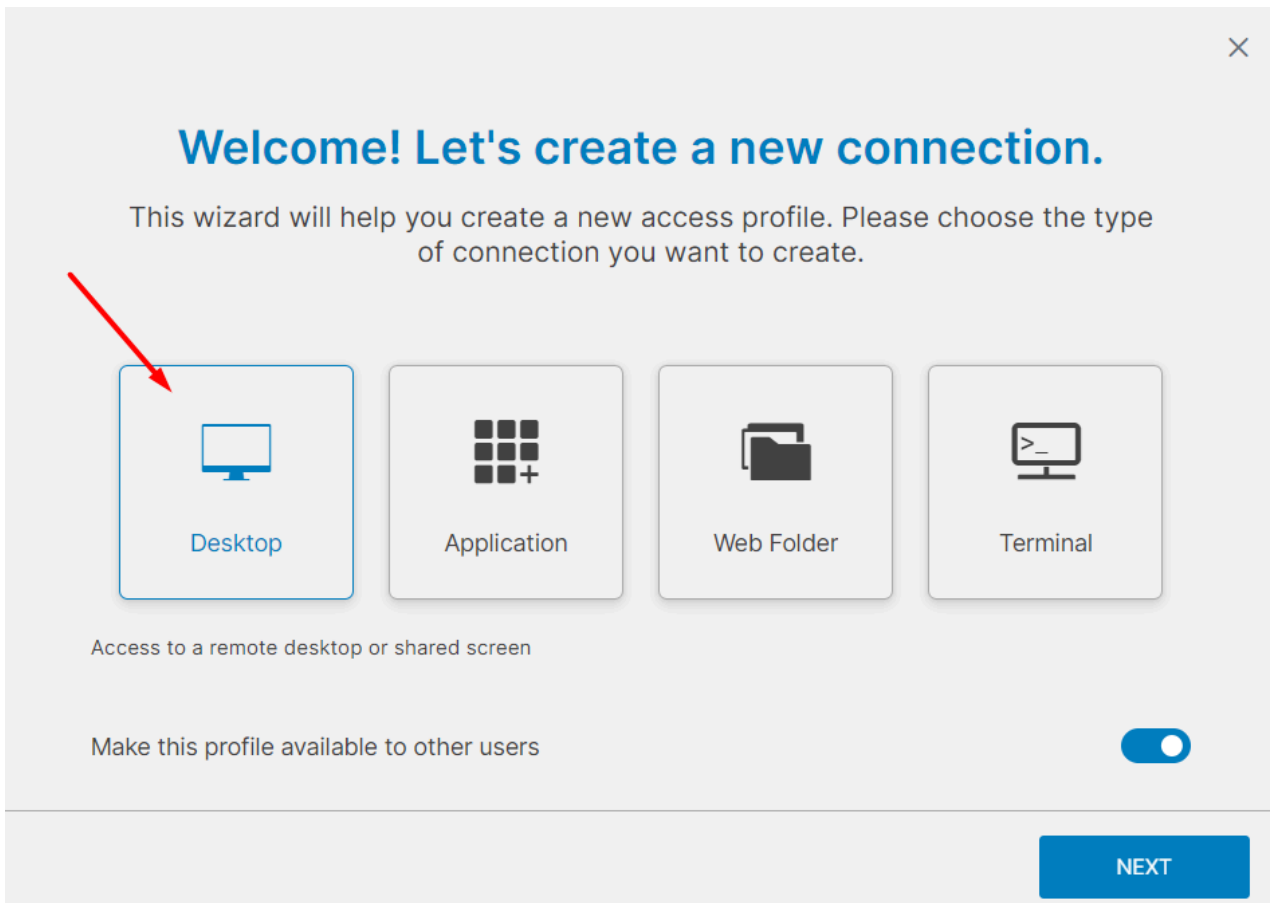
When you execute it, you should see the multi-terminal emulator in your screen:



Thinfinity VNC

Connecting to a Thinfinity VNC Instance

In order to connect to your ThinVNC instance through your Thinfinity® Remote Workspace, go to your Thinfinity® Remote Workspace Landing Page, and click on "New Profile". Select **Desktop** and click Next.



Welcome! Let's create a new connection.

This wizard will help you create a new access profile. Please choose the type of connection you want to create.

Desktop

Application

Web Folder

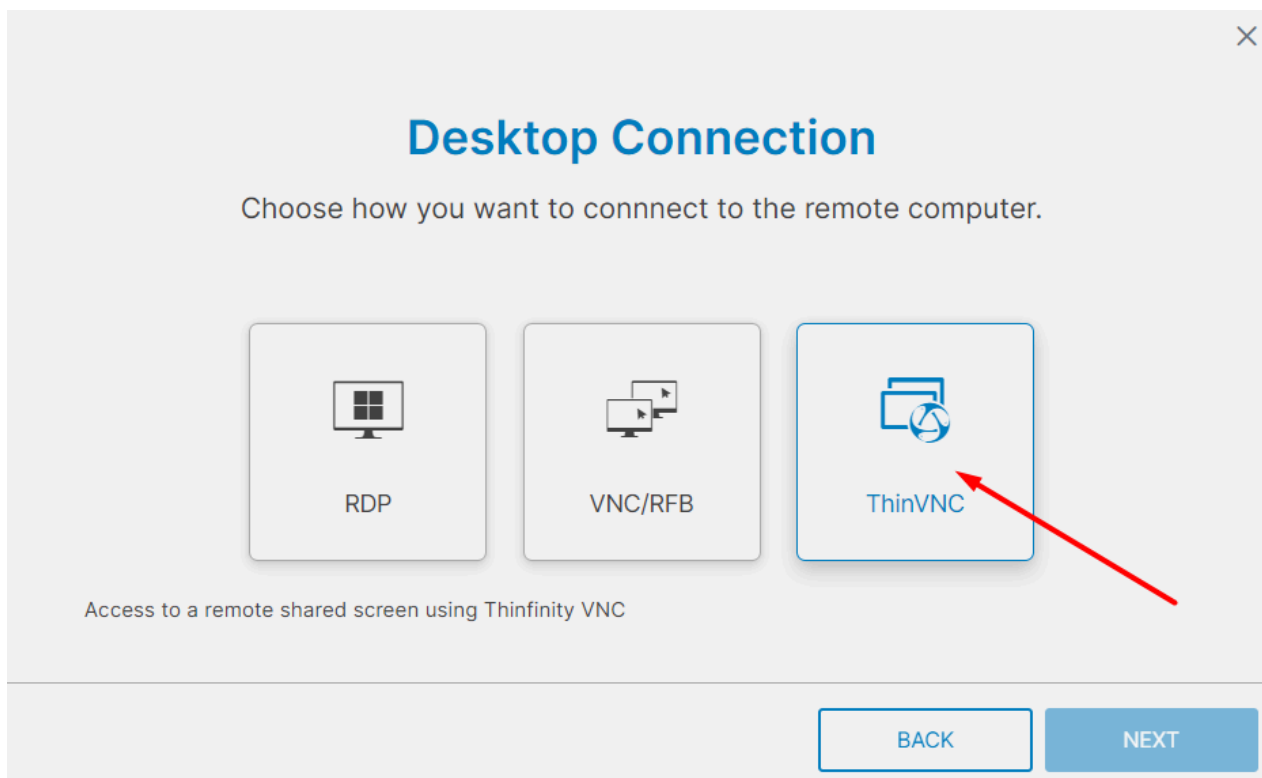
Terminal

Access to a remote desktop or shared screen

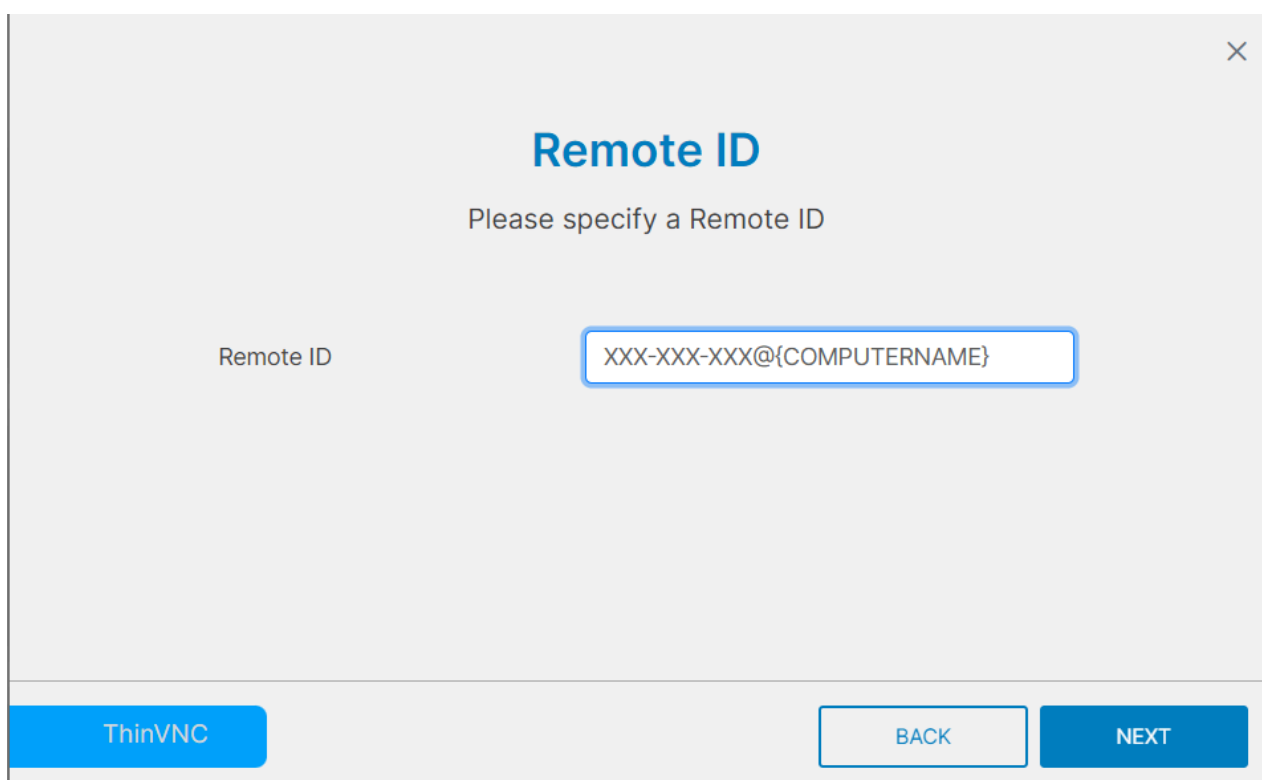
Make this profile available to other users ☒

NEXT

Select **ThinVNC** and click Next.



In the next screen you will be prompted for the **Remote ID** from your ThinVNC Instance. This value should already be declared in your ThinVNC instance and can be found in the "Gateway Access" tab in your ThinVNC manager.



Thinfinity VNC ×

File Help

General Direct Access Gateway Access Security Screen Sharing License

☒ Enable

URL:

Network ID:

Remote ID:

Password:

Status: **Registered**

Click "Next", in the following screen, you will be prompted for the **Password** that's declared in your ThinVNC manager below the RemoteID.

×

Credentials

Please specify a password

Password

Password confirmation

ThinVNC

Click Next, in the next screen, you will be prompted for a name for the profile. Input whichever name you desire for it:

×

Profile Name

Enter a new name for this profile. This will be used as a friendly name for this connection.

Name

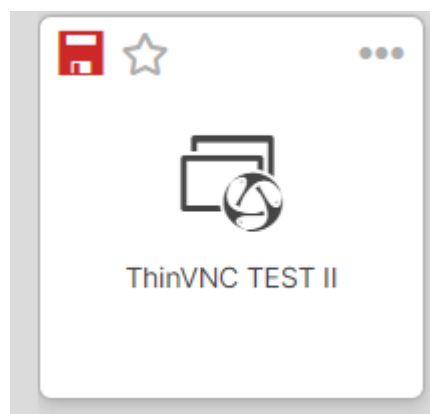
ThinVNC TEST II

ThinVNC

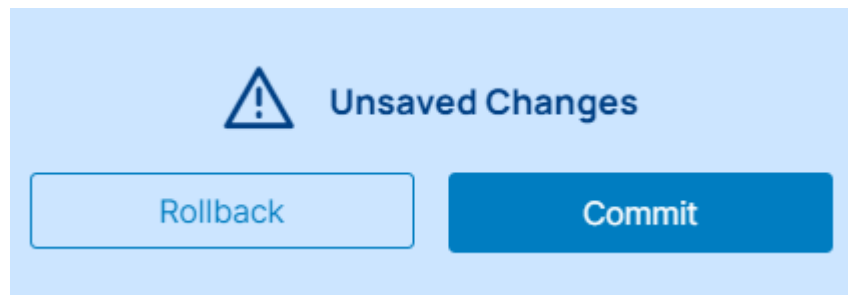
BACK

DONE

Click Done, and you should now see your ThinVNC profile in your Thinfinity® Remote Workspace Landing Page, ready to use:



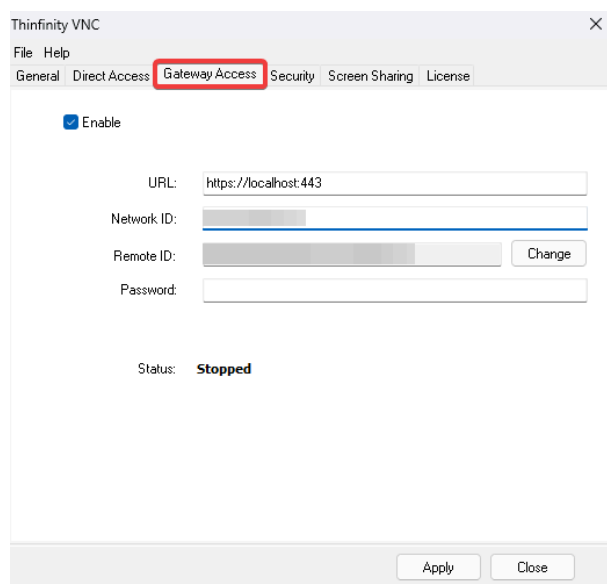
Afterwards, click **Commit** to save changes in the lower right side of the screen:



You should now be able to connect through your ThinVNC connection from your Workspace.

Configuring the Thinfinity VNC Agent to work with Workspace

In order to configure the Thinfinity VNC Agent, head to the Thinfinity VNC Manager's Gateway Access tab:



URL [String]: The URL that points to your Thinfinity® Remote Workspace Landing Page. If it's the same server you're using ThinVNC on, you can use localhost and your desired protocol+port.

NETWORK ID [String]: The Network ID identifies this installation. Any Thinfinity® Remote Workspace servers that want to share their resources through one or more Gateways must match their Network ID.

REMOTE ID [String]: This value identifies your computer/server (Where the agent is installed). Thinfinity® creates a random ID automatically, it could be modified using *any* alphanumeric value.

Password [String]: This password corresponds to the computer's RemoteID. This password is what your Thinfinity® Remote Workspace requires to validate against the ThinVNC service to make the connection between both services. This is not for allowing/restricting access to users.

In short, the **URL & Network ID** values are provided by your Thinfinity® Remote Workspace server environment. And the **REMOTE ID & Password** both need to be declared in the ThinVNC side and then copied in your Thinfinity® Remote Workspace Landing Page when creating the ThinVNC profile.

Advanced Features

Bidirectional Audio Redirection

By default, the microphone redirection will be enabled.

Access Profiles:

Enable Bidirectional Audio Redirection on the Thinfinity® Remote Workspace Configuration Manager:

- Go to the '*Access Profiles*' tab.
- Edit the profile where you want to enable remote sound.
- Go to the '*Resources*' tab.
- Check the '*Enable Sound*' option:

Thinfinity Configuration Manager - Profile Editor

Name: Localhost

Virtual Path: Localhost

Access Key: tiYlfmYqip8tN2Va3WSkrK1vGNfvTLby

Label(s): \

Visible ☒ Default profile ☐

RDP ☒ RDS Web Feed ☐

General | Display | **Resources** | Program | Experience | Advanced | Printer | Permissions | Restrictions | Access Hours | Auth

☒ Enable Clipboard

☒ Enable Intermediate Disk

Disk name:

ThinDisk

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

☒ Automatically download any newly-added file

☐ Disable these file extensions:

☒ **Enable Sound**

Sound quality:


Optimum

Ok Cancel

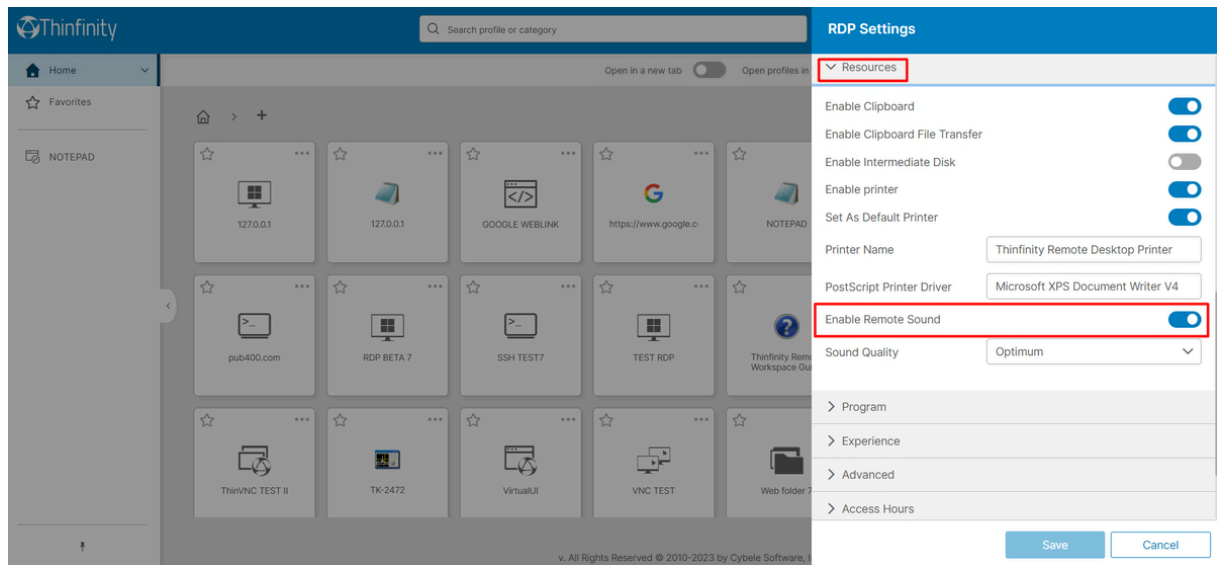
- The default sound quality is the '*Optimal*'. You can increase the quality, by setting it up to '*Excellent*', or make it lower, to gain performance.
- On the Web Interface, connect to a remote machine using this profile and try to listen to any sound playing remotely.

Other authentication methods (none, "+" profile):

Enable sound right before connecting on the web interface:

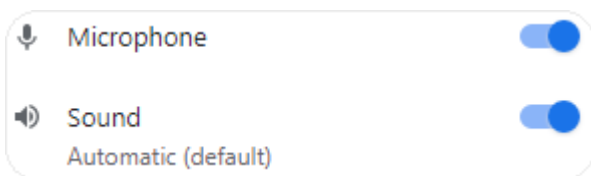
- Once on the web interface, click on the Edit button  (pen on the top-right corner of the Profile button) and go to the '*Resources*' tab.
- Check the option '*Enable Remote Sound*':

- Choose the quality.



- Connect and play a remote sound from your preferred browser.

i When you have the microphone redirection enabled, you would need to allow access to said microphone on your browser as well:



i You can copy the file '*web.settings.js*' to '*C:\ProgramData\Cybele Software\Thinfinity\Workspace\DB*'. This way, your settings won't be lost when upgrading Thinfinity® Remote Workspace in the future.

Remote Active Directory

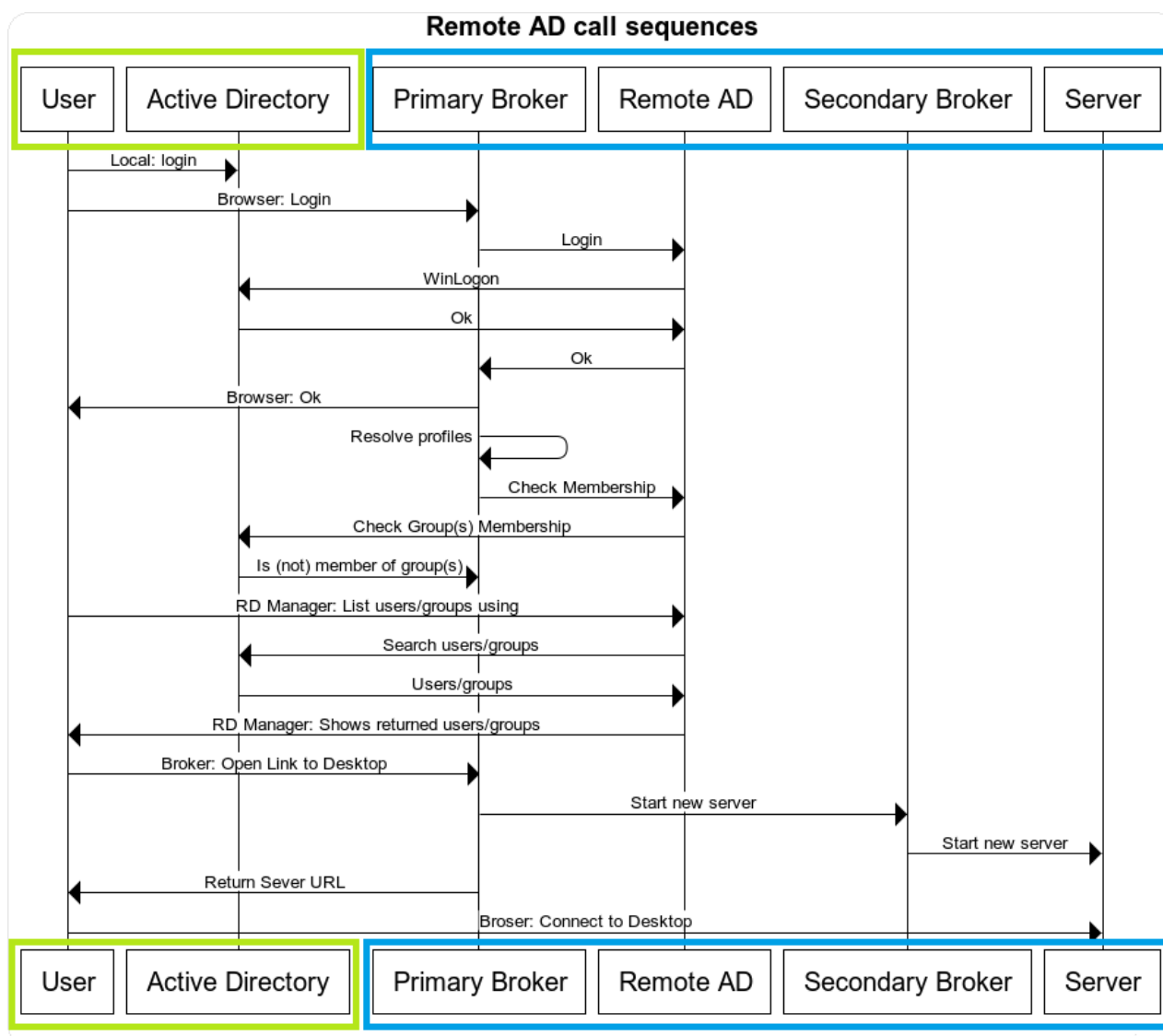
Authentication Against a Remote Active Directory services

Thinfinit® Remote AD Services will allow the same access security all around, allowing the client to manage users and groups in their own environment.

Thinfinit® Remote AD Services will connect to the client's Active Directory through a restricted user account. It will query only for the information needed to manage the login and end-user's permissions to access the remote apps.

Thinfinit® Remote Workspace will validate end-users against their own AD and will map with a user account on the app-side AD to create the remote windows session.

Validation and encrypted data will be all still handled by the client's AD and according to their environment's policies. The primary broker exchanges information with the Remote AD service on-demand as shown in the following flow:



Login process:

Thinfinit® Remote Workspace landing page requests your user's login credentials and validates them against the clients' AD. If validated correctly, the end-user will access the Thinfinit® Remote Workspace main page, which will allow them to select the app they need to run. By using this method of authentication we can guarantee transparency for your users as well as a secure access method in line with your current security policies.

Validating user permissions:

Each app or desktop link to be presented to the end-user must be validated against the AD according to the configured permissions of the profile. Thinfinit® Remote Workspace will validate the current logged on user against the users and groups

associated to the profile. To do this it will query remotely to the clients' AD to verify membership. Only true or false is returned on the query, thus no information can be cached.

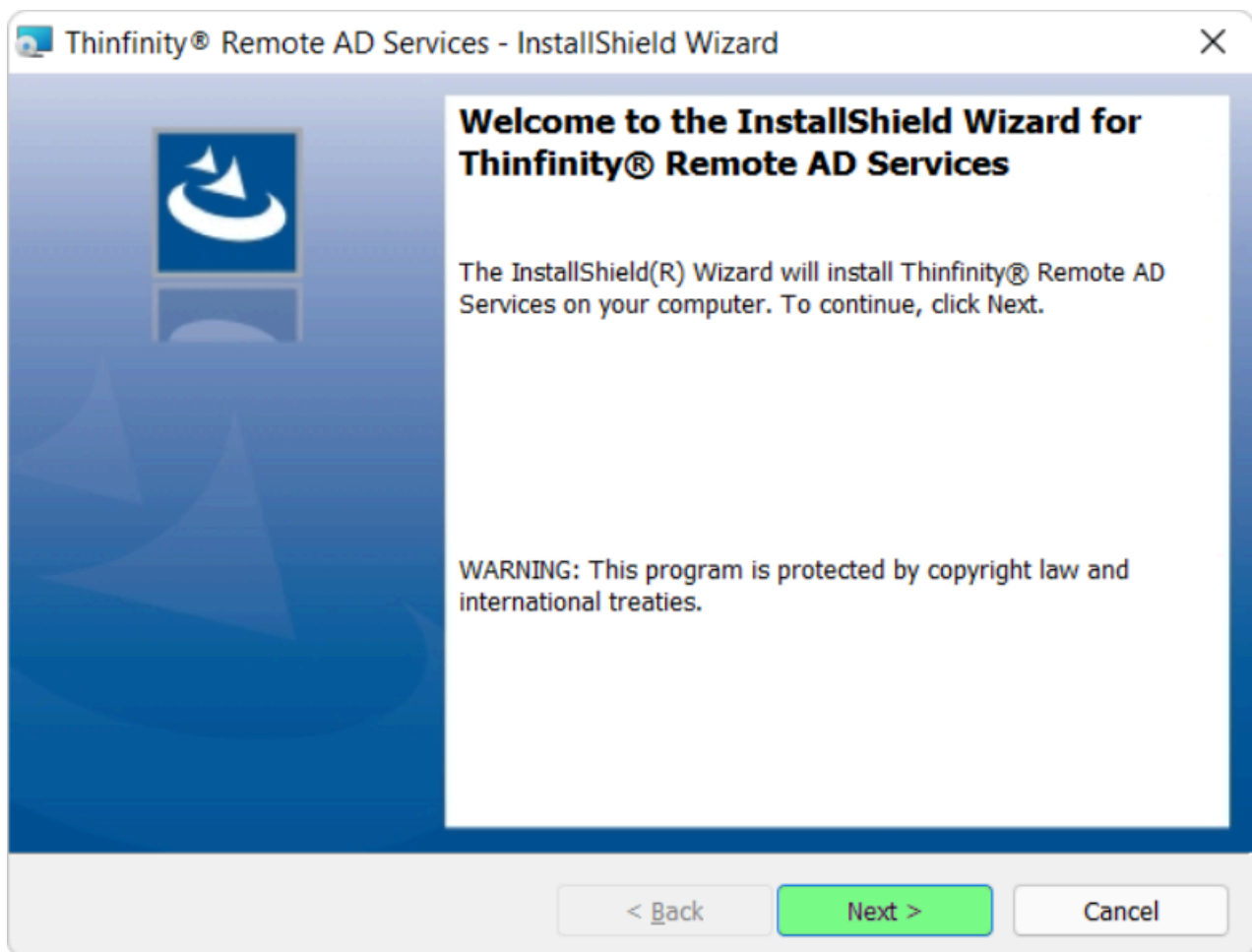
Configuring Thinfinity® Remote Workspace permissions:

Thinfinity® Remote Workspace needs to access the remote AD to list users and groups (only IDs) to associate them to each profile that requires access permissions. Only IDs are retrieved and restricted to the groups that Thinfinity® Remote AD Services is allowed to based on the Windows Service user account configured.

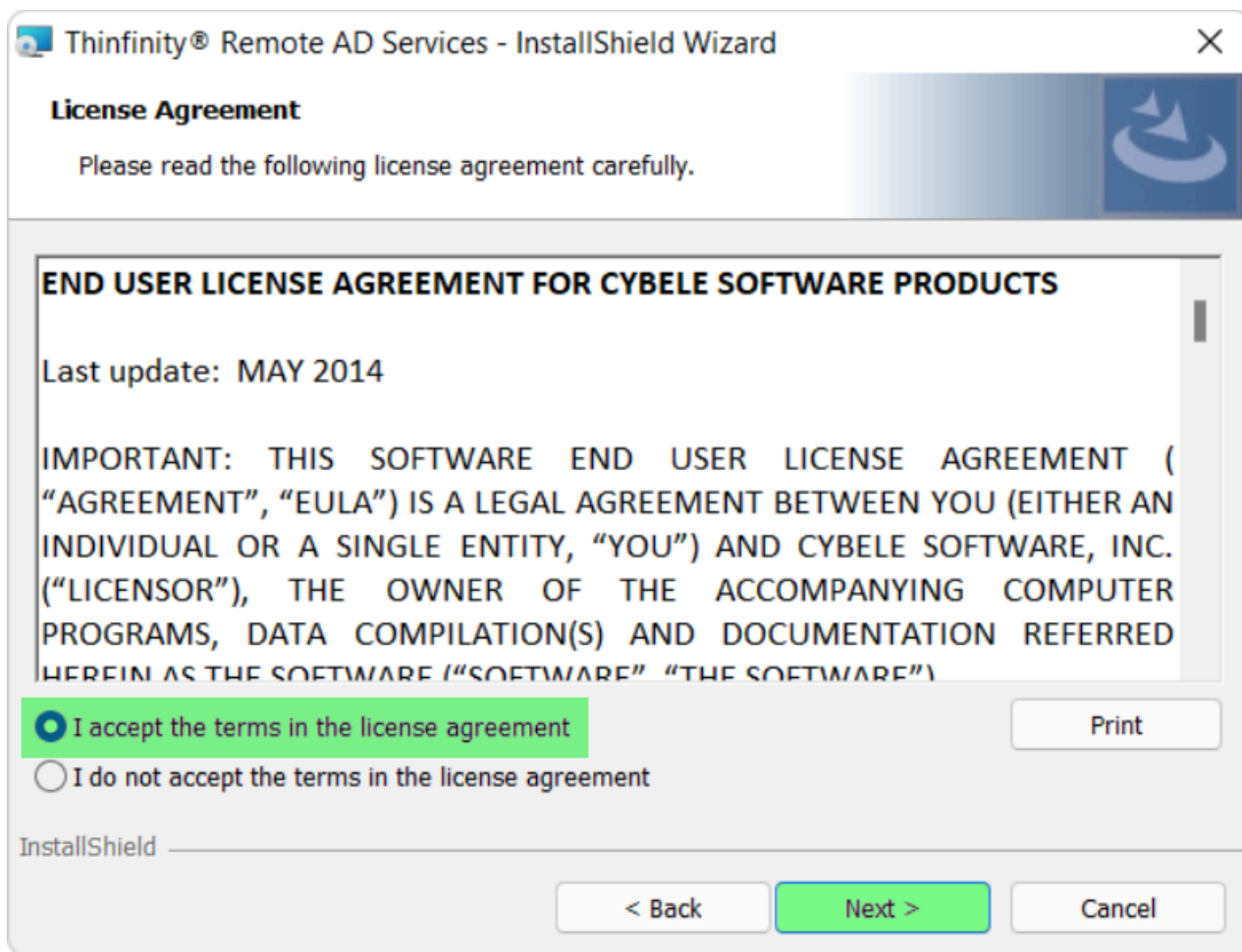
How to install and configure Thinfinity® Remote AD Services

The setup is very simple. All you need to do is install Thinfinity® Remote AD Services on a server joined to the AD you wish to integrate and point this to your Thinfinity® Remote Workspace. Follow the steps below to install it and configure both parts:

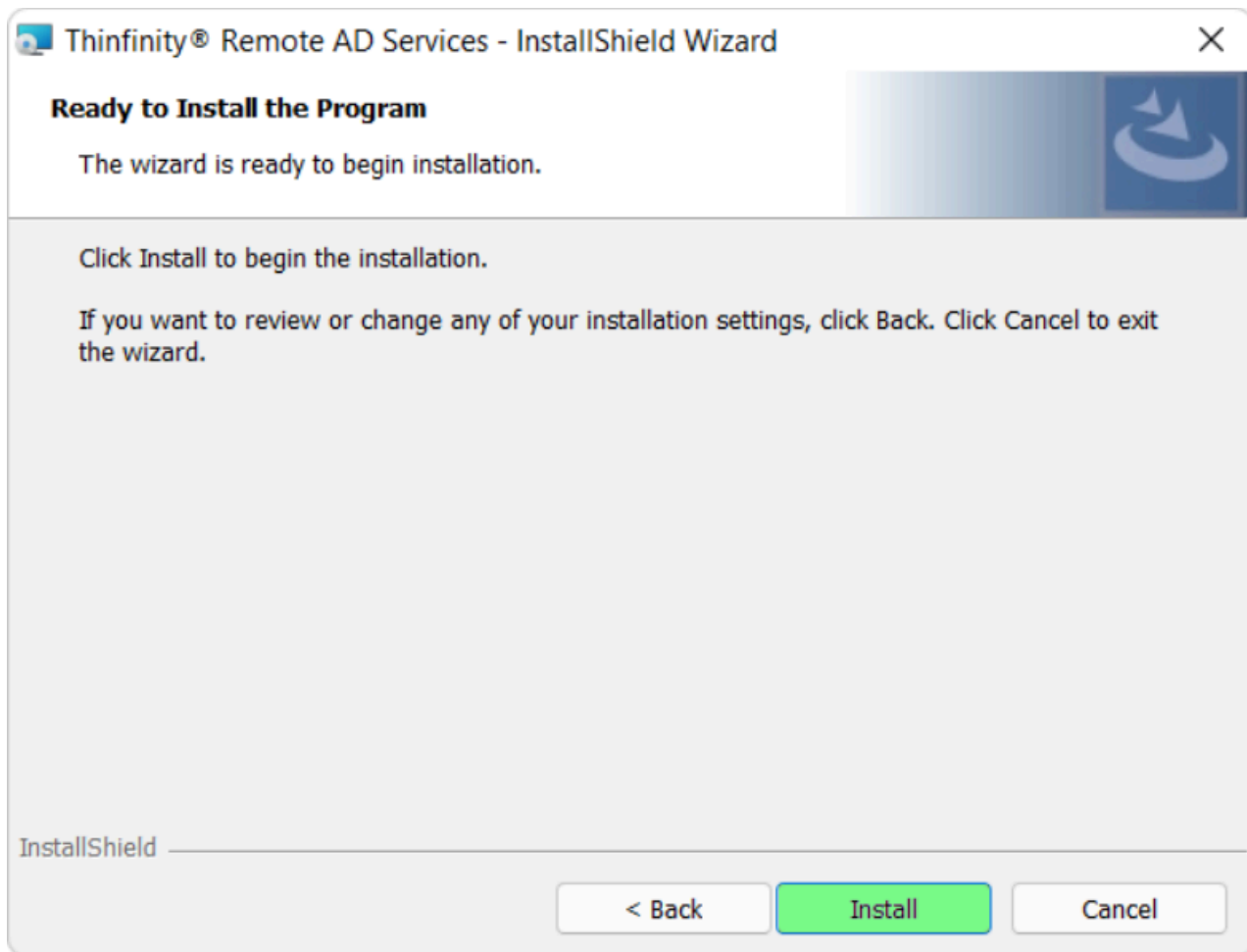
- Run the setup on the server you wish to integrate its AD with.
- On the first screen press '*Next*':



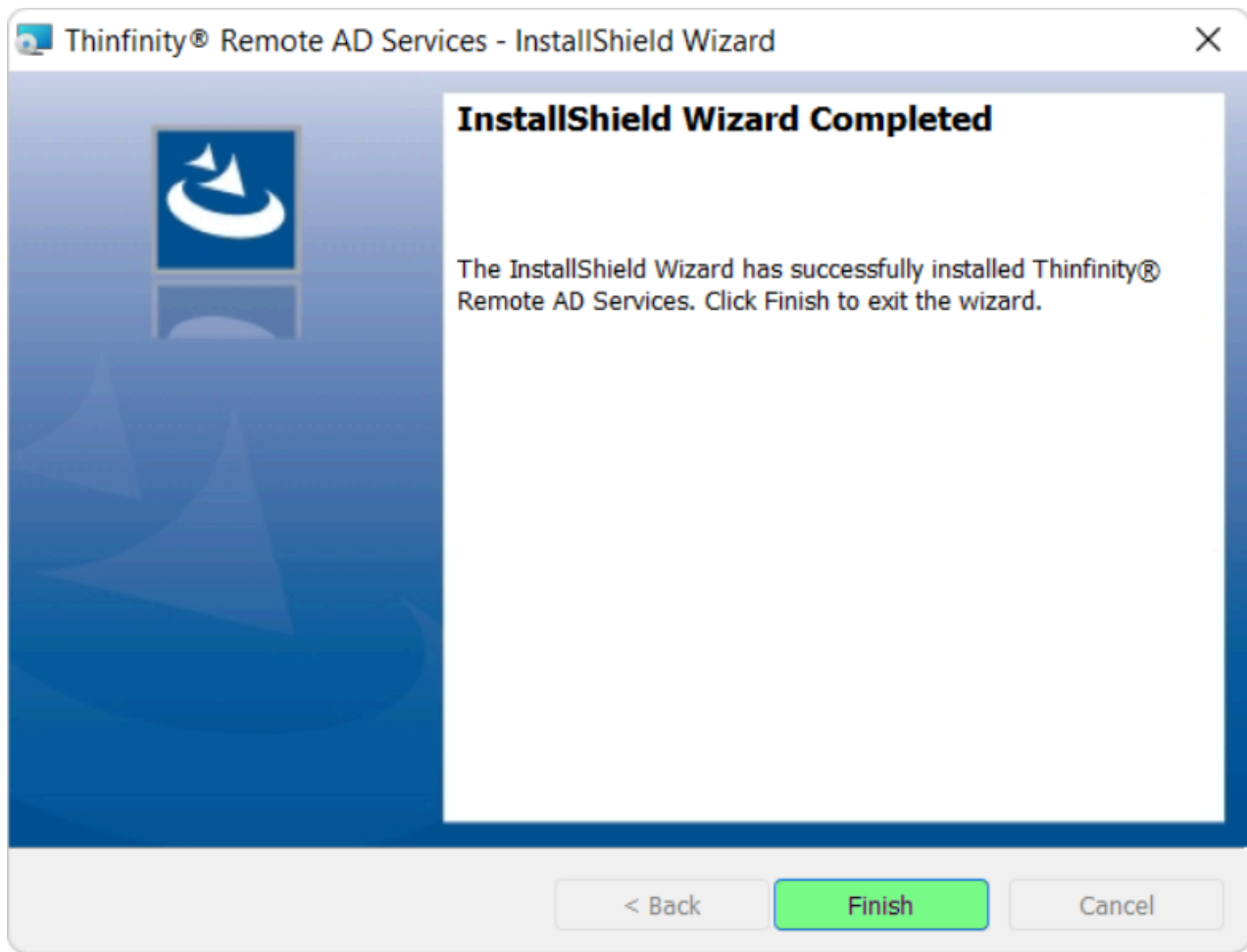
- Accept the license agreement and hit '*Next*':



- On this screen, press '*Install*':



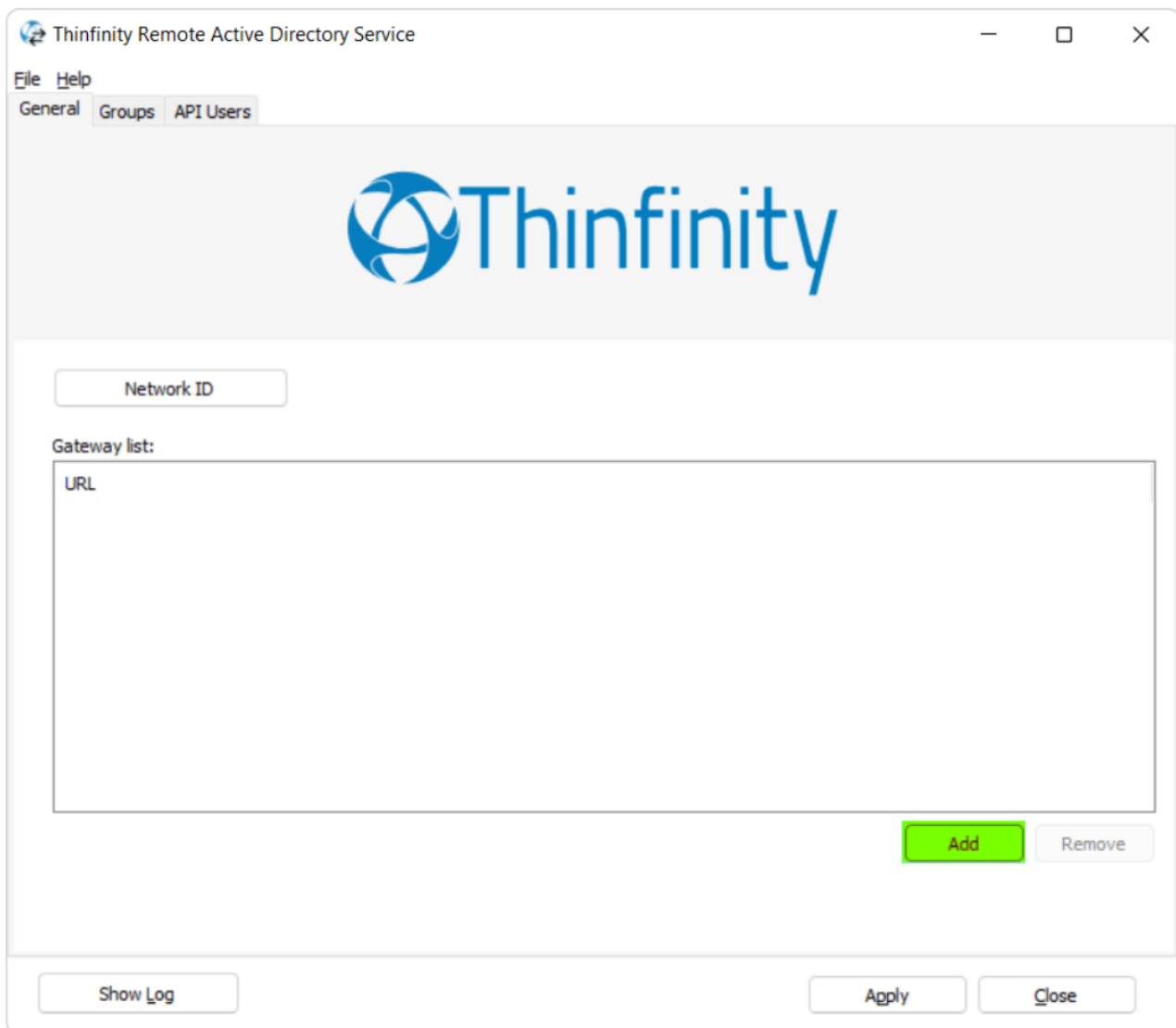
- After the installation is done, press '*Finish*':



To run the Thinfinity® Remote AD Services manager you will need to start a command line as admin, then navigate to '*C:\ProgramData\Cybele Software\Thinfinity\Workspace\DB*' and run call the exe with the argument below:

`Thinfinity.RemoteDesktop.RemoteAD.exe /manage`

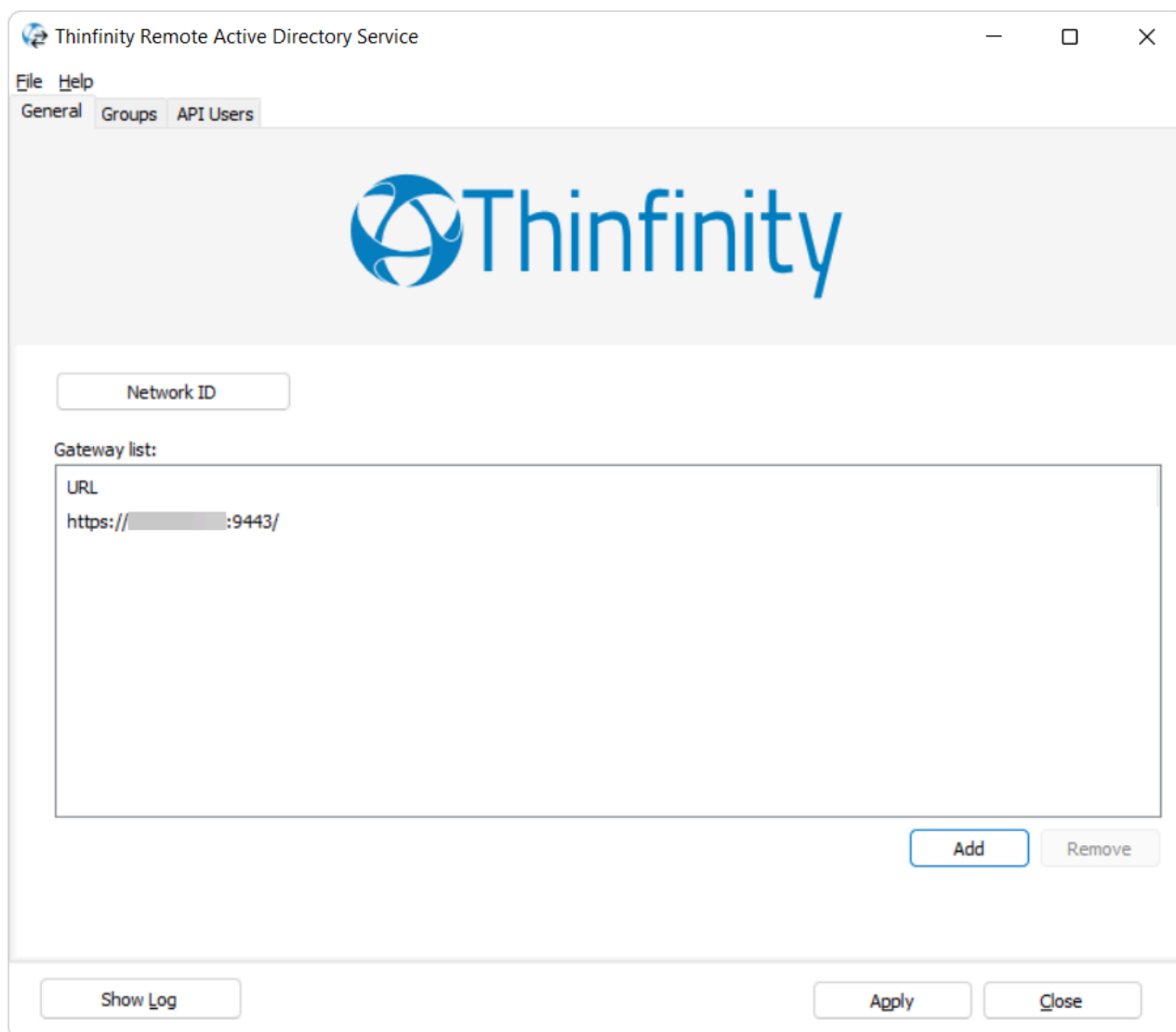
You should see the screen below:



The screenshot shows a window titled "Thinfinitiy Remote Active Directory Service". It has a menu bar with "File" and "Help". Below the menu bar are three tabs: "General", "Groups", and "API Users". The "General" tab is selected. The main area features the Thinfinity logo at the top. Below the logo is a text input field labeled "Network ID". Underneath this is a section titled "Gateway list:" followed by a large text area labeled "URL". At the bottom right of the "Gateway list:" section are two buttons: "Add" (highlighted in green) and "Remove". At the bottom of the window are three buttons: "Show Log", "Apply", and "Close".

In here, you need to configure the '*Network ID*', this must match with the Network ID you have configured in your Thinfinity® Gateway(s) and Broker(s).

Then, click on '*Add*' and enter your Gateway's public URL:



Once you finish installing Thinfinity® Remote AD Services, there are a few settings we have to update back on the Broker server.

On each one of them, you will have to enable this service by editing '*C:\ProgramData\Cybele Software\Thinfinity\Workspace\DB\settings.ini*'. In here, you will need to enable the DirectoryServices under the '*General*' tab:

```
[General]
```

```
DirectoryServices=true
```

Bear in mind that the '*General*' flag most surely exists already. Just add the '*DirectoryServices=true*' in here.

Now you must go to '*C:\ProgramData\Cybele Software\Thinfinity\Workspace\DB*' and create a JSON called '*directory.services.json*'. You will have to edit this and

add:

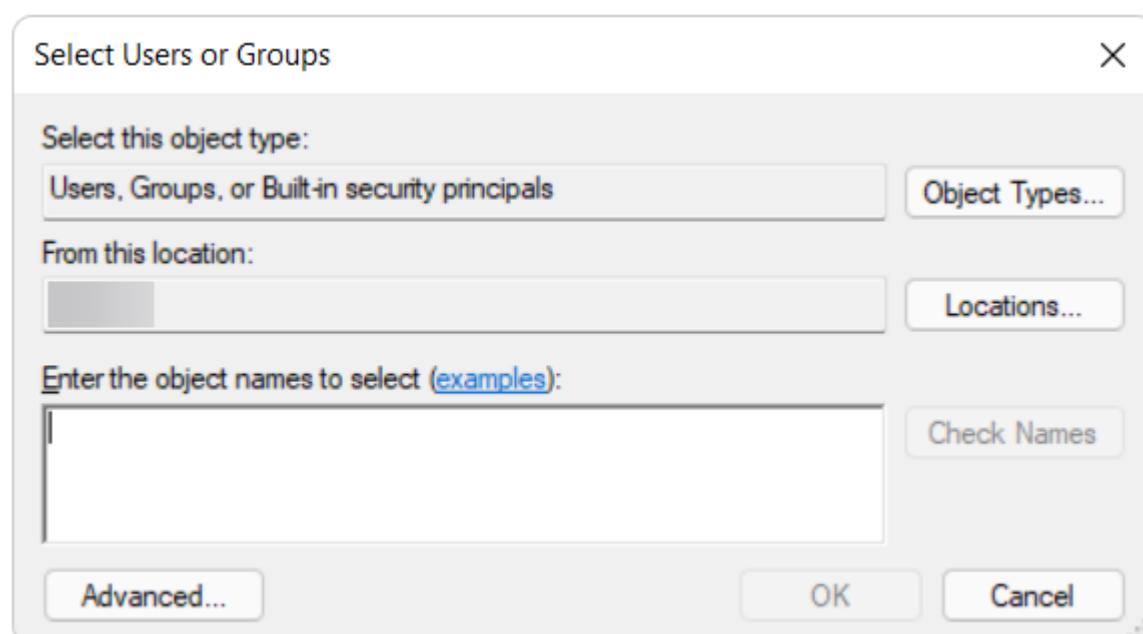
```
{
  "Services": [
    {
      "id": "cybelesoft", "name": "Cybele
AD", "filter": "cybelesoft\\\\\\.+", "url": "/__ds@cybelesoft__/dirsvc/api/v1/"
    }
  ]
}
```

Description:

ID: Reference ID to identify the AD Mapping

Name: A descriptive name to identify the mapping in Thinfinity® Remote Workspace.

Filter: You must enter the domain name as the user would type it in. You can add a wild card expression as above (.+) so it will map any username under this domain. Keep in mind, you will have to add 4 backslashes "\\\\\\\\" after the domain name.



URL (registration parameter): You have to enter the domain name URL under the following format "__ds@[domain]__".

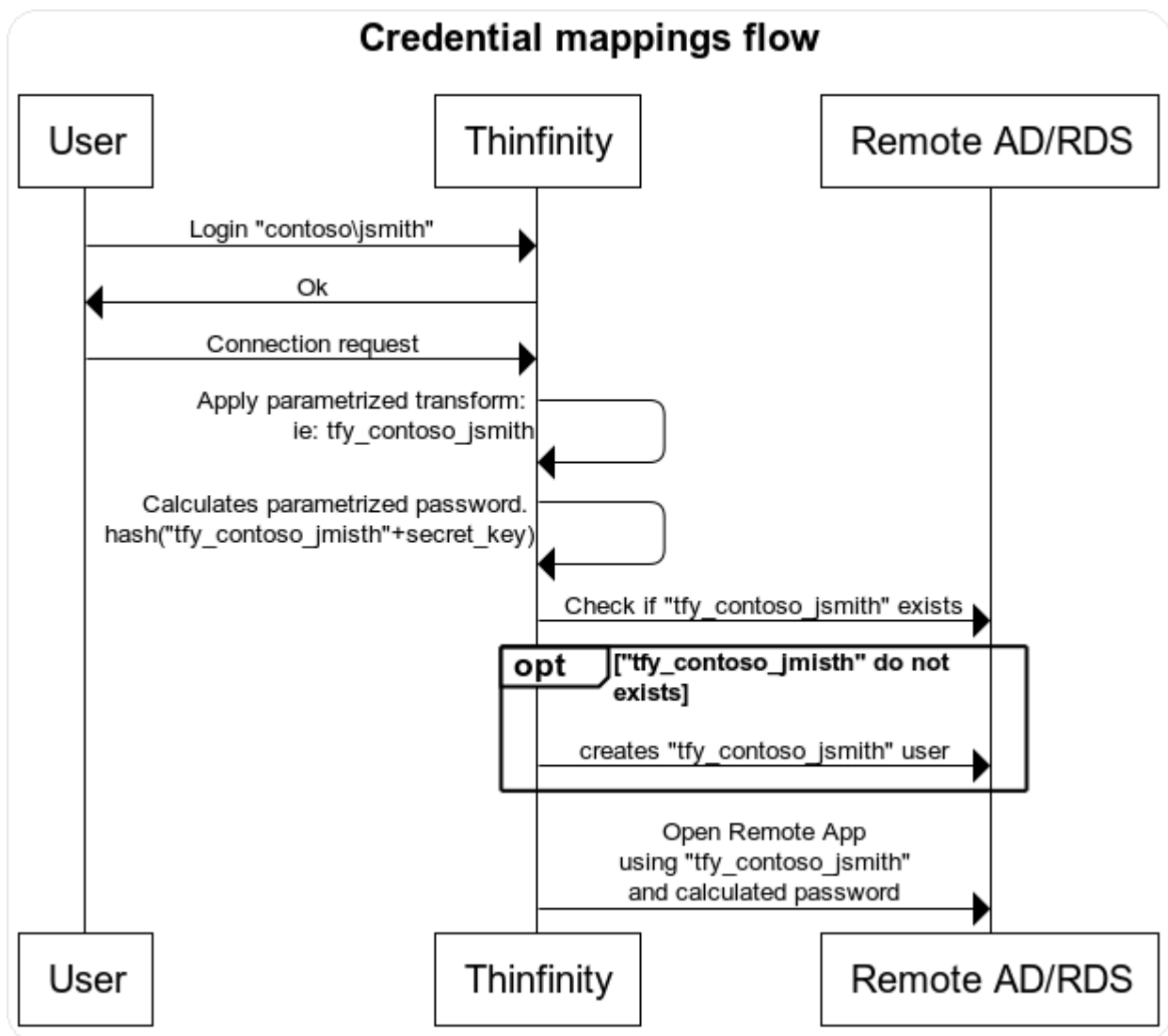
Keep in mind that you will have to create a separate mapping (ID) for each Remote AD you wish to join to Thinfinity® Remote Workspace, separated by a comma (,).

Active Directory credentials mapping

End-users will use their local Active Directory credentials in order to login into Thinfinity® Remote Workspace. When the end-user requires access to the remote application, an RDS session will be created using mapped credentials belonging to the remote Active Directory.

Thinfinity® Remote Workspace will provide an automatic, parameterized procedure to create and map credentials, avoiding the need to do this manually:

- Every time the connection is required, Thinfinity® Remote Workspace will check if the mapped remote credentials exist; If they do not, new credentials will be created on the remote Active Directory and associated with the local UserID
- New credentials will be created based on a parametrized formula, calculating the associated UserID and a secure predictable password
- Mapped credentials are calculated every time, and therefore there is no need to restart any services in order for changes to apply



WebBridge - Direct File Transfer

With Thinfinity® Remote Workspace we introduced an enhanced method for file transfer. Features like Drag and Drop makes the entire process extremely easy and convenient. We simplified the way users interact with their local and remote files, providing the necessary tools for your user's day to day activities.

To take advantage of all the features, the admin will need to install an executable component called Thinfinity® WebBridge.


WebBridge will enable the ability to Drag and Drop files straight from the browser. This component will also create a temporary Virtual Disk called "ThinDisk" that the users can alternatively use as the main directory to safely and easily transfer files to and from the remote machine.

- [How to install Thinfinity® WebBridge](#)
- [WebBridge: User Experience](#)

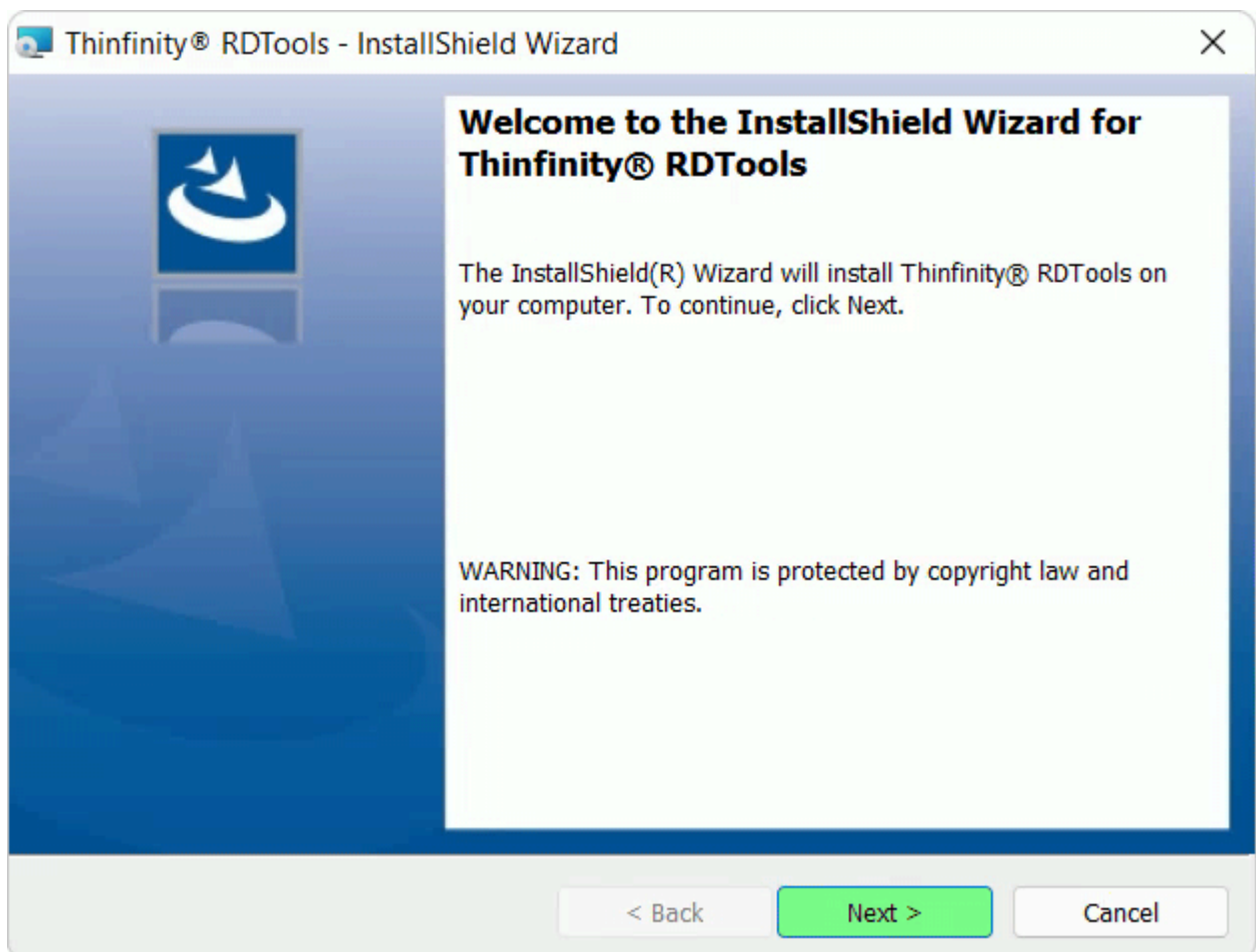
How to install Thinfinity® WebBridge

You'll find the steps to install Thinfinity® WebBridge below:

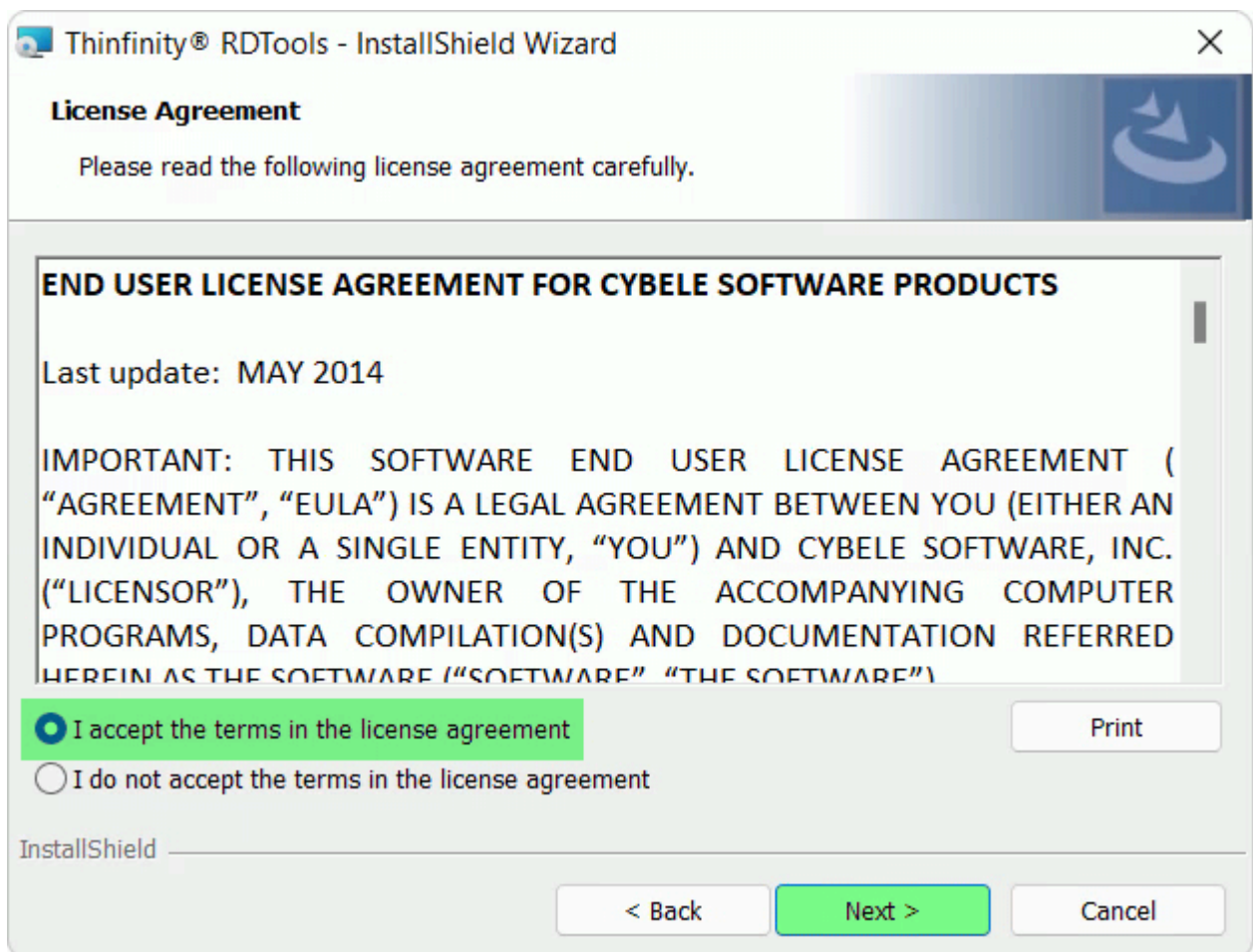
- First-off, download Thinfinity® WebBridge on the server and run the setup '*Thinfinity_RDTools_v6.0_Setup_x64.exe*'.

 Bear in mind, Thinfinity® WebBridge has to be installed on the Remote Desktop machine you wish to upload/download files to/from. The client computer does not require to install any plug-in or add-on.

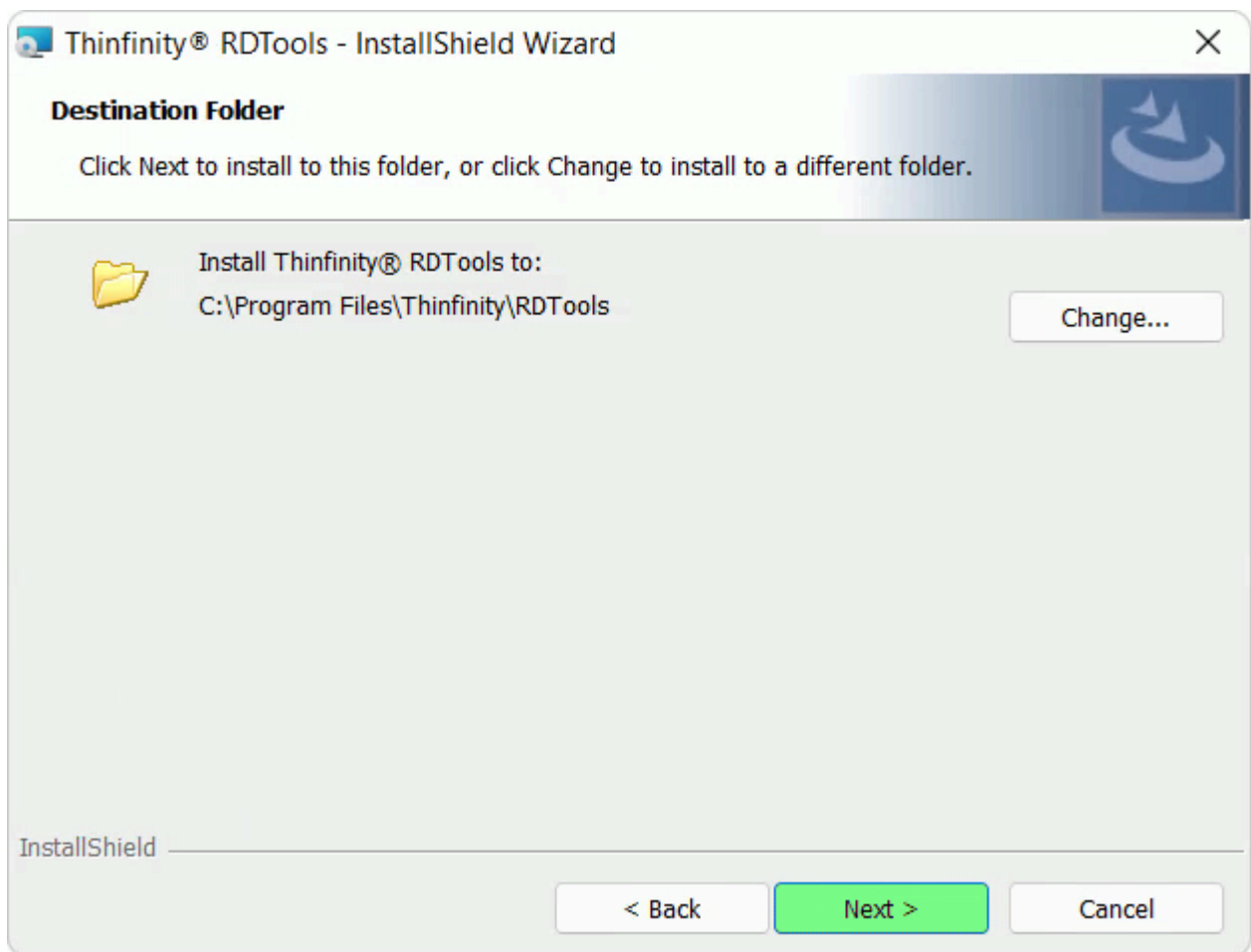
- In the first screen, press '*Next*':



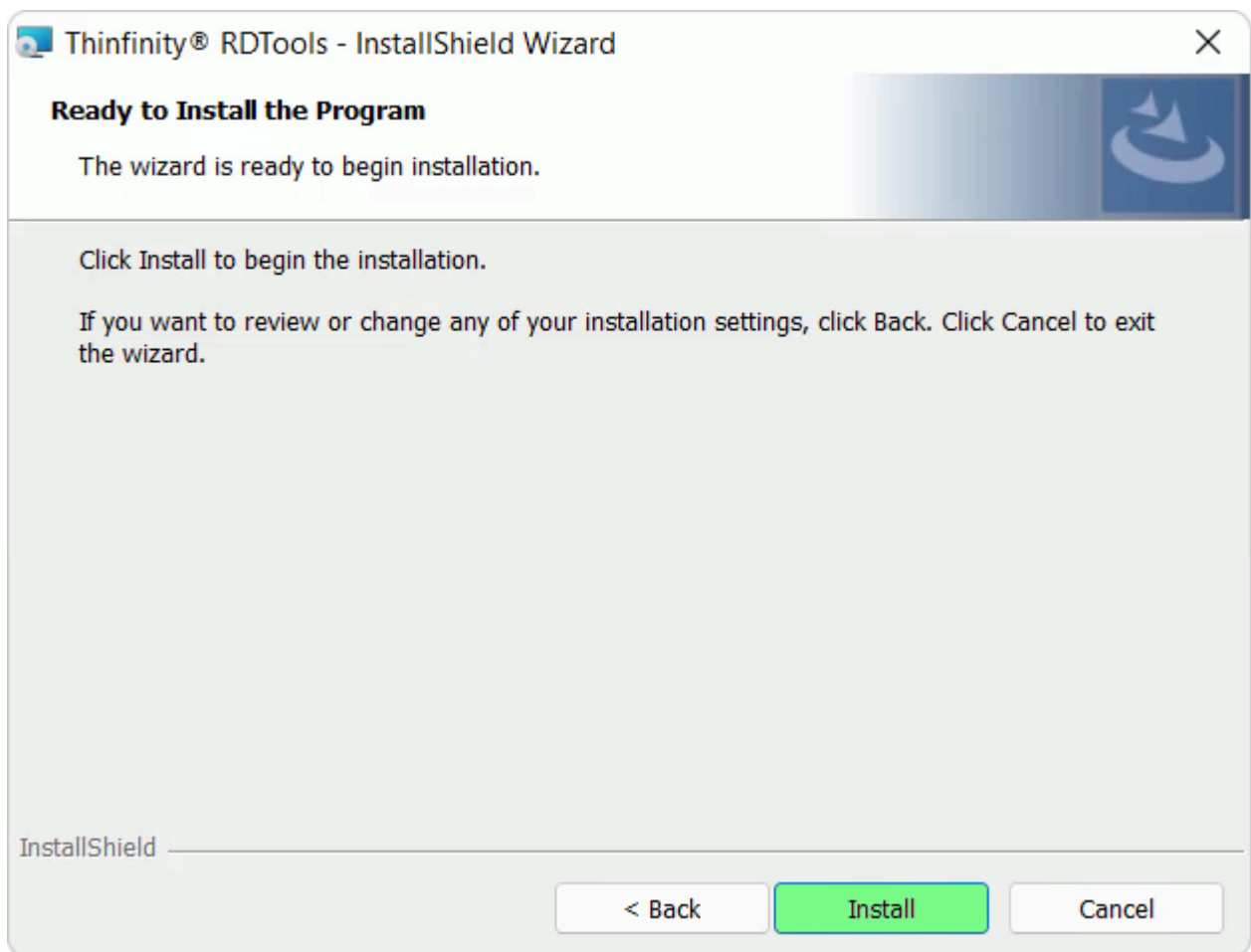
- Accept the License Agreement and press '*Next*':



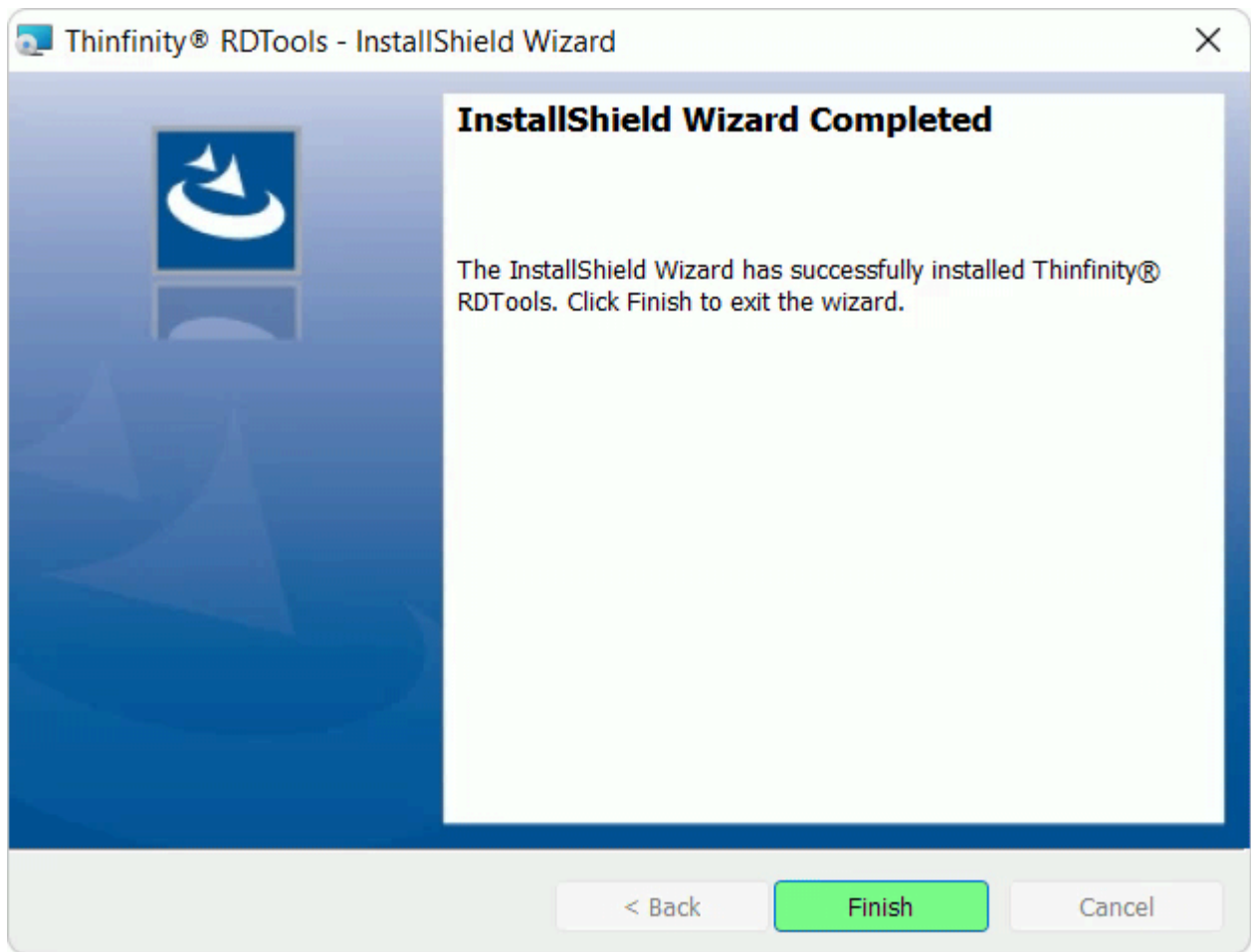
- Select the Destination Folder and press 'Next':



- Click '*Install*':



- After the installation completes, press '*Finish*':



Now you should be ready to connect to this server and use the WebBridge drive. To find more details on how to use WebBridge, please navigate to the next section "User Experience".

WebBridge: User Experience

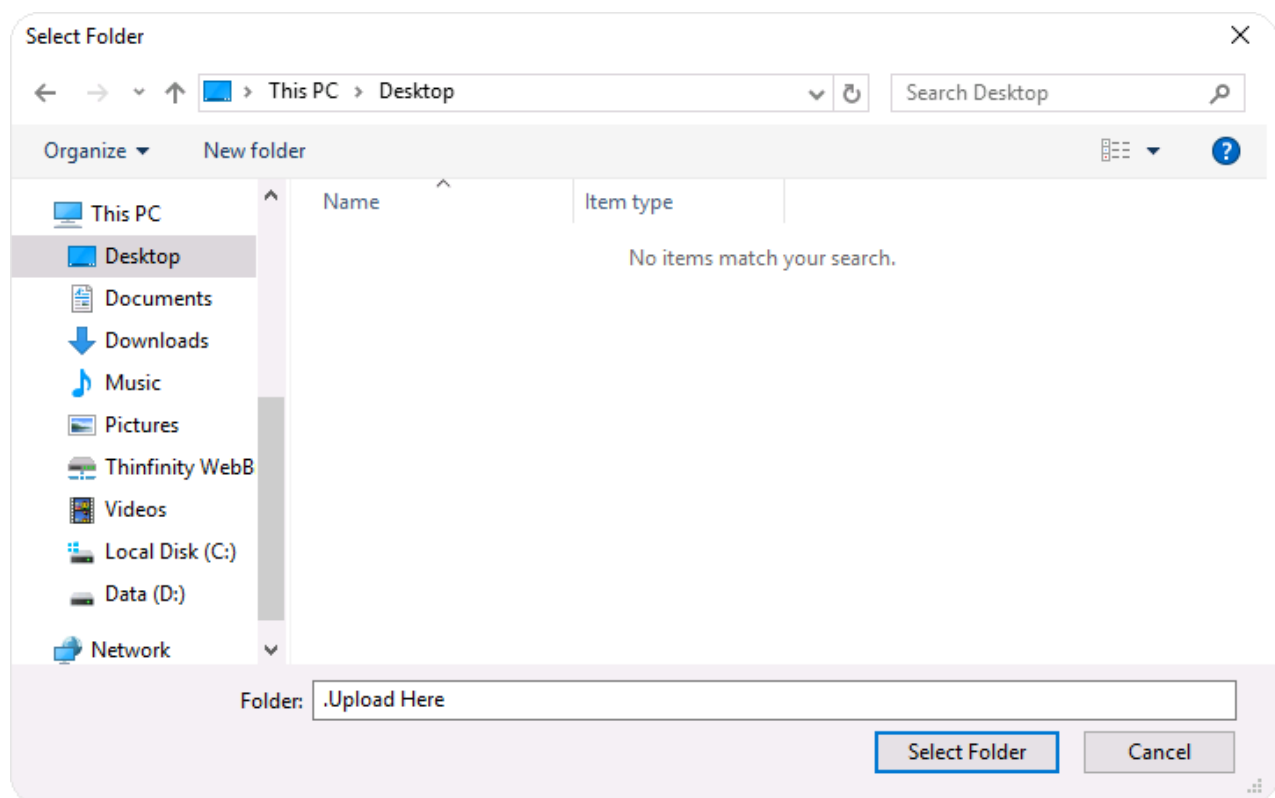
Transferring files from your local PC to your remote desktop session has never been easier.

How to upload files:

There are 2 different ways you can upload a file to your remote desktop session:

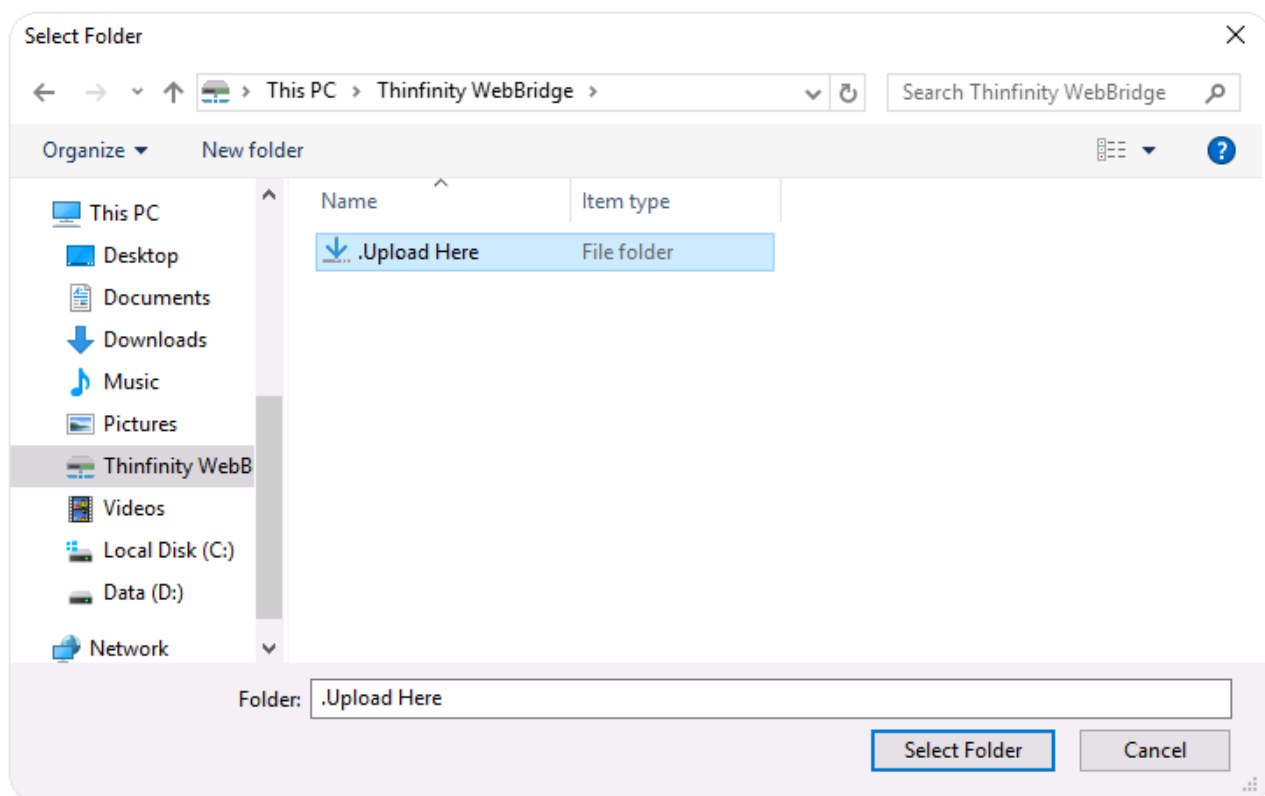
- You can drag and drop files directly into the browser where the remote desktop session is running.

After you drag a file into the browser, you will be prompted to save the file:



Here you can select any folder you have permissions to in the remote desktop.

- Go to the "Thinfinity® WebBridge" drive and double click "Upload Here":

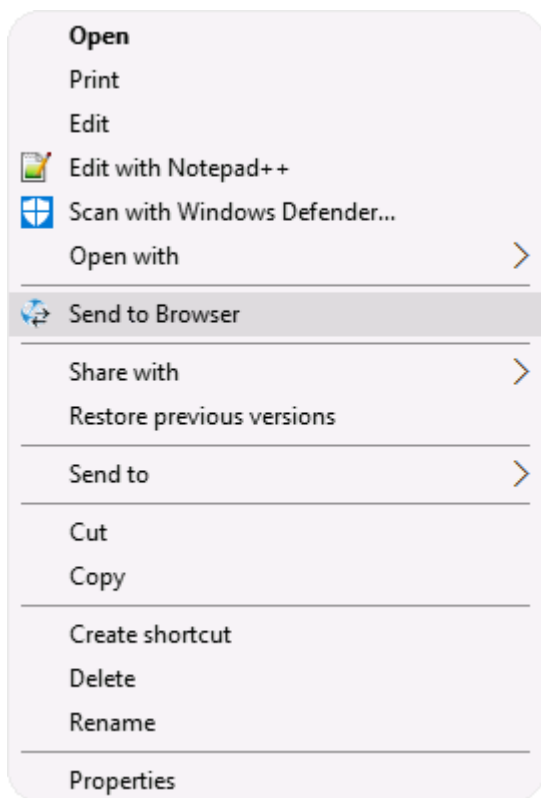


This will open your local "File Open" dialog, where you can select a file and upload to the "Thinfinity® WebBridge" drive.

How to Download files:

To download files, there are also 2 different methods:

- You can drag and drop files into the "Thinfinity® WebBridge" drive. This will save the file in the WebBridge drive and will automatically download from your browser.
- Right click any file in the remote desktop session, and select "Send to Browser" to automatically download:



- ⓘ If you are working on a file that is stored in the "Thinfinity® WebBridge" drive and you update it, WebBridge will detect these changes and download the file again so you don't lose any of your information.

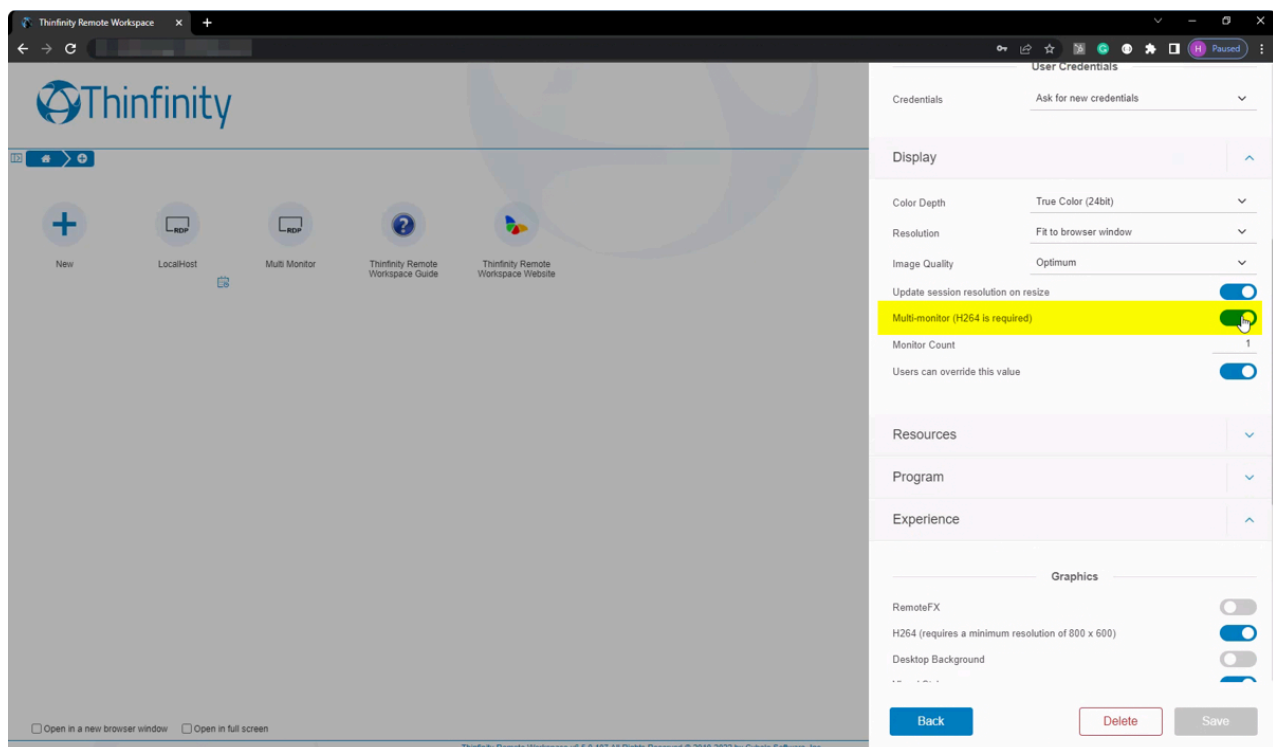
Multi-Monitor

The Multi-monitor feature must support a seamless transition between home and workplace environments by providing users with a **remote access solution that replicates the setup they usually run at the office**. Users can access business-critical resources from any location, and they can work with the same display configuration they are already familiar with.

How to enable Multi-Monitor

One of the requirements to be able to use Multi-Monitor, is having H264 enabled. To find how to do so, please visit ["How to Enable H264 on your Acces Profile"](#)

Once H264 is enabled, activating Multi-Monitor is very simple. If you are in the Web Manager, edit any of your RDP connections and in the Display options, enable the option "Multi monitor" as shown below:



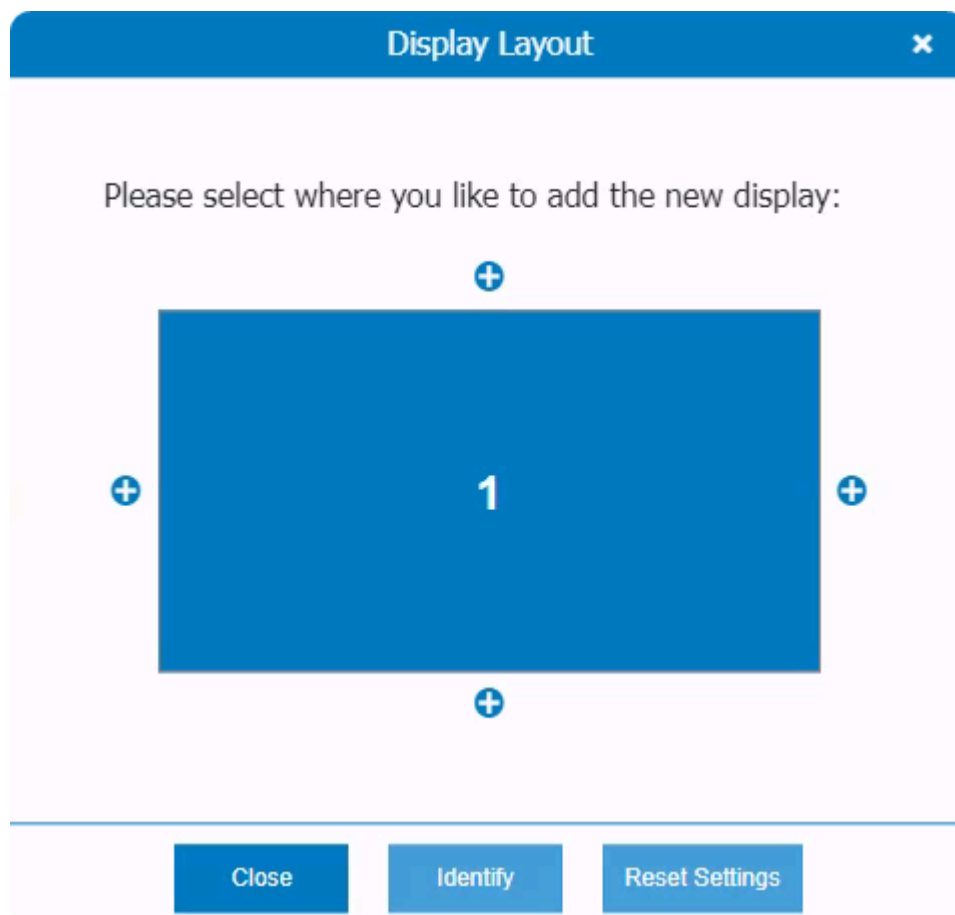
From here you will also be to select in advance how many display you wish to start when connecting, from the option "Monitor Count".

User Interfac

After connecting to profile with Multi-Monitor enabled, you will be able to spawn new monitors from the menu bar at the top-middle of the screen:



Here you will be able to pull up the display layout and choose to which sides you wish to extend the display:



Redirecting Devices

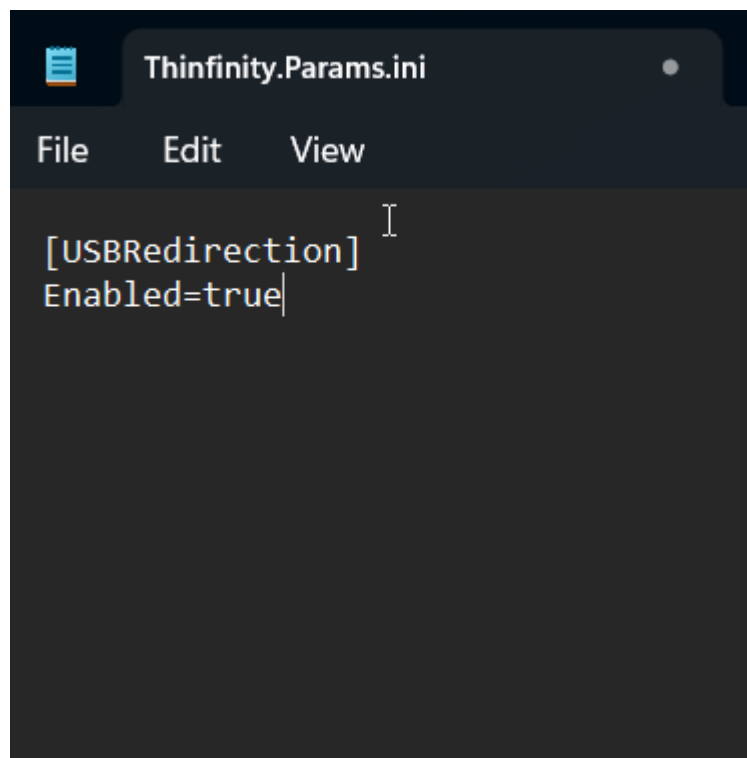
USB Redirection

USB redirection is a technology that allows you to plug an external device into a USB port on the endpoint and access the device from within a remote desktop or application.

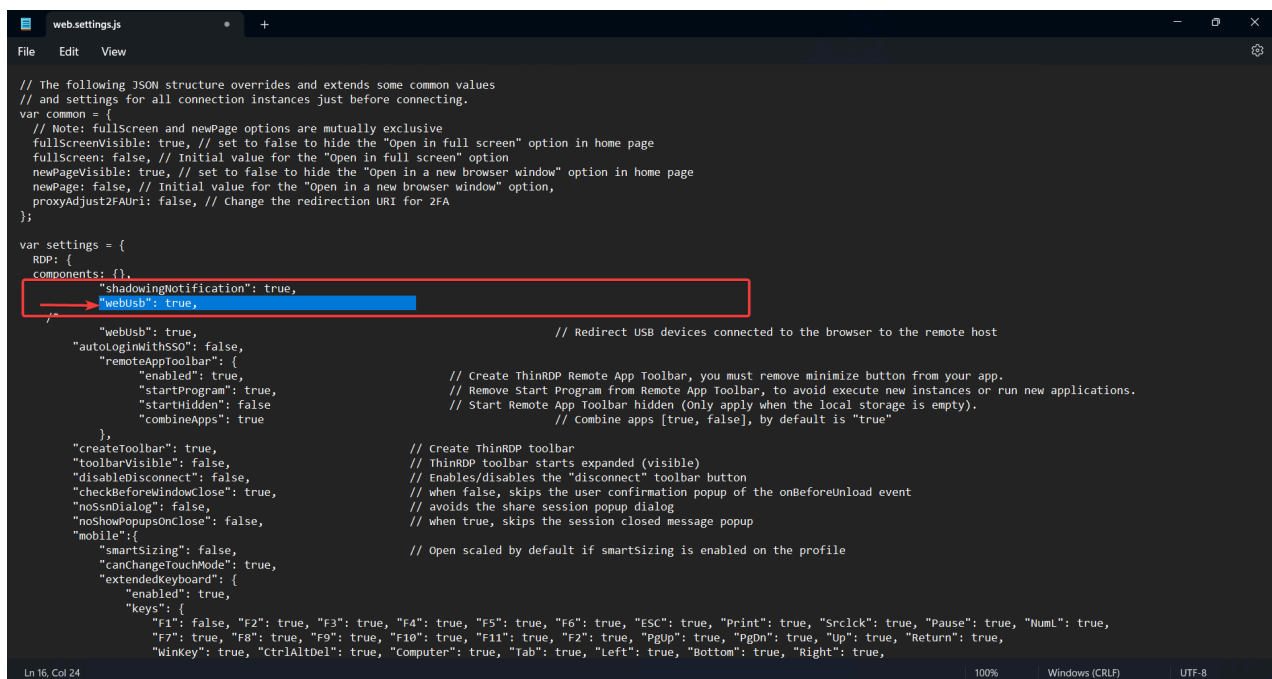
In order to have your USB Pendrive/Key redirected to your **Thinfinity Workspace** profiles connections you need to follow these steps:

- 1 - Navigate to the following path> **C:\Program Files\Thinfinity\Workspace\bin64**
- 2 - Create a file called> "**Thinfinity.Params.ini**"
- 3 - Edit **Thinfinity.Params.ini** as it showed in the following picture and save it.

[USBRedirection]Enabled=true



- 4 - Navigate to the following path> **C:\Program Files\Thinfinity\Workspace** and edit the file called **web.settings.js**



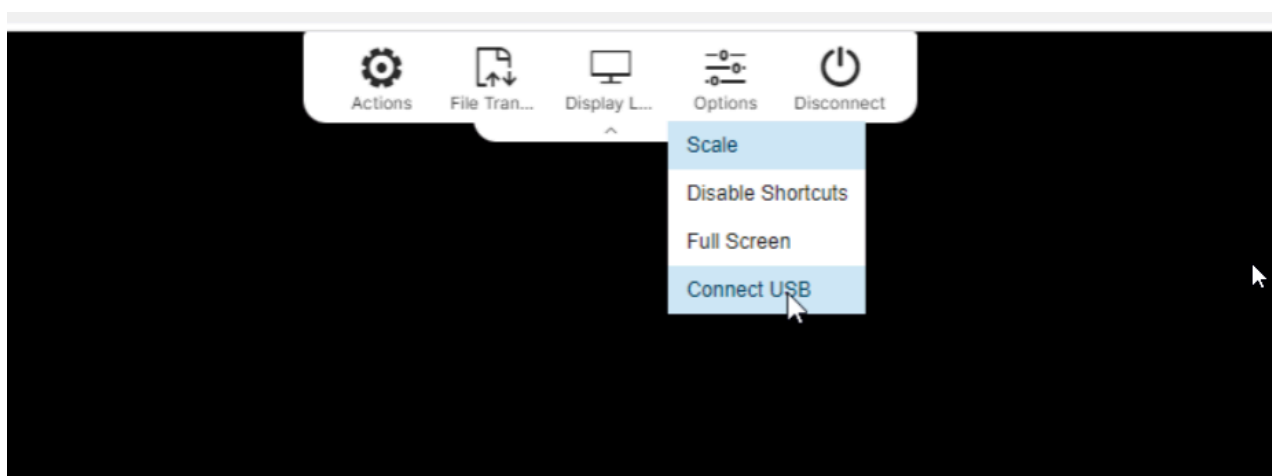
```

// The following JSON structure overrides and extends some common values
// and settings for all connection instances just before connecting.
var common = {
  // Note: fullscreen and newPage options are mutually exclusive
  fullscreenVisible: true, // set to false to hide the "Open in full screen" option in home page
  fullscreen: false, // Initial value for the "Open in full screen" option
  newPageVisible: true, // set to false to hide the "Open in a new browser window" option in home page
  newPage: false, // Initial value for the "Open in a new browser window" option,
  proxyAdjust2FAUri: false, // Change the redirection URI for 2FA
};

var settings = {
  RDP: {
    components: {},
    "shadowingNotification": true,
    "webusb": true,
    "webusb": true, // Redirect USB devices connected to the browser to the remote host
    "autoLoginWithSSO": false,
    "remoteAppToolBar": {
      "enabled": true, // Create ThinRDP Remote App Toolbar, you must remove minimize button from your app.
      "startProgram": true, // Remove Start Program from Remote App Toolbar, to avoid execute new instances or run new applications.
      "startHidden": false, // Start Remote App Toolbar hidden (Only apply when the local storage is empty).
      "combineApps": true // Combine apps [true, false], by default is "true"
    },
    "createToolBar": true, // Create ThinRDP toolbar
    "toolbarVisible": false, // ThinRDP toolbar starts expanded (visible)
    "disableDisconnect": false, // Enables/disables the "disconnect" toolbar button
    "checkBeforeWindowClose": true, // when false, skips the user confirmation popup of the onBeforeUnload event
    "noSsdDialog": false, // avoids the share session popup dialog
    "noShowPopupsOnClose": false, // when true, skips the session closed message popup
    "mobile": {
      "smartSizing": false, // Open scaled by default if smartSizing is enabled on the profile
      "canChangeTouchMode": true,
      "extendedKeyboard": {
        "enabled": true,
        "keys": {
          "F1": false, "F2": true, "F3": true, "F4": true, "F5": true, "F6": true, "ESC": true, "Print": true, "SrcIck": true, "Pause": true, "NumL": true,
          "F7": true, "F8": true, "F9": true, "F10": true, "F11": true, "F12": true, "PgUp": true, "PgDn": true, "Up": true, "Return": true,
          "WinKey": true, "CtrlAltDel": true, "Computer": true, "Tab": true, "Left": true, "Bottom": true, "Right": true,
        }
      }
    }
  }
}

```

You need to add the line> "webUsb": true as it shown in the picture above 5 - Open your Thinfinity Workspace connection from the browser and connect the USB from Thinfinity Tool Box.



You should get the following window in your browser:

qatestcybele.ddns.net wants to connect

USB Receiver

Unknown device from Chicony Electronics Co., Ltd

Logitech USB Headset

Unknown device from Elan Microelectronics Corp.

USB 10/100/1000 LAN

USB Keyboard

Unknown device from Intel Corp.



Connect

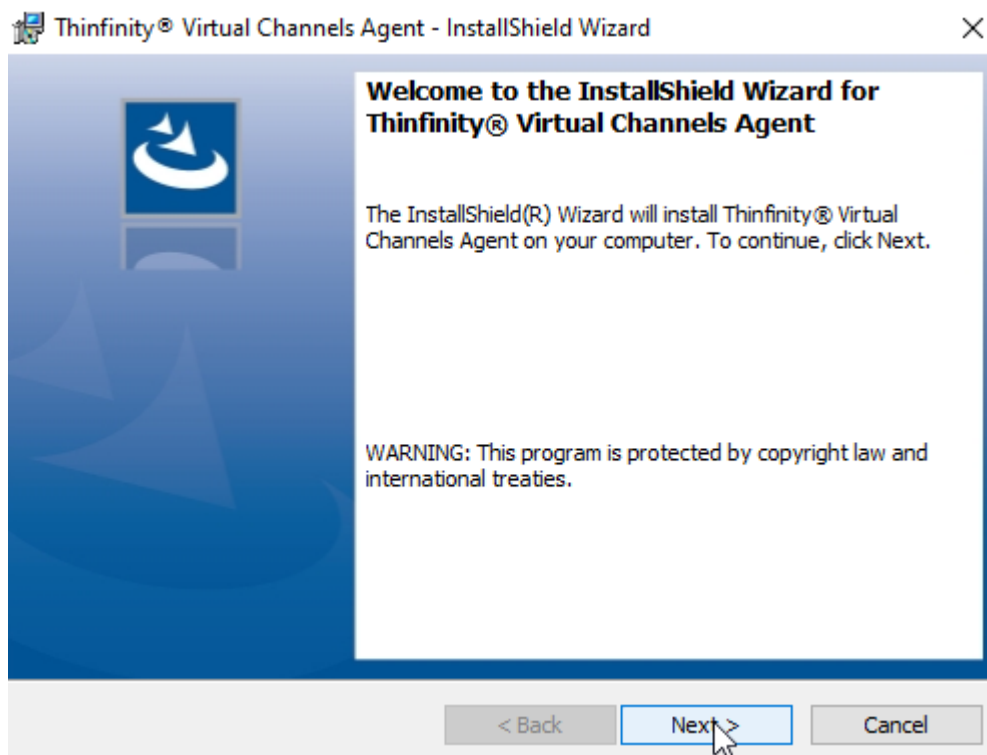
Cancel

Printer & Scanner Redirection

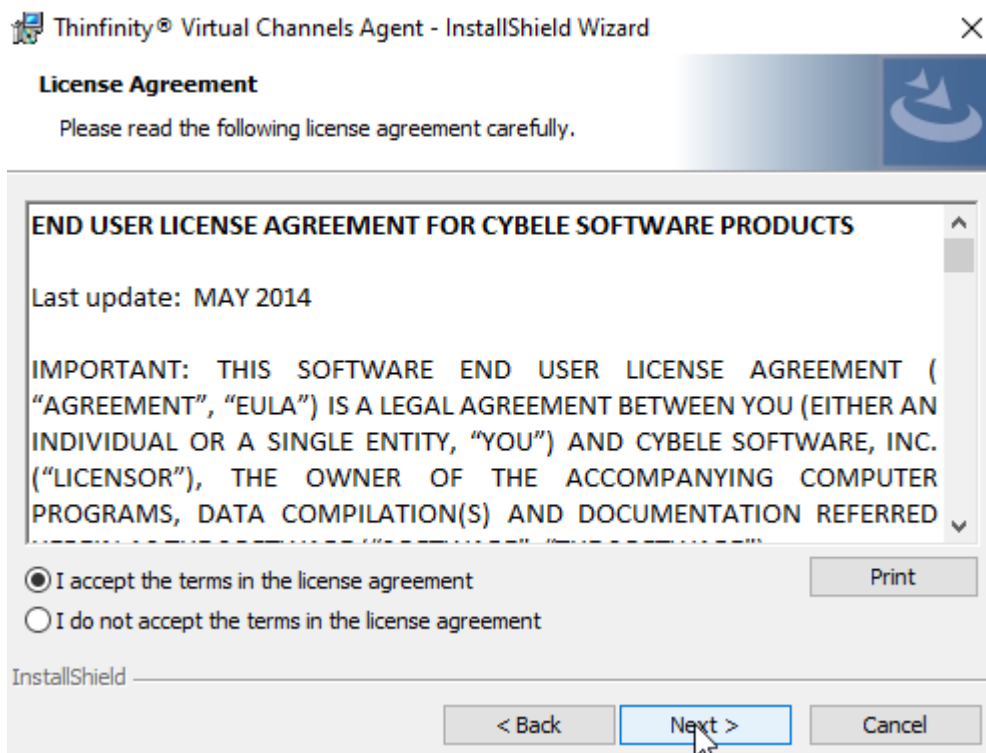
How to install and use the Thinfinity Remote Printer Agent

Once you have downloaded the file, execute the setup and follow these steps:

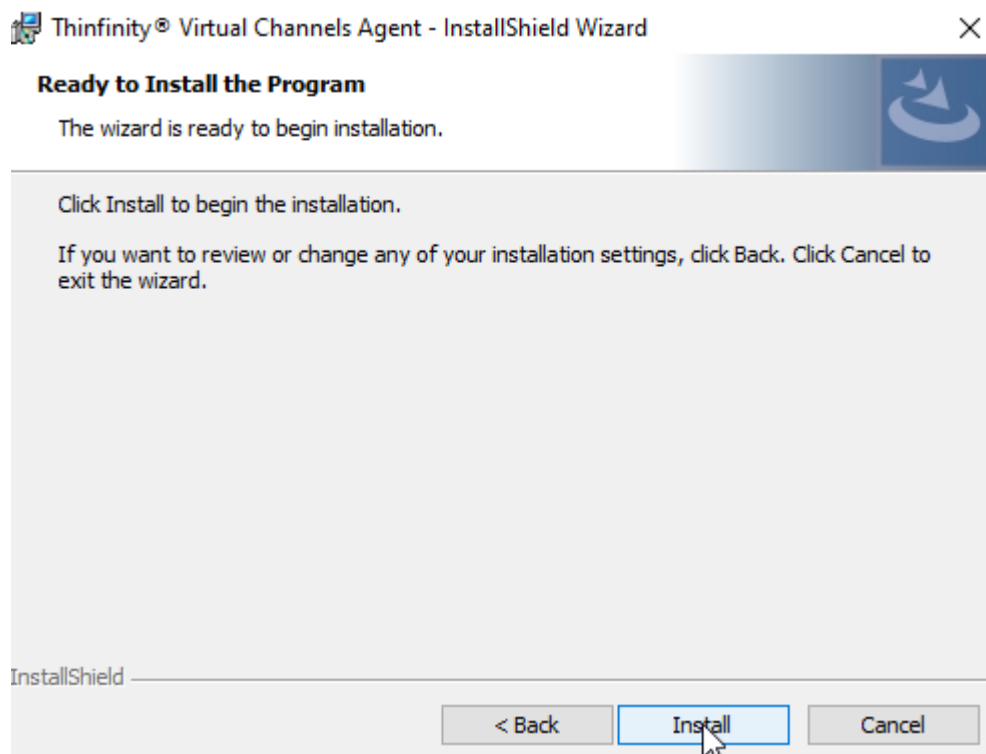
In the 'Welcome' screen, press 'Next':



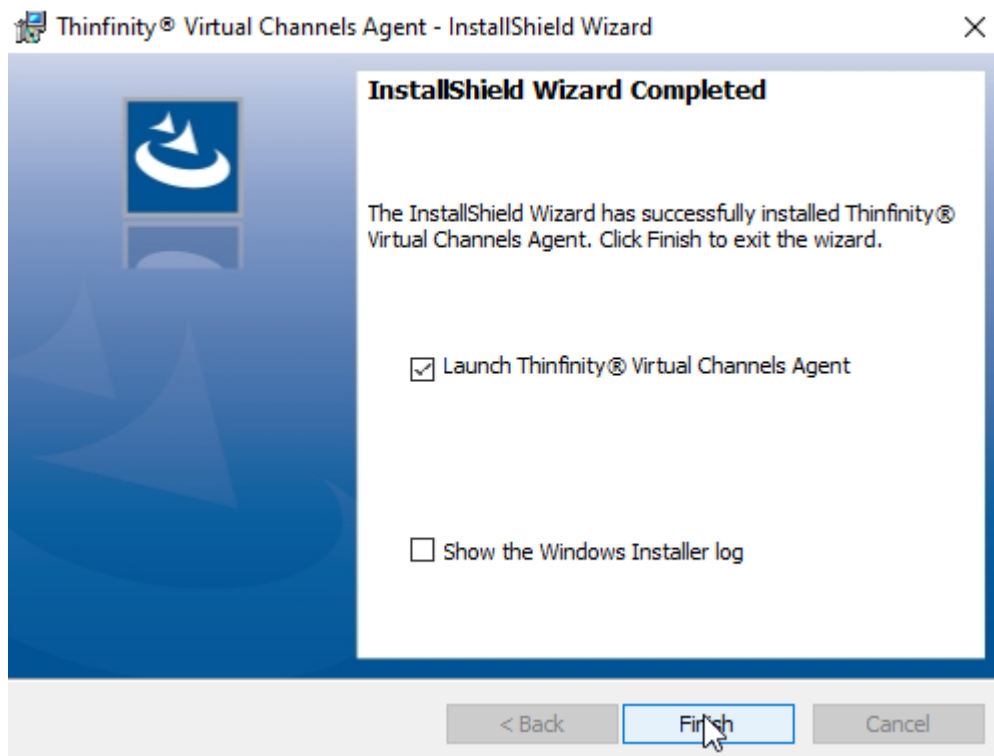
Check 'I accept the terms in the license agreement' and press 'Next':



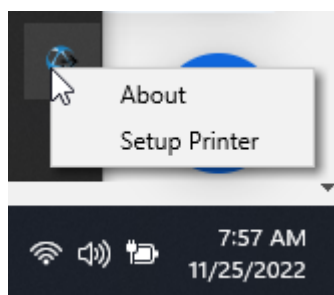
Click 'Install':



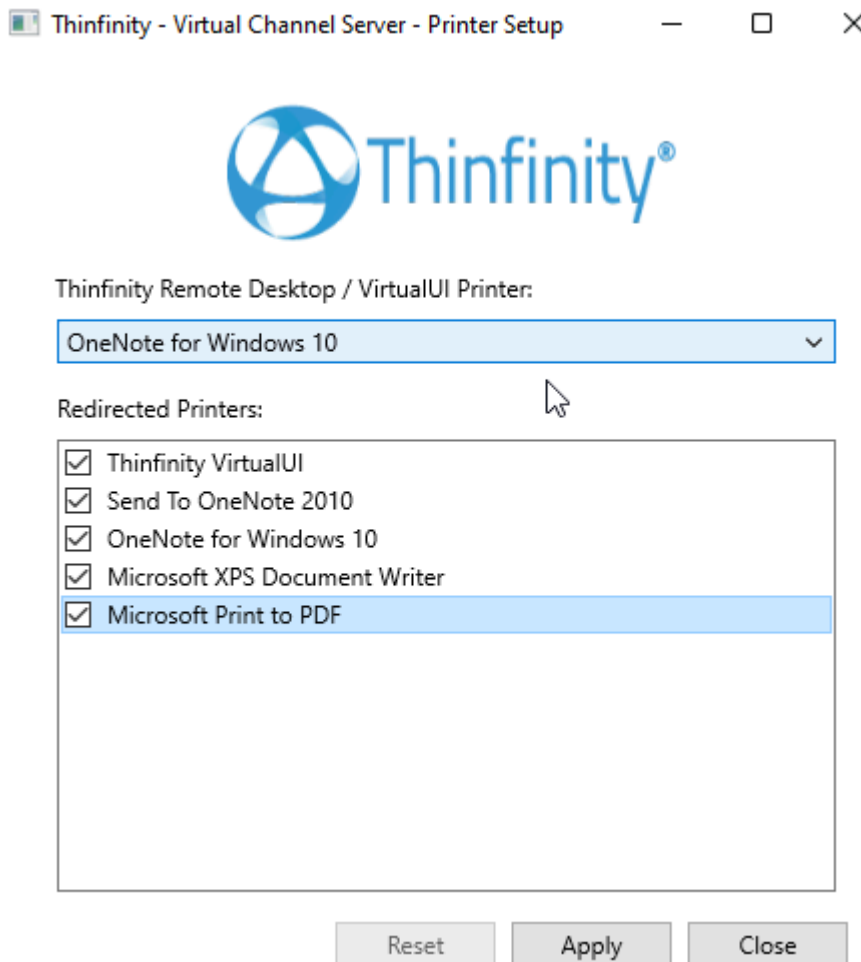
Check the box 'Launch Thinfinity® Virtual Channels Agent' and click 'Finish':



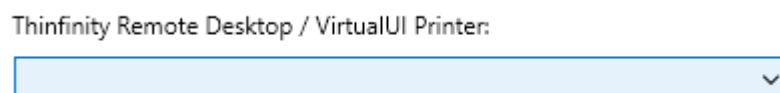
Now that we have finished installing the agent, you should be able to see a small icon for it in your system tray. You can right-click it and select 'Setup Printer' to configure your printer(s):



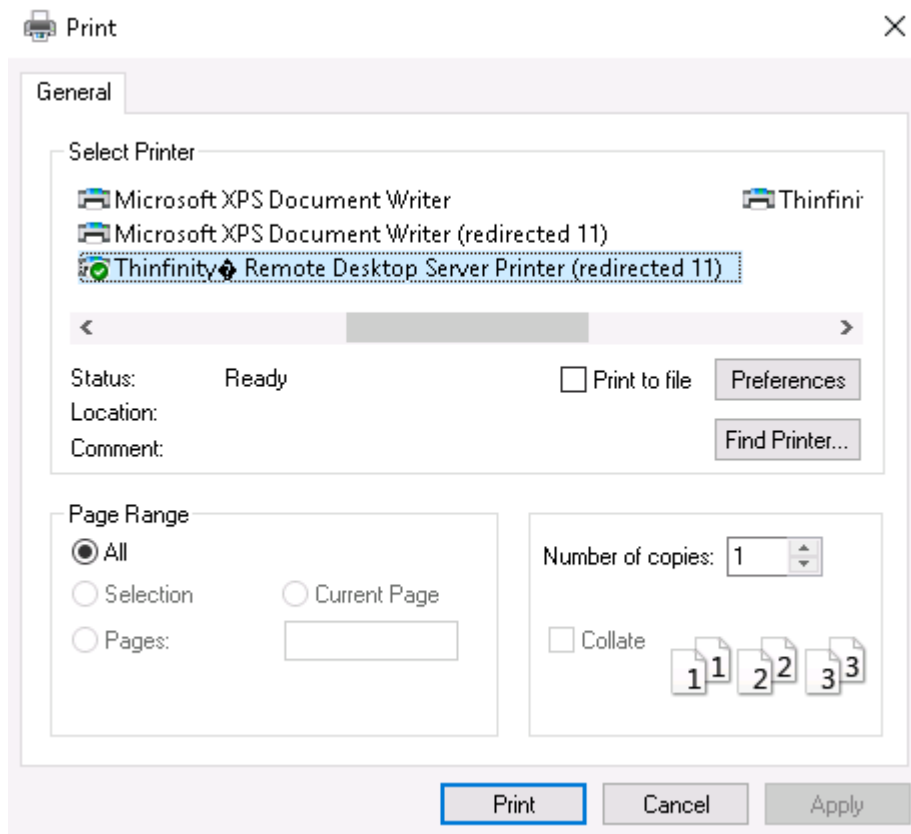
The agent should look similar to this:



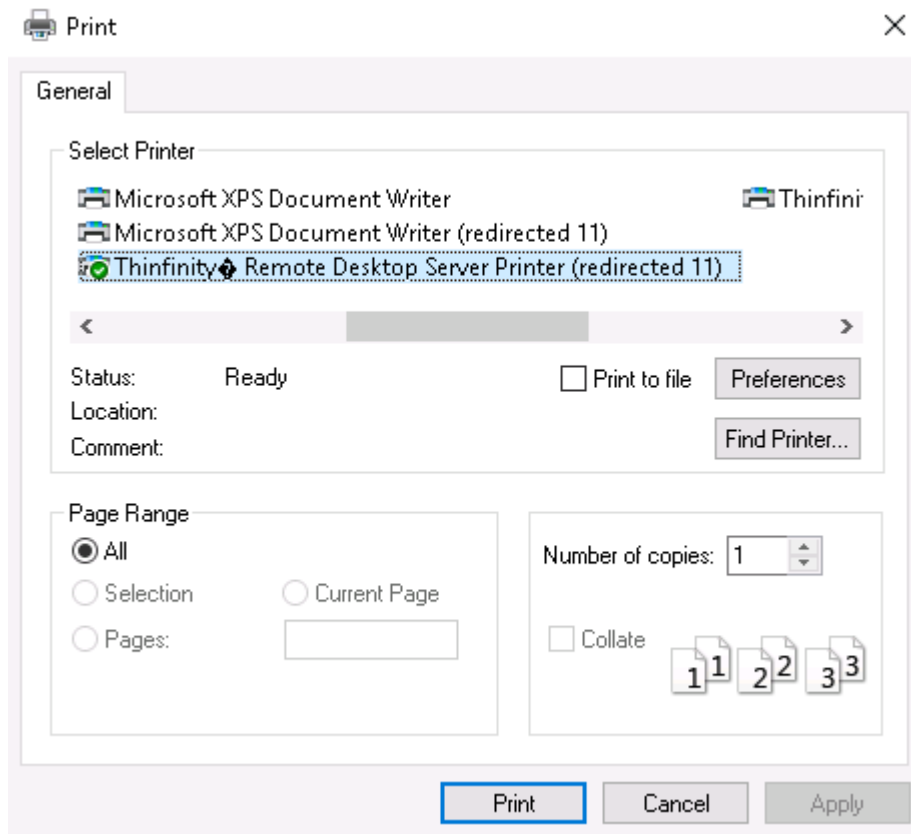
You can see there are 2 different sections in the agent. There is a combobox to choose a printer and a list with checkboxes that will show all your available printers. In the combobox you will select the default printer you want the "Thinfinity® Remote Desktop Printer / Thinfinity® VirtualUI Printer" to send the job to. If you leave this combobox blank, like below:



It will send the job to the normal remote printer, which will create a PDF file and print to the browser. The redirected printers box will let you select which other printers you wish to have available on the 'remote desktop/application'. Below is a practical example to understand this better:



In the screenshot above, you can see a few printers that say 'redirected' on its name. These printers are the ones I have 'checked' in the 'Redirected Printers' box. If I send the print job to 'Thinfinity® Remote Desktop Server Printer' (or Thinfinity® VirtualUI Printer) as in the screenshot below, the job will go to my local 'Microsoft Print to PDF' (the printer I chose in the combo box):



But I will still be able to choose a different local printer if I wish (the ones allowed in the 'Redirected Printers' box).

Web Settings

You can easily define some global parameters for all remote access connections, regardless of the selected profile by using **web.settings.js**. You can find this file in the installation directory. It is an editable javascript file that contains a global variable called **Settings**. The *Settings* 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 Workspace 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 Workspace [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 Workspace reads the values in Settings and merges its parameter list with the profile settings, overriding the profile attributes with the Settings 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 `web.settings.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 Settings 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](#)

Extend the Thinfinity® Workspace 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

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 Workspace 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 Thinfinity® Remote Workspace Toolbar

The customSettings global variable is a JSON object defined in the customSettings.js file, which you'll find in the Thinfinity® Remote Workspace 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 Workspace 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);
    ...
});
```

Customizing the Toolbar

By default, the Thinfinity® Remote Workspace 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 Workspace 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 Workspace installation.

General toolbar customization parameters

The `customSettings` global variable has two parameters that affect the complete toolbar:

The ***createToolbar*** parameter enables the Thinfinity® Remote Workspace Toolbar creation. Setting it to false will result in a Thinfinity® Remote Workspace 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 the customsettings.js file. The options that you set through this method will affect all the Thinfinity® Remote Workspace 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.

Using web.settings.js

The web.settings.js file is distributed with the installation of Thinfinity® Remote Workspace. You will find this file in the 'webrdp' folder in the Thinfinity® Remote Workspace installation directory.

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

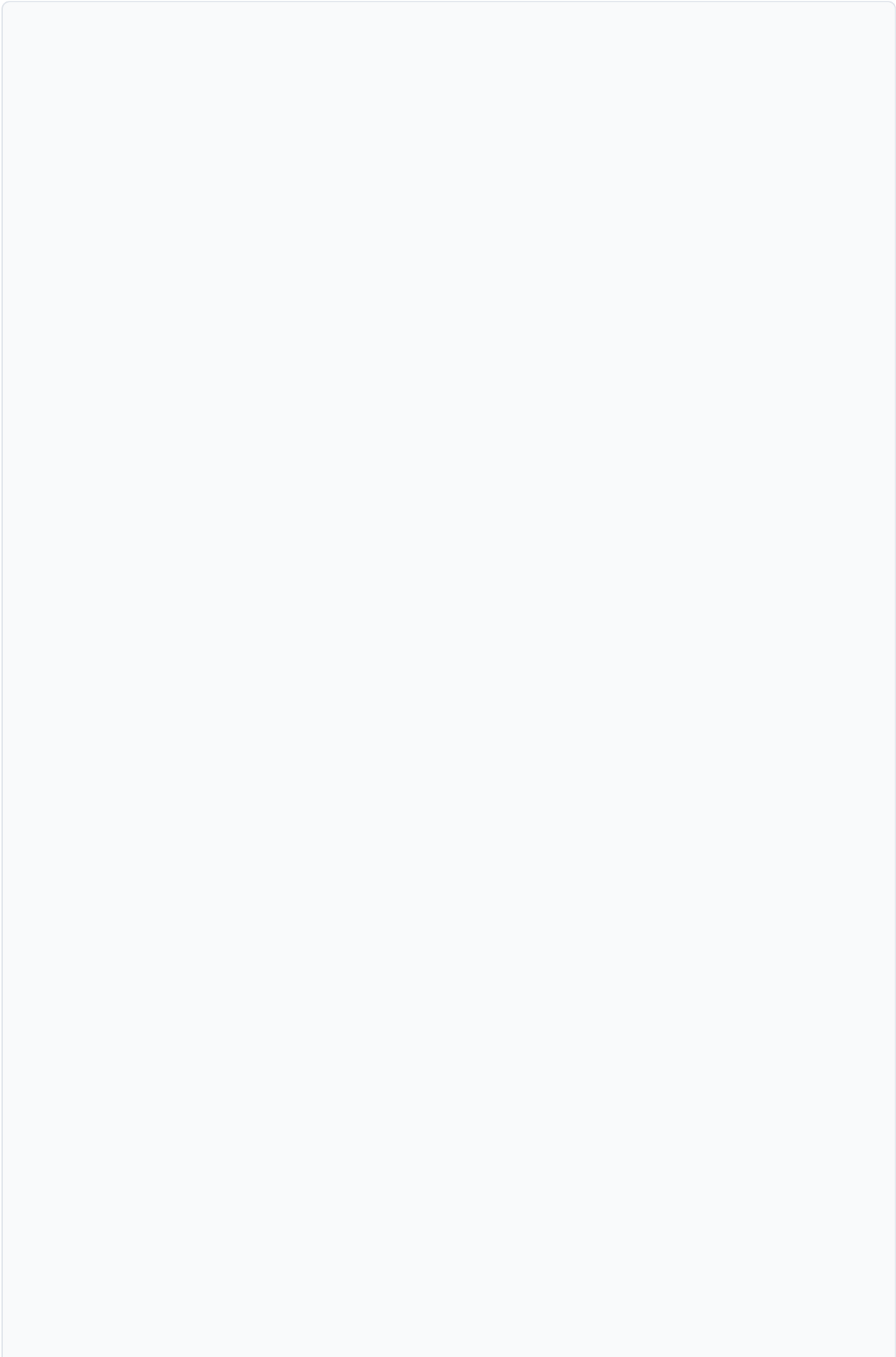
The initial values include the createToolbar and toolbarVisible parameters. Change their value to false/true following the format.

```
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 web.settings.js

In these examples, the comments are being used to describe the functions and to reference the name options have in the Thinfinity® Remote Workspace 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.imgQHighestBtn",  
// "Highest"  
"optionsMenuBtn.imgQualityBtn.imgQOptimumBtn",  
// "Optimum"  
"optionsMenuBtn.imgQualityBtn.imgQGoodBtn",  
// "Good"  
"optionsMenuBtn.imgQualityBtn.imgQFastestBtn",  
// "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 Workspace immediately. Remember that settings in web.settings.js file will override those in the [connect method](#).

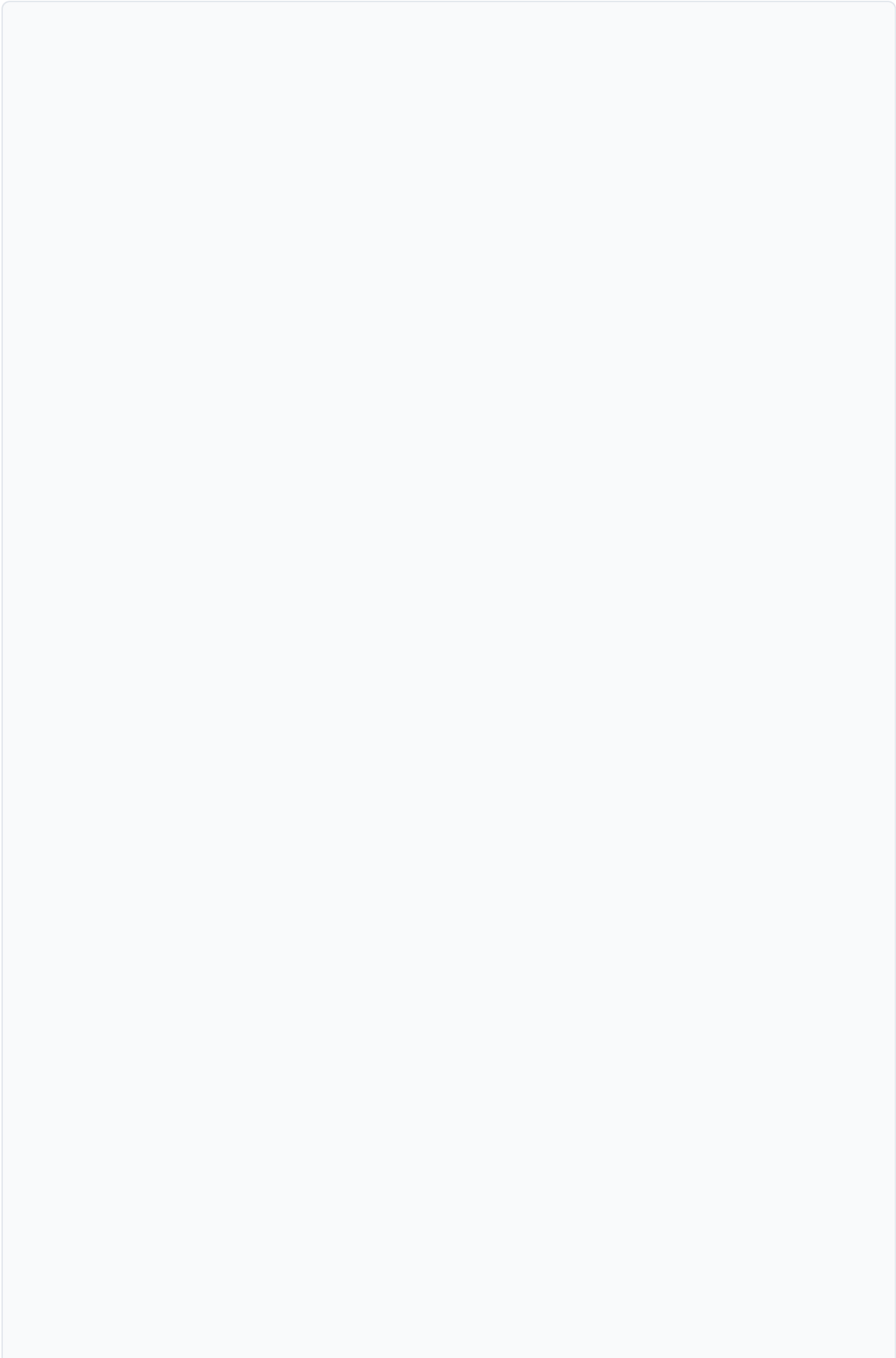
The toolbar customization is not the only thing you can do with web.settings.js. Read more about all the parameters you can include in [Web Settings](#).

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 Workspace 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.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"  
]  
}
```

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 Workspace toolbar.

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

Remote FX

The RemoteFX Codec implemented in Thinfinity® Remote Workspace 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 Workspace 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 Workspace 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 Workspace, 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 Workspace 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 to work with Thinfinity® Remote Workspace Remote FX Codec

- Run gpedit.msc
- 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"
- Set the "Enable RemoteFX encoding for RemoteFX clients designed for Windows Server 2008 R2 SP1" option to [Enabled]
- 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](#)

GFX and H264 Support

For GPU applications and video rendering

H264 Thinfinity® Remote Workspace Technology

In order to stream video and other graphic intensive file structures over the internet, you have to compress it using a technology called Codecs. A codec makes use of an encoder that converts a video or large file into a compressed format as well as a decoder that decompresses it at the other end. Most computer users are familiar with a ZIP file that is used to email large files. There are codecs used for still images such as JPEG or PNG and audio codecs such as MP3. Without codecs, it would take a lot longer for users to download files of all types.

In order to deliver a virtual desktop or application experience to remote users, you have to use codecs as well. The remote display protocol either utilizes a bitmap-based codec such as a bitmap image file (BMP) or a video-based codec such as H.264 which is an industry standard for video compression. Most remote access technologies use only Bitmap codecs. While these codecs are ideal for basic user experiences involving text and static content, they are insufficient when it comes to streaming video or GPU-intensive applications. This is why most remote access solutions cannot meet the expectations of users today that are accustomed to HD-like experiences.

Thinfinity® Remote Workspace makes use of JPG, PNG and, H.264 codecs. In most cases, the common remote display protocols are utilized, but H.264 is automatically enabled when needed in order to deliver high-quality video at very low data rates. In fact, Thinfinity® Remote Workspace is one of the only remote access solutions that offers native H.264 capability. And while we may be one of the only ones in the industry with these capabilities, there is no client or proprietary software to install on client machines as users only need an HTML5 web browser to obtain a local-like HD experience.


How to Enable H264 on your Access Profile

Enabling H264 support for one of your Access Profiles is very simple.

Just open Thinfinity® Configuration Manager and edit the profile you wish to enable this feature on.

Go to the '*Experience*' tab and mark the checkbox '*H264*':

The screenshot shows the 'Thinfinity Configuration Manager - Profile Editor' window. The 'Experience' tab is selected and highlighted in green. In the 'Graphics' section, the 'H264' checkbox is checked and highlighted in green. Other settings visible include 'Name: New Profile', 'Virtual Path: New_Profile', 'Access Key: aayu9aKwUBdJNaV6xaSLOaaXG-jawuO5', 'Label(s): \', 'Visible' checked, 'RDP' selected, 'Default profile' unchecked, and 'RDS Web Feed' unchecked. The 'Browser' section has 'Smart sizing' checked. The 'Input' section has 'Multitouch redirection' unchecked. The 'Graphics' section has 'Remote FX' unchecked, 'Desktop background' unchecked, 'Visual styles' checked, 'Menu and window animation' unchecked, 'Font smoothing' checked, 'Show window contents while dragging' unchecked, and 'Desktop Composition' unchecked. The 'None' button is visible next to the 'Name' field. The 'New Key' and 'Select Label' buttons are visible next to the 'Access Key' and 'Label(s)' fields respectively. The 'Ok' and 'Cancel' buttons are at the bottom right.

 Keep in mind, H264 takes advantage of your GPU, hence, this server must have an

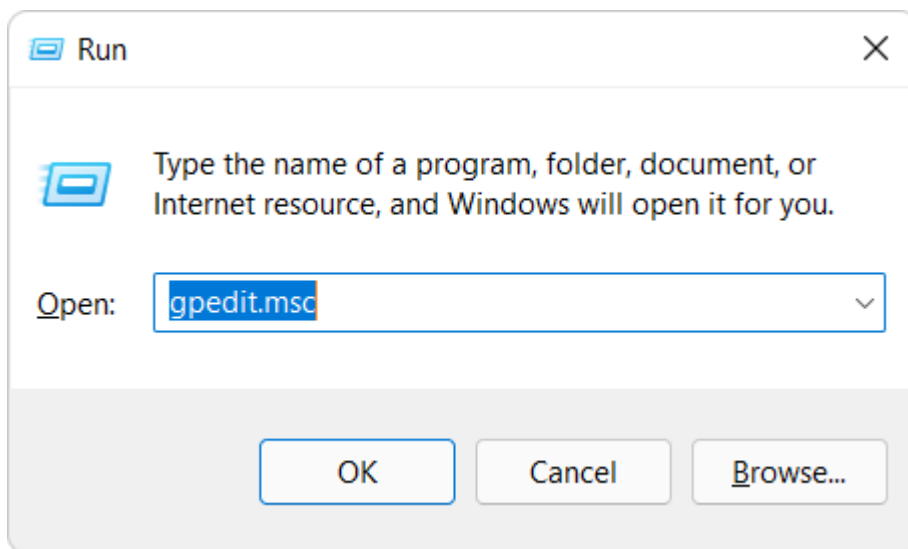
H264 compatible graphic card installed

For more details on how to enable H264 on the remote desktop, please jump to the next section [Preparing a Remote Desktop for H264 support](#).

Preparing a Remote Desktop for H264 support

To enable H264 on the remote desktop you will have to enable 3 policies in the '*Group Policy Editor*'.

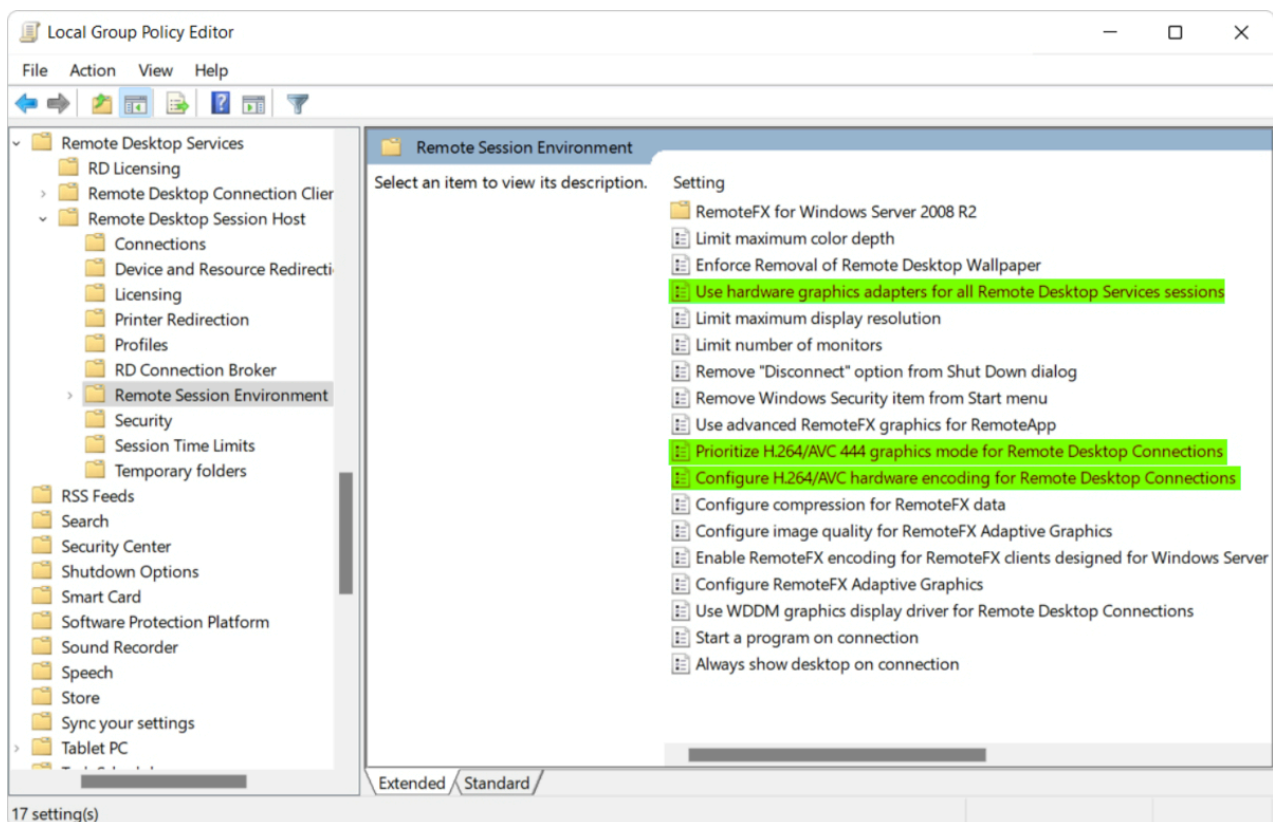
First, run '*gpedit.msc*' to access Windows Group Policy Editor:



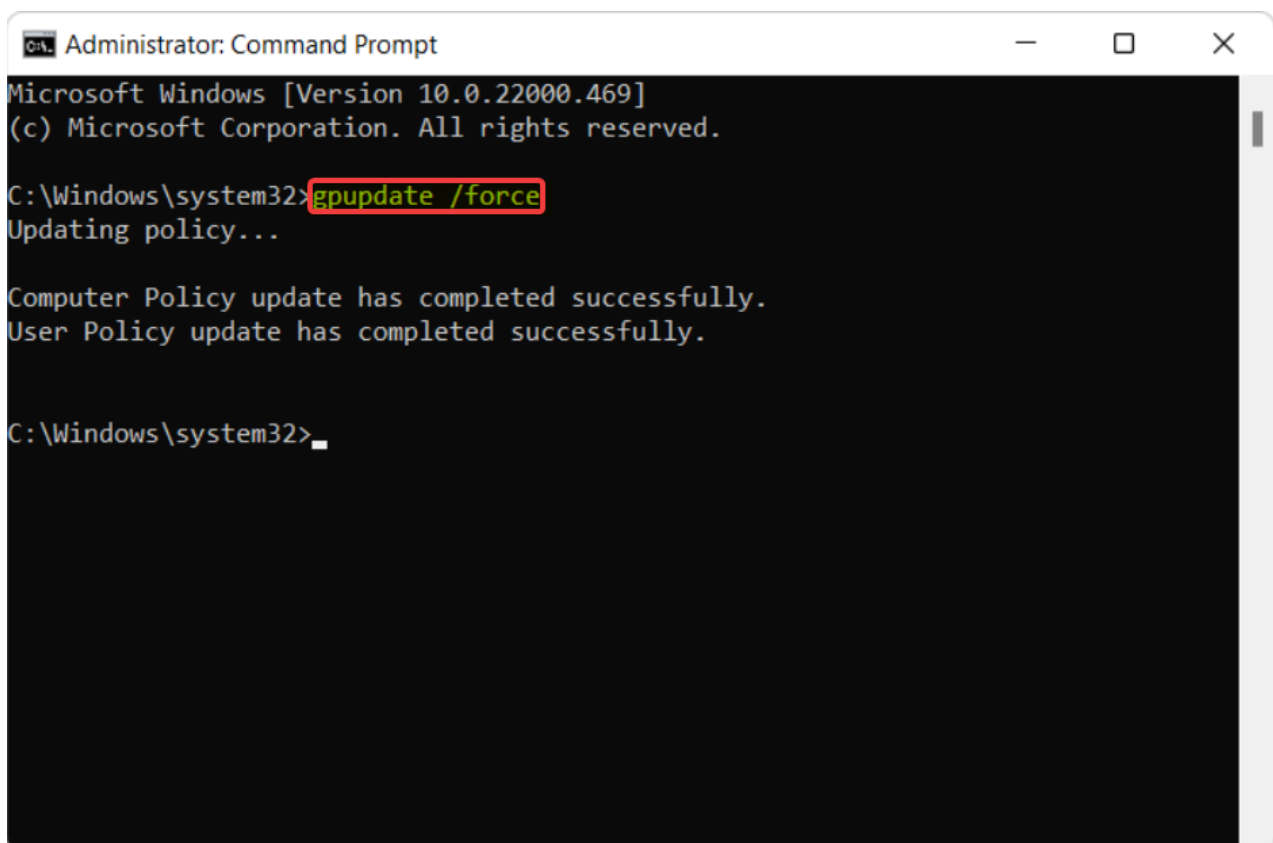
In Windows Registry Editor, navigate to '*Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Remote Session Environment*'

Here you will have to enable the following policies:

- *Use hardware graphics adapters for all Remote Desktop Services sessions*
- *Prioritize H.264/AVC 444 graphics mode for Remote Desktop Connections*
- *Configure H.264/AVC hardware encoding for Remote Desktop Connections*



Once you have enabled these policies, open a '*Command Prompt*' window as administrator and run the command '*gpupdate /force*' to update your group policies:



Save Session

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

You can now record the sessions in a lightweight format that will be interpreted by Thinfinity® Remote Workspace 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 Workspace server.

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 Workspace, 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](#).

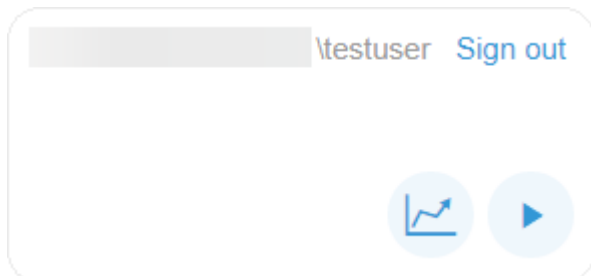
After checking this option, the connections will be recorded and listed to be viewed by the corresponding users.

Read more:










- [Play recorded sessions](#)





Play Recorded Sessions

When a user has the appropriate permissions to see sessions, they will see a "Play" icon below the "Sign out" button.



By clicking on this icon, you will access the Sessions Playback screen.

Sessions Playback						
						  
	Host	User	Start Date	End Date	Duration	
	localhost	EC2AMAZ-0I97FR1\testuser	28.5.2020, 10:50:31	28.5.2020, 10:50:36	00:00:05.609	
	localhost	EC2AMAZ-0I97FR1\testuser	28.5.2020, 10:50:22	28.5.2020, 10:50:26	00:00:04.066	
	New Profile 1	EC2AMAZ-0I97FR1\testuser	25.5.2020, 11:33:19	25.5.2020, 11:33:32	00:00:13.041	

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

Multi-touch Redirection

Multi-touch Redirection for desktop touch devices:

Thinfinity® Remote Workspace 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 Workspace 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 Workspace 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® Configuration Manager](#)
- [Gestures](#)

Enhanced Browser and DPI Support

Among the wide range of valid resolutions that Thinfinity® Remote Workspace 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 Workspace program folder. Then, if it doesn't exist there yet, it is copied to "C:\ProgramData\Cybele Software\Thinfinity\Workspace" 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",

Model Inheritance

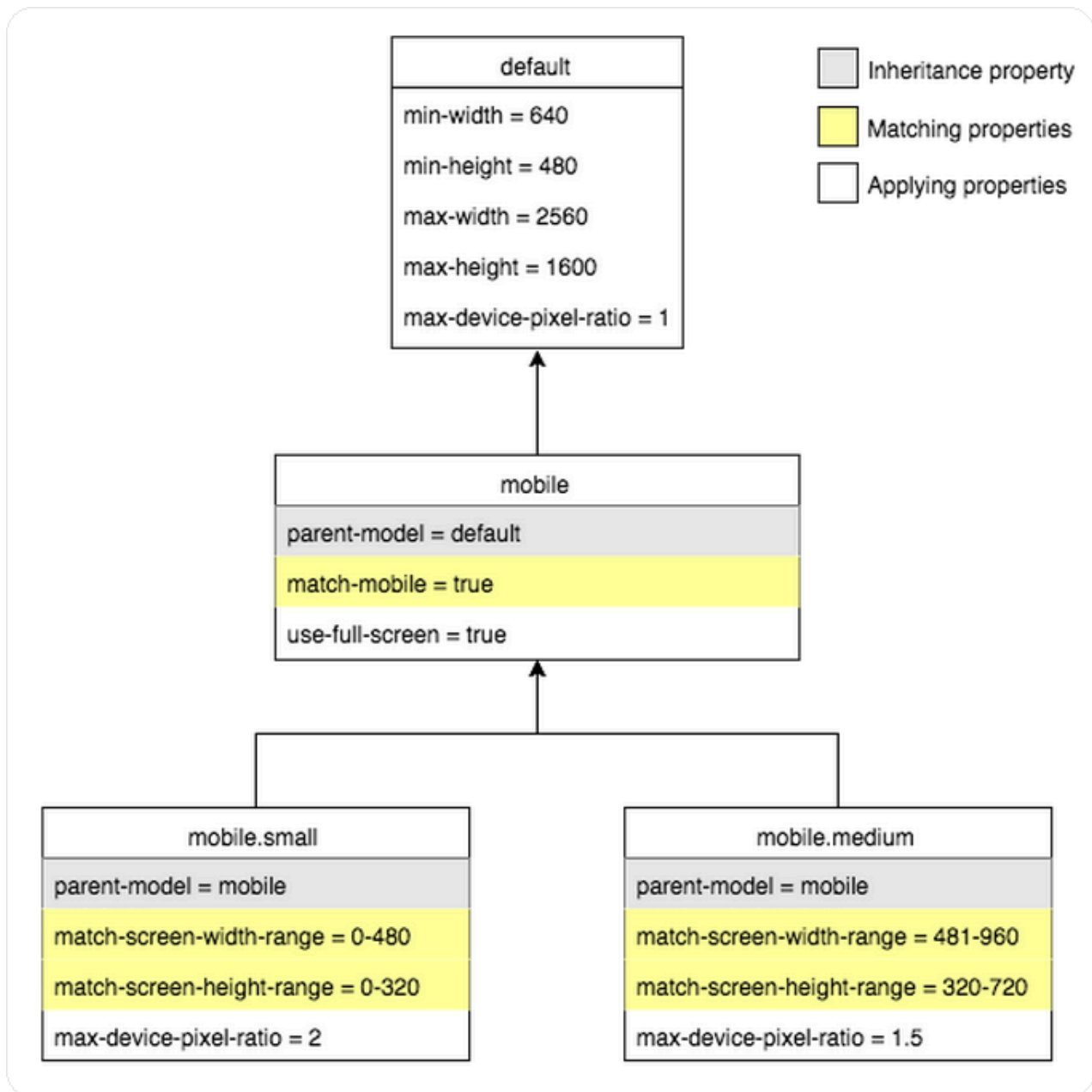
A section defines a ***model***, and each model contains a set of properties divided in two groups: *matching properties* and *applying properties*.

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:



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.

PROPERTY	DESCRIPTION
match-device-pixel-ratio	Matches any device with a specific pixel ratio.
match-mobile	Matches any mobile device.
match-orientation	Matches any device with the specified orientation: landscape or portrait.
match-screen-height-range	Matches any device with a screen height in the specified range. This range is expressed as From-To (for example, 900-1200).
match-screen-width-range	Matches any device with a screen width in the specified range. This range is expressed as From-To (for example, 400-600).
match-screen-height	Matches any device with a specified screen height.
match-screen-width	Matches any device with a specified screen width.
match-user-agent	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:

parent-model

Establish the parent model for this model.

The following properties deal with the display resolution:

PROPERTY	DESCRIPTION
device-pixel-ratio	Overrides the original device pixel ratio, scaling the content accordingly.
max-device-pixel-ratio	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.

PROPERTY	DESCRIPTION
height	Remote desktop height.
width	Remote desktop width.
max-height	Remote desktop maximum height.
max-width	Remote desktop maximum width.
min-height	Remote desktop minimum height.
min-width	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.

PROPERTY

DESCRIPTION

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

Miscellaneous properties:

PROPERTY	DESCRIPTION
use-full-screen	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.

The Calculation Process

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

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

- If the width and height properties exist, then it applies them.
- If the browser width is less than the min-width, it applies min-width.
- If the browser height is less than the min-height, it applies min-height.
- If the browser width is greater than the max-width, it applies max-width.
- If the browser height is greater than the max-height, it applies max-height.
- If a specific device-pixel-ratio was specified, it applies it.
- 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.

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.

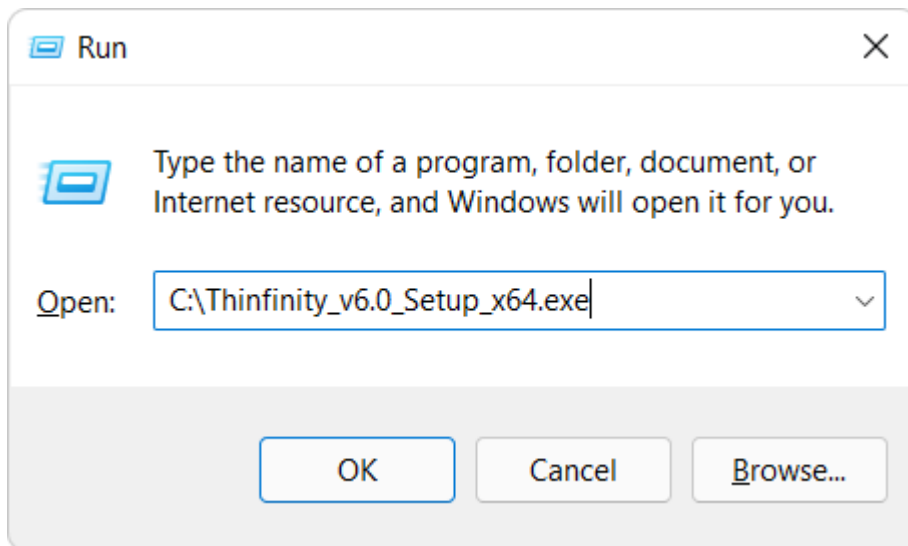
[iphone4]: The ipad will match the user agent keyword 'iphone' specified in the match-user-agent property, together with the match-screen-width and match-screen-height properties. An iphone6, with a screen width of 667px, and a screen height of 375px, would match the 'iphone' user agent keyword, but 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
```

Silent Install Options

The Thinfinity® Remote Workspace 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 Workspace installation or if you are deploying it over your local network.



Thinfinity® Remote Workspace Line Switches

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

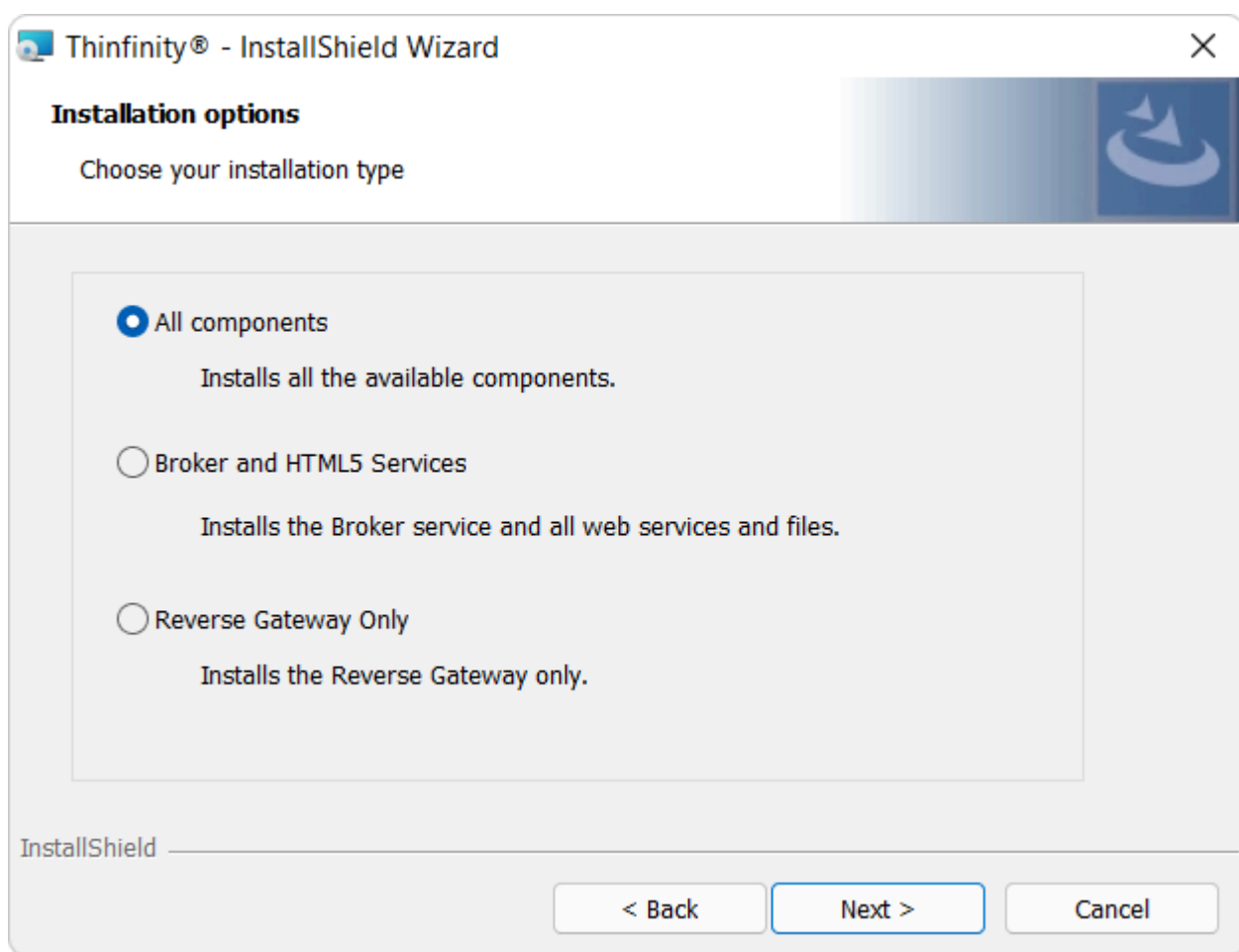
```
C:\Thinfinity_v6.0_Setup_x64 /s /v/qn
```

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

Variable	Description	Default value
<i>SM_TYPE</i>	Values: <ul style="list-style-type: none">- 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	

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



The default installation will install the All components option.

Examples

- Installing Broker and HTML5 Services only:


```
C:\Thinfinity_v6.0_Setup_x64 /s /v"/qn SM_TYPE=\"SM_Broker\""
```

- Installing Reverse Gateway Only:

```
C:\Thinfinity_v6.0_Setup_x64 /s /v"/qn SM_TYPE=\"SM_Gateway\""
```

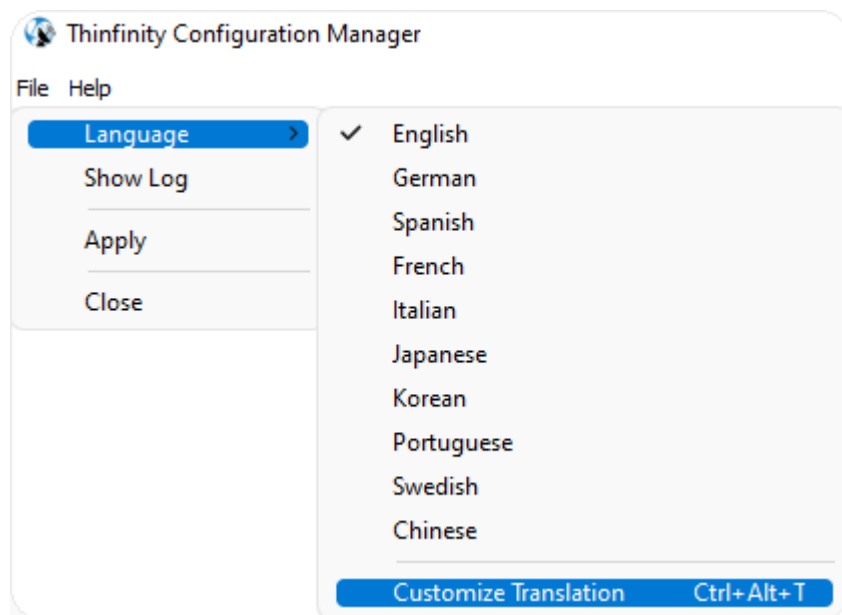
- Installing All components and passing the registration parameters:

```
C:\Thinfinity_v6.0_Setup_x64 /s /v"/qn EMAIL=\"yourmail@domain.com\"  
SERIAL=\"POIT-NNMG-PATV-54AQ-MBVT-MNAI-EQCI-MCTV\""
```

Customize Translation

Customize Translation is a feature found on Thinfinity® Remote Workspace, where you can customize each message displayed by Thinfinity® Remote Workspace on both the Web and Configuration Manager.

In order to access the translation customization click on the File menu, and under the Language menu, click on Customize Translation:



Search for the word you wish to translate, in the "Search filter text" and a dropdown menu with the available options will be displayed:

Translation Customizer

Search filter text

☒ Ignore Case

☒ Filter Source Texts

☒ Filter Translation Texts

Source text	Translation Text

Add New Message

Delete Selected Item

Source text

Translation

Apply

Close

In this case, we are searching for all the 'Disconnect' options:

Translation Customizer

Search filter text ☒ Ignore Case ☒ Filter Source Texts ☒ Filter Translation Texts

Source text	Translation Text
Disconnect	Disconnect
Disconnect your Screen Sharing session.	Disconnect your Screen Sharing session.
Disconnected	Disconnected
Disconnecting	Disconnecting

Source text
Disconnect your Screen Sharing session.

Translation
Disconnect your Screen Sharing session.

Once you select the translation you wish you change, the text will be displayed in the following editable fields:

Source text
Disconnect your Screen Sharing session.

Translation
My new Translation.

Write the new desired translation in the "Translation" field, and the click on the "Apply".

Source text

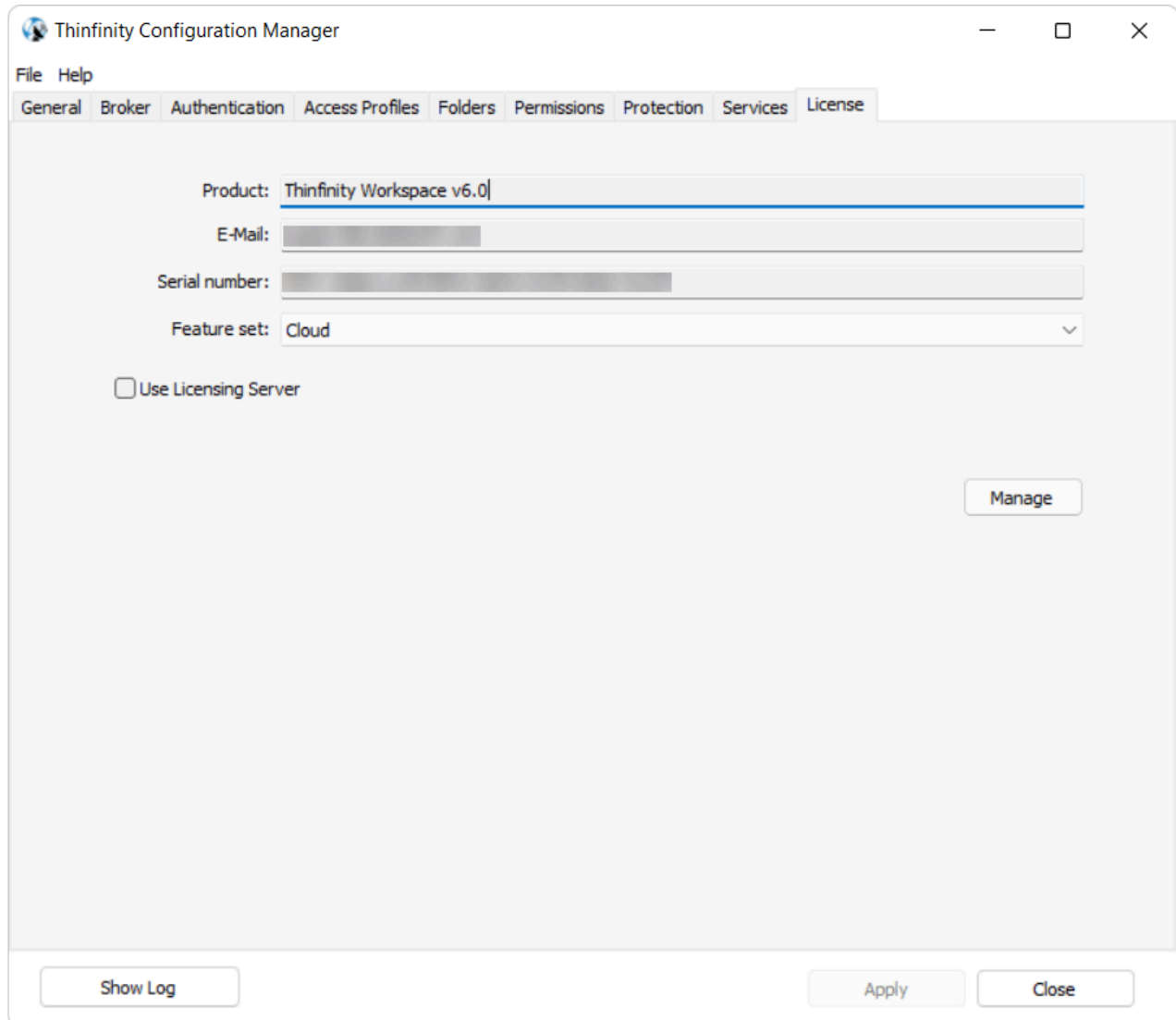
Disconnect your Screen Sharing session.

Translation

My new Translation.

License Manager

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



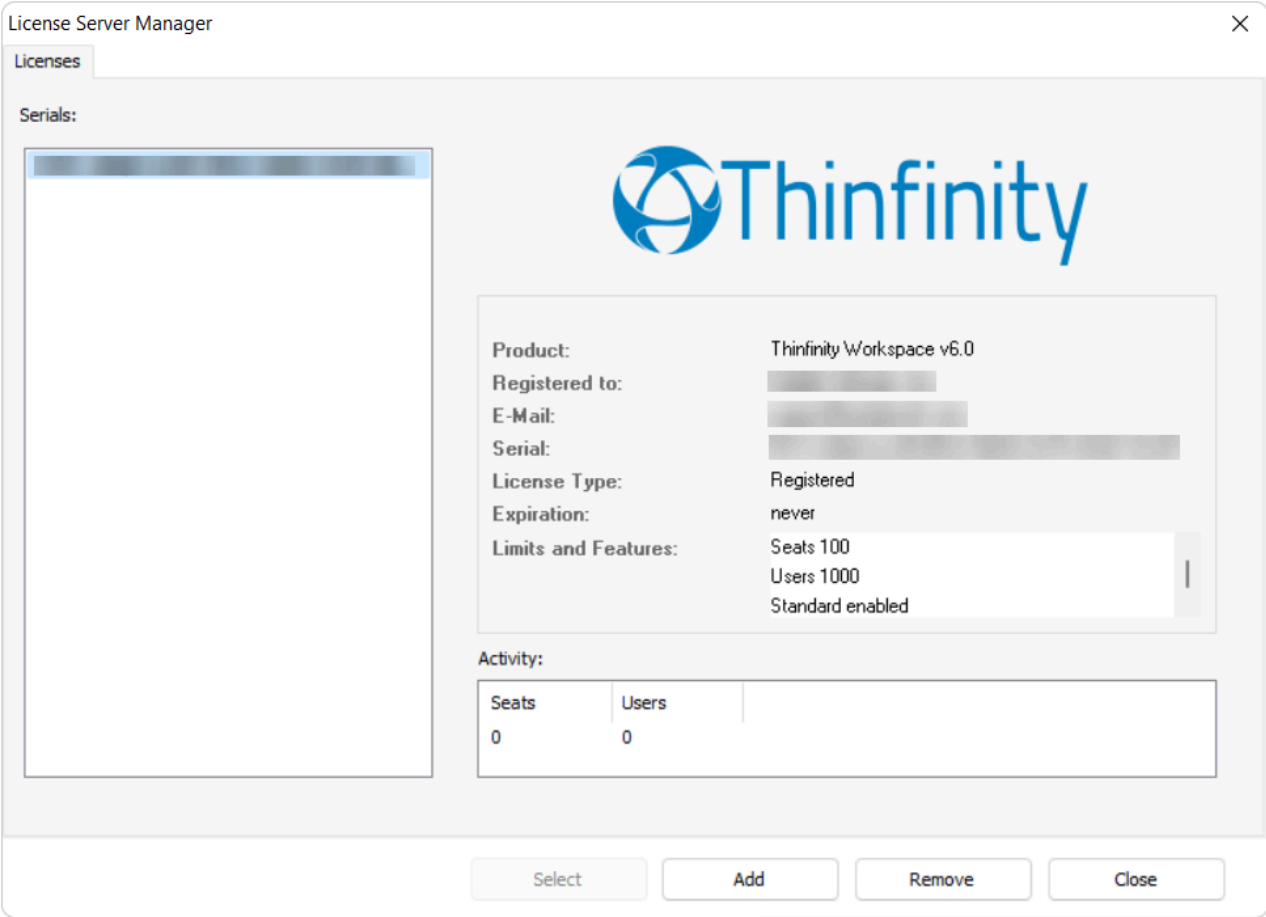
The screenshot shows the 'Thinfinity Configuration Manager' window with the 'License' tab selected. The window has a standard macOS-style title bar with minimize, maximize, and close buttons. Below the title bar is a menu bar with 'File' and 'Help'. A tabbed interface shows several tabs: 'General', 'Broker', 'Authentication', 'Access Profiles', 'Folders', 'Permissions', 'Protection', 'Services', and 'License'. The 'License' tab is active, displaying the following fields:

- Product:** A text field containing 'Thinfinity Workspace v6.0'.
- E-Mail:** A text field that is currently empty.
- Serial number:** A text field that is currently empty.
- Feature set:** A dropdown menu with 'Cloud' selected.
- ☐ Use Licensing Server

At the bottom right of the main content area is a 'Manage' button. At the bottom of the window are three buttons: 'Show Log', 'Apply', and 'Close'.

License Activation

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



OPTION	DESCRIPTION
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:

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 ↗.

Get a new Trial Serial Number

In order to register a 30-day trial license for Thinfinity® Remote Workspace, please follow these steps:

- If you haven't installed Thinfinity® Remote Workspace yet, please check this article first:

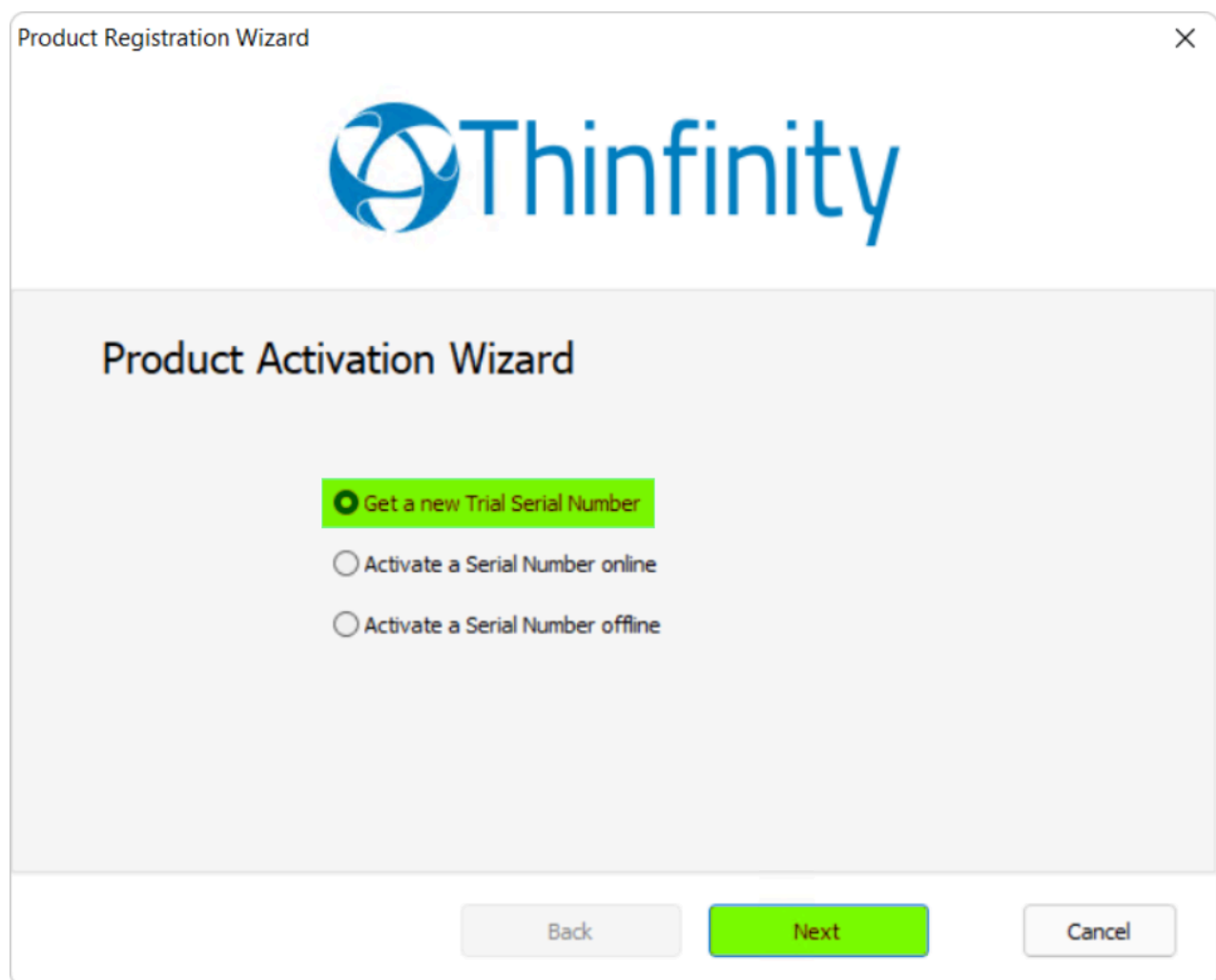


Installing Thinfinity® Remote Workspace

Thinfinity® Remote Workspace




- After installing Thinfinity® Remote Workspace, you'll be prompted with the following window when you open it for the first time. Check the first option '*Get a new Trial Serial Number*' then hit '*Next*':



- You'll now be prompted to enter a '*Registration Name*' and an '*E-Mail*' address, hit '*Next*' afterwards:

Product Registration Wizard ×



Get a Trial Serial Number

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

License:

Registration Name:

E-Mail:

- Once you filled this information, check your inbox for the serial key, then enter the '*E-Mail*' address and the '*Serial*' key you received and click on '*Next*':

Product Registration Wizard ×



Register Serial Number

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

License:

E-Mail:

Serial:

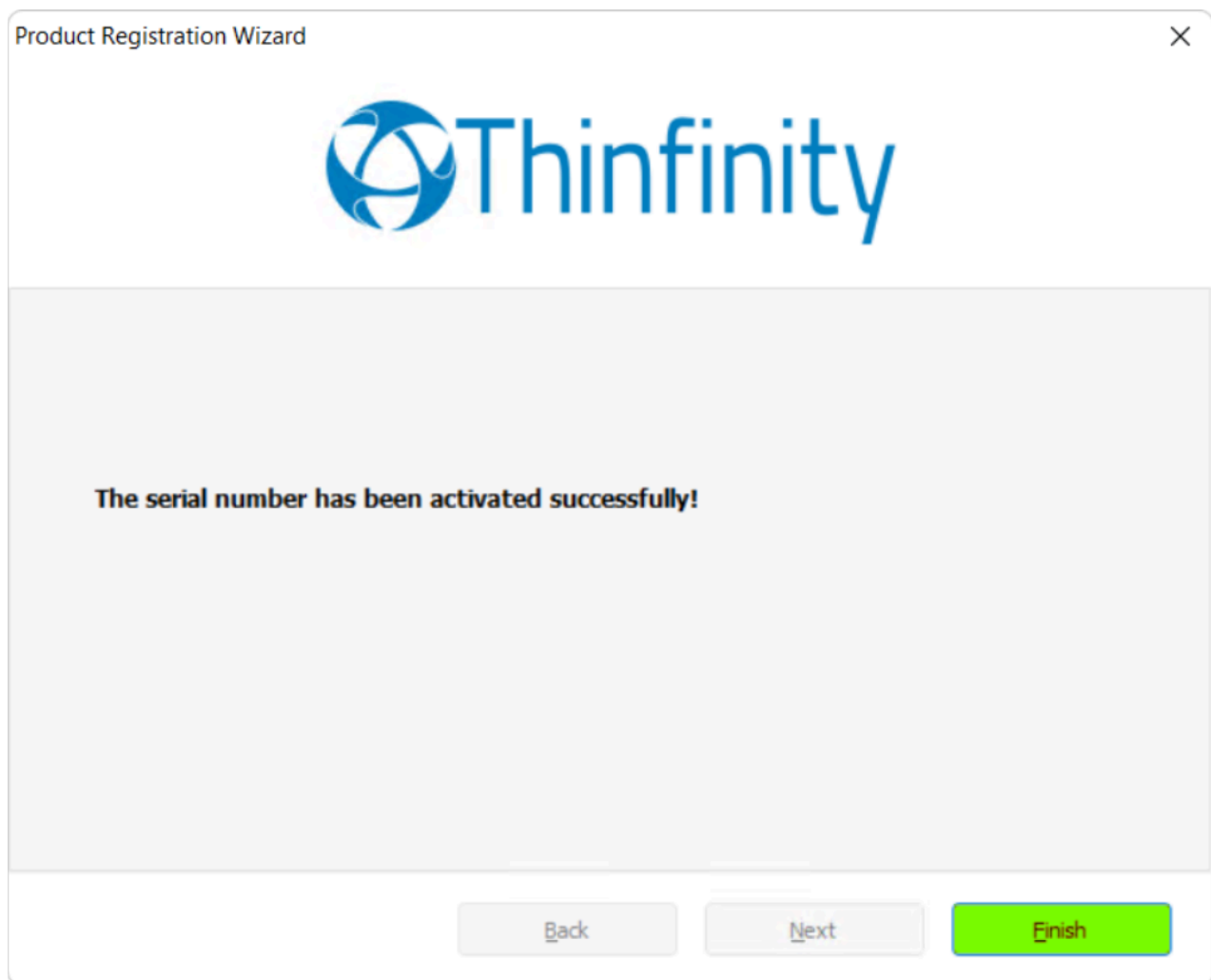
Licensing Server URL:

Primary:

Backup:

Your request has been successfully processed. An e-mail with the generated serial number has been sent to

- You have now registered your 30-day trial license of Thinfinity® Remote Workspace with unlimited access to all its features! Click on '*Finish*' to exit the Wizard:



Activate a Serial Number Online

In order to register a license for Thinfinity® Remote Workspace via the online method, please follow these steps:

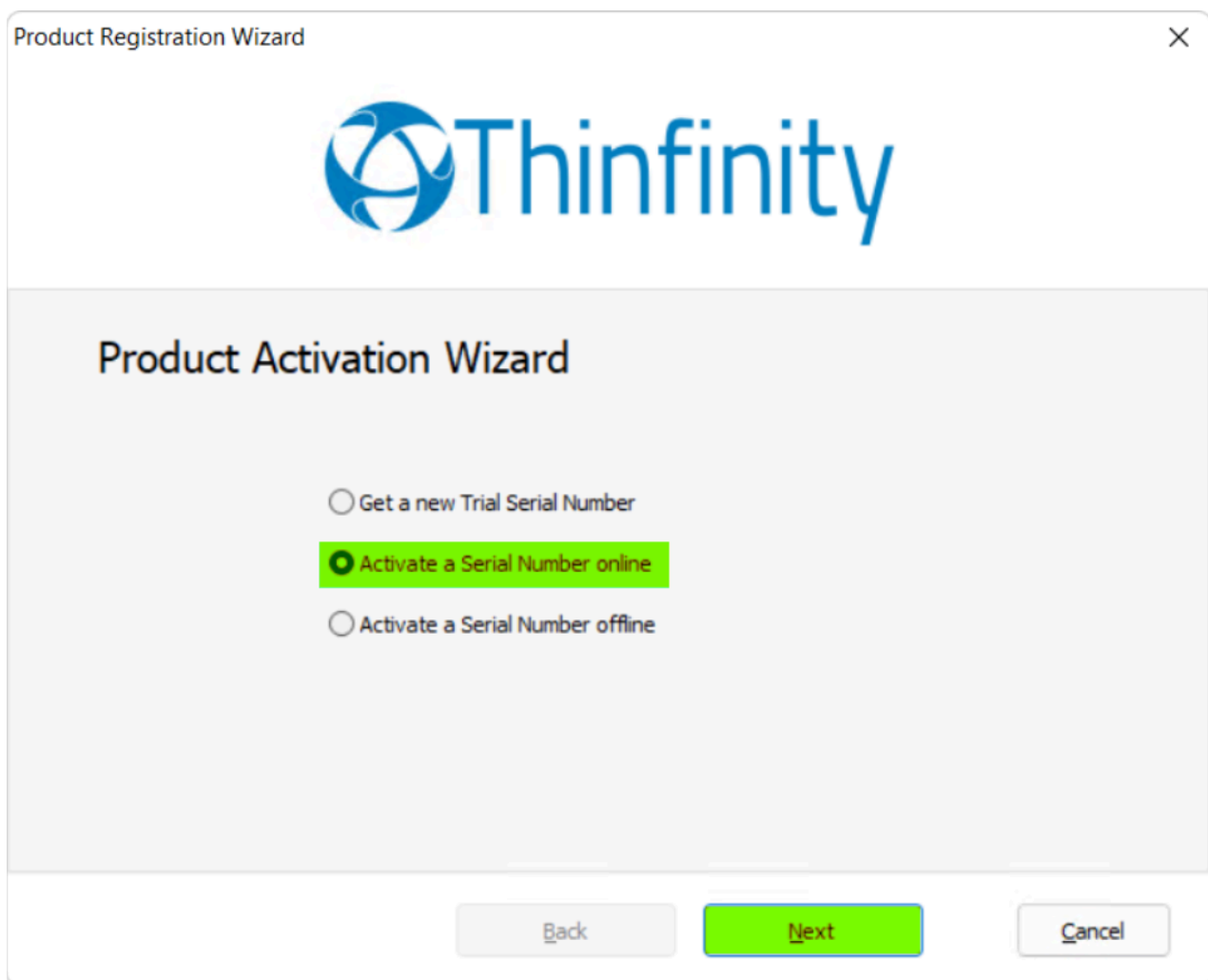
- If you haven't installed Thinfinity® Remote Workspace yet, please check this article first:



Installing Thinfinity® Remote Workspace
Thinfinity® Remote Workspace




- After installing Thinfinity® Remote Workspace, you'll be prompted with the following window when you open it for the first time. Check the second option '*Activate a Serial Number online*' then hit '*Next*':



- Enter the '*E-Mail*' and '*Serial*' key belonging to your Thinfinity® Remote Workspace license and hit '*Next*':

Product Registration Wizard
×



Register Serial Number

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

License:

E-Mail:

Serial:

Licensing Server URL:

Primary:

Backup:

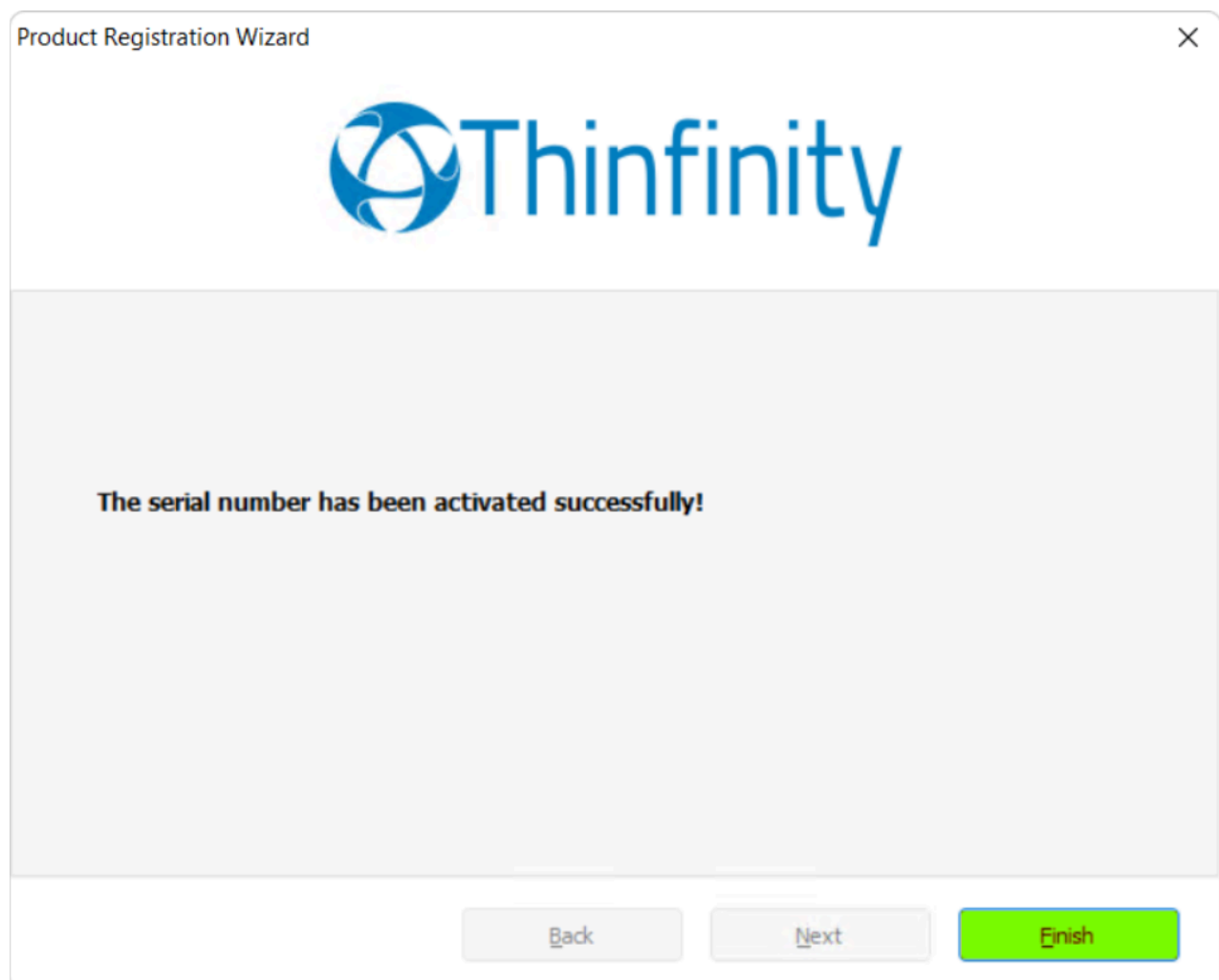
OPTION	DESCRIPTION
E-mail	Enter the e-mail address you've registered with.
Serial	Enter the serial information we provided you.
Licensing Server URL	If you installed the License Server administrator, enter the License Server URL. Otherwise leave this blank.*

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

- That you are entering the exact '*E-Mail*' and '*Serial*' number sent to you. The best practice to do this correctly is to copy - paste it, being careful not to include any spaces before or after said serial key.
- 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](#) ↗.

- You have now completed the online registration for your Thinfinity® Remote Workspace license! Click on '*Finish*' to exit the Wizard:



Activate a Serial Number Offline

Manual Activation is an activation option only for those cases when you want to activate Thinfinity® Remote Workspace 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](#). [↗](#)

In order to register a license for Thinfinity® Remote Workspace via the offline method, please follow these steps:

- If you haven't installed Thinfinity® Remote Workspace yet, please check this article first:

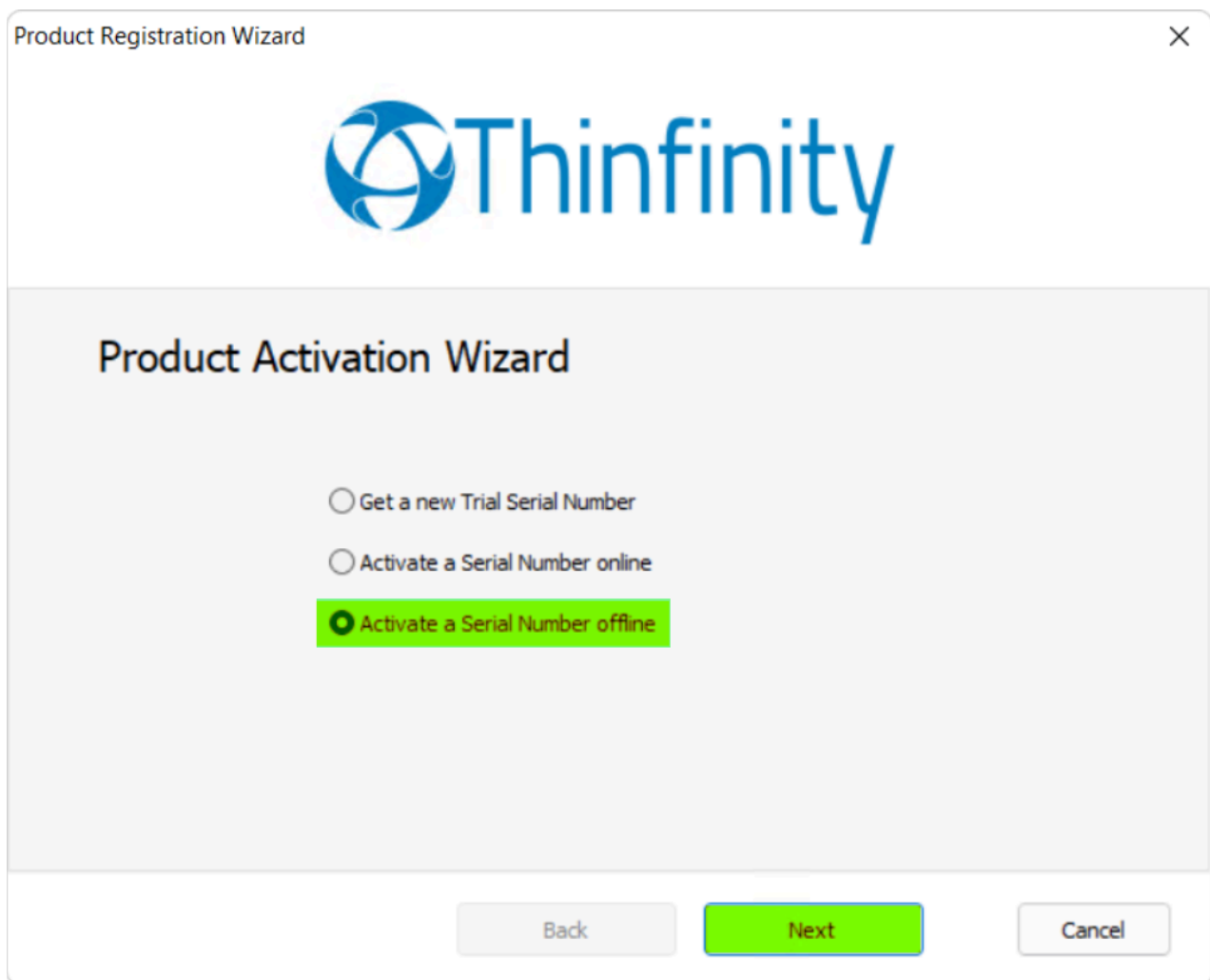


Installing Thinfinity® Remote Workspace

Thinfinity® Remote Workspace




- After installing Thinfinity® Remote Workspace, you'll be prompted with the following window when you open it for the first time. Check the third option '*Activate a Serial Number offline*' then hit '*Next*':



- In this window you would need to input the '*Serial*' key and click on '*Generate Activation Key*' to create an '*Activation Key*' that you would need to send to us via email to support@cybelesoft.com:

Product Registration Wizard
×




Register Serial Number

Enter the Serial Number to generate an offline activation key

License:

Serial:

Activation Key:



OPTION	DESCRIPTION
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 .

- Once you receive our email reply with the Smart Key needed to complete the offline activation process, you should be able to copy it and paste it on this field, then click 'Next':

Product Registration Wizard

Thinfinity

Activate license

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

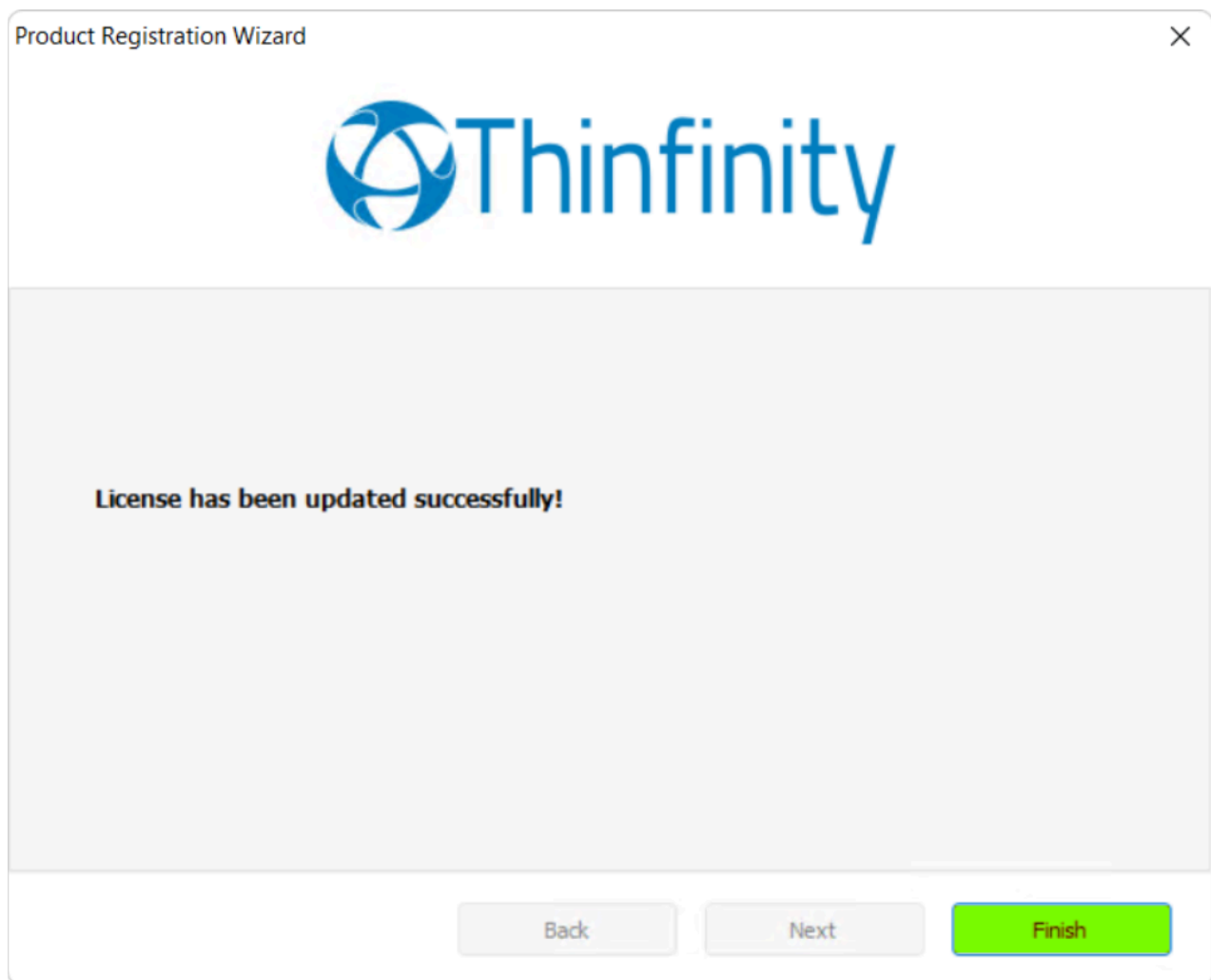
Back

Next

Cancel

OPTION	DESCRIPTION
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.

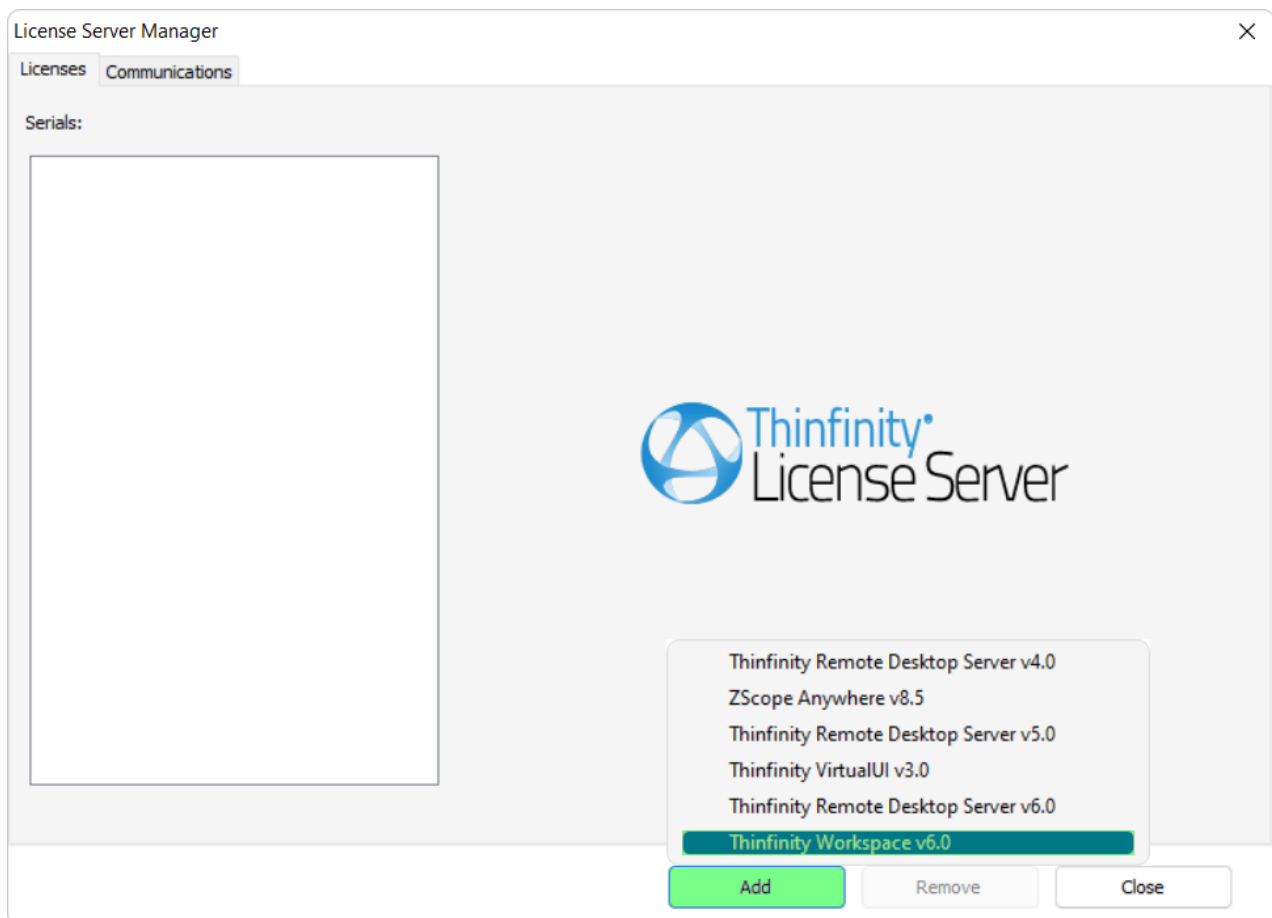
- You have now completed the offline registration for your Thinfinity® Remote Workspace license! Click on '*Finish*' to exit the Wizard:



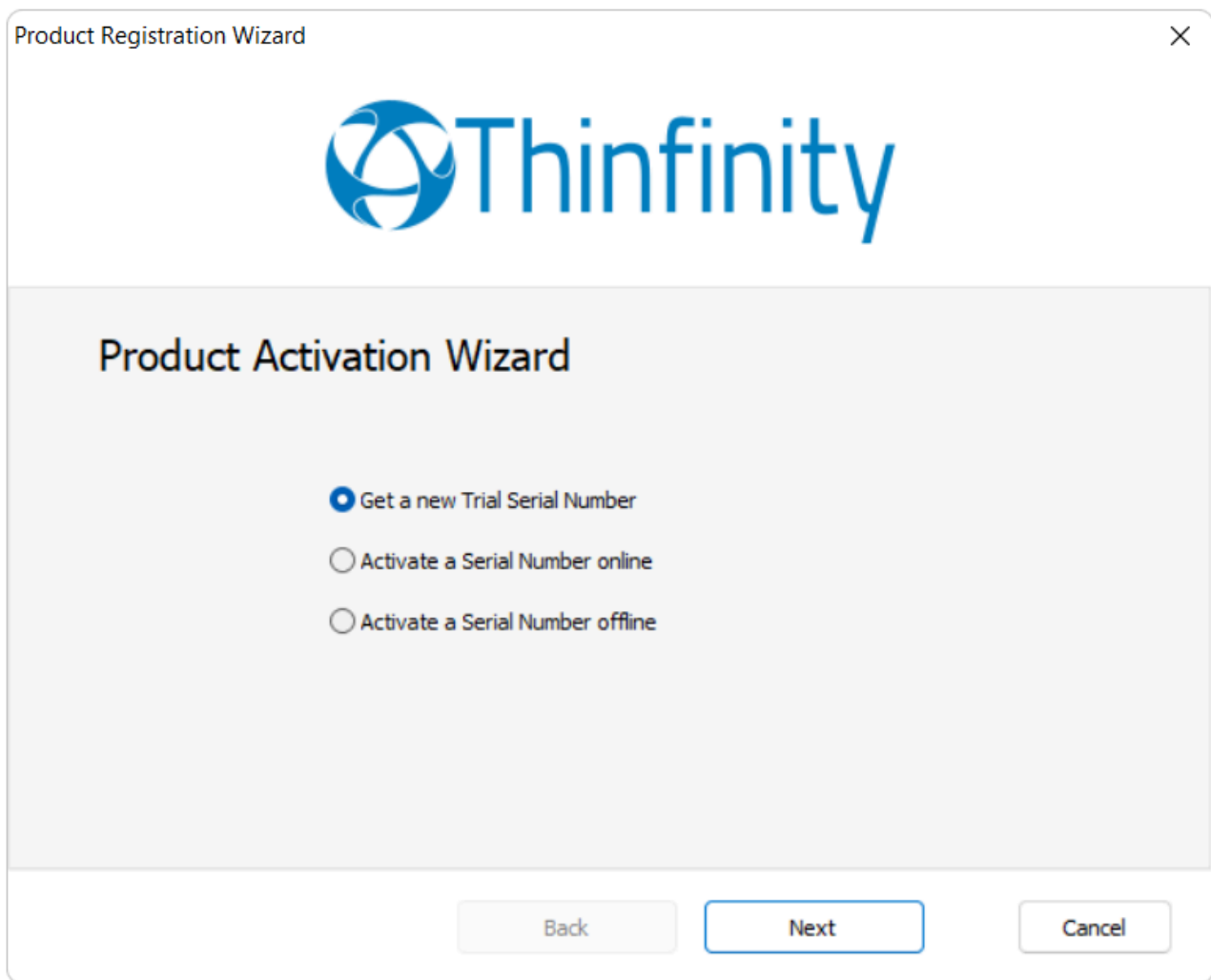
Registering Your License With The License Server Manager

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

- Open the License Server Manager and click on Add and select Thinfinity® Remote Workspace:




- Next up, you'll be able to select to register a trial license, or a purchased one via online or offline methods:



- In the next window, you'll be able to enter the e-mail address and the serial key belonging to your Thinfinity® Remote Workspace license. Hit Next afterwards:

Product Registration Wizard



Register Serial Number

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

License:

Thinfinity Workspace v6.0

E-Mail:

Serial:

Licensing Server URL:

Primary:

<optional>

Backup:

<optional>

Back

Next

Cancel

OPTION	DESCRIPTION
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.

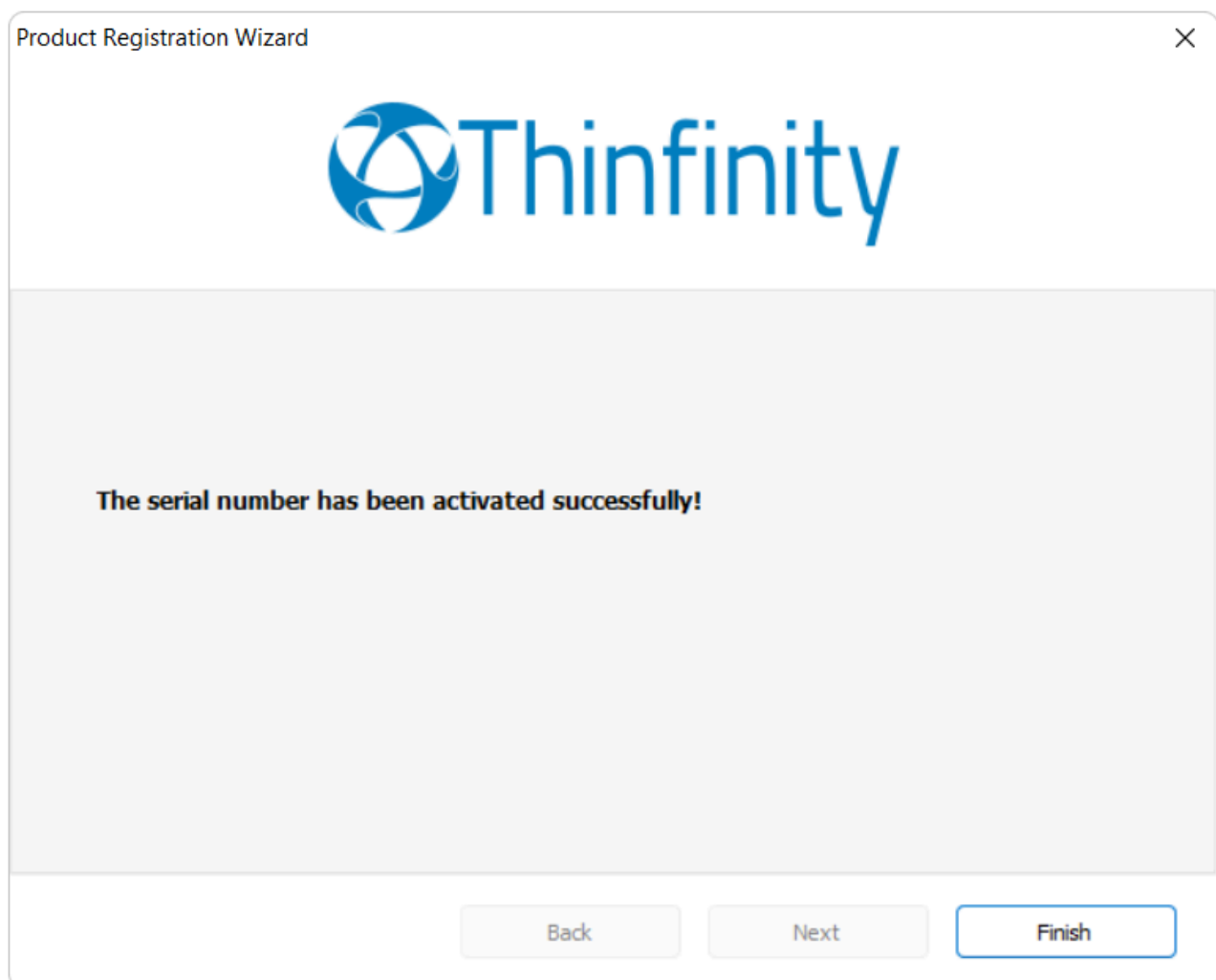
If the license information is incorrect, you will see this warning: "The license information is invalid". In this case, please verify the following:

- 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:



Please keep in mind that you would have to modify the Network ID in the Gateway tab and make sure it matches with all the servers you wish to share the license to.

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

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

Credentials Management

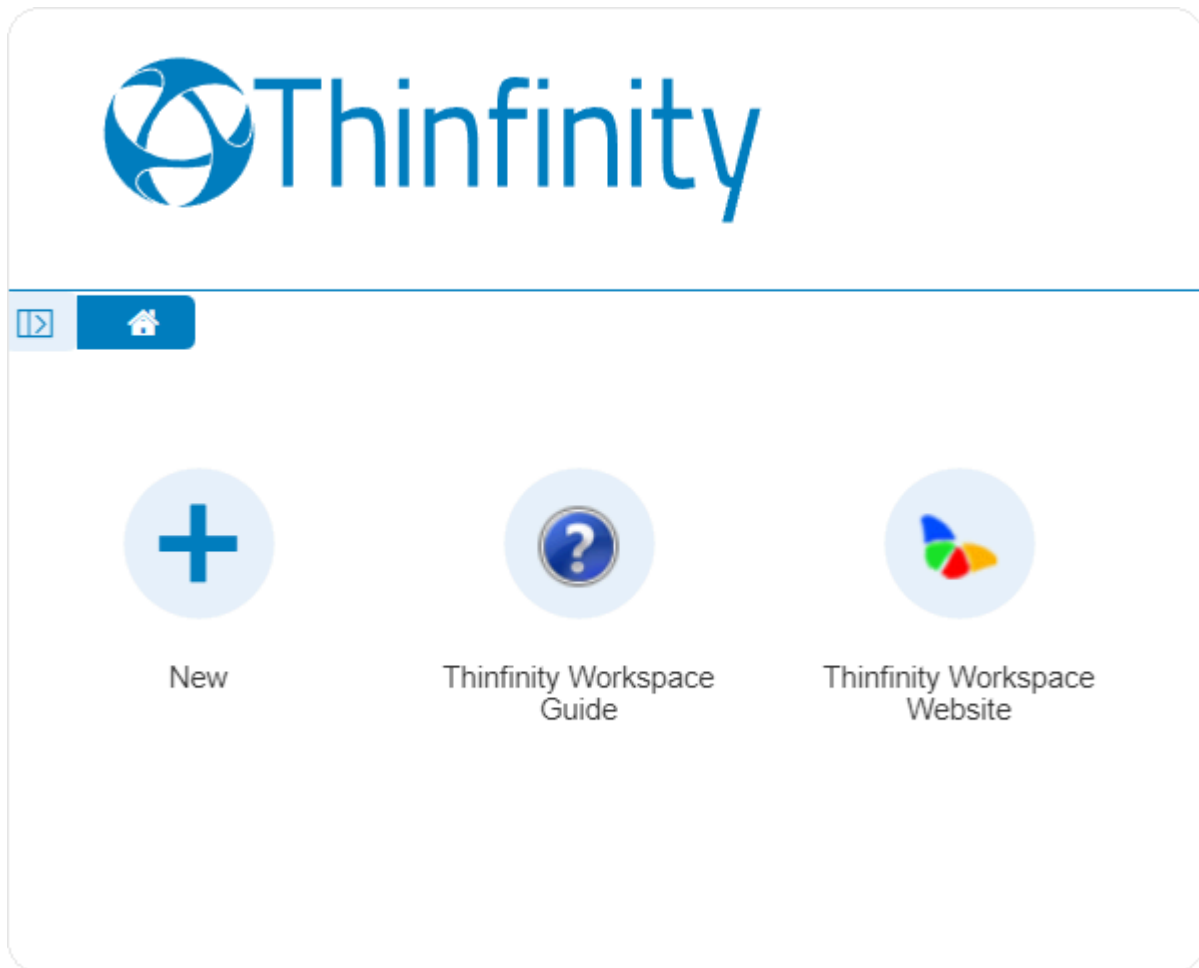
With Thinfinity® Remote Workspace, your users can manage their credentials on a user-by-user basis.

[.User-based Access Profiles](#)

[.Credentials Management](#)

User-based Access Profiles

With Thinfinity® Remote Workspace, the users will find a button on the landing screen: The "New" button.



Once clicked, you will see the New Access menu:

×

New Access

This wizard will help you create a new access profile. Please select the type of access you want to create a profile for.

Access type: Remote Desktop ▼

Make this profile available to other users ☐

- Remote Desktop
- VNC/RFB
- Terminal
- Web Link
- Web VPN
- Label

Back

Next

If After entering the address to your remote connection, you'll be prompted to specify the credentials for it:

×

Authentication

Select how you want to handle the credentials to access this resource.

Use Credentials ☒

Username:

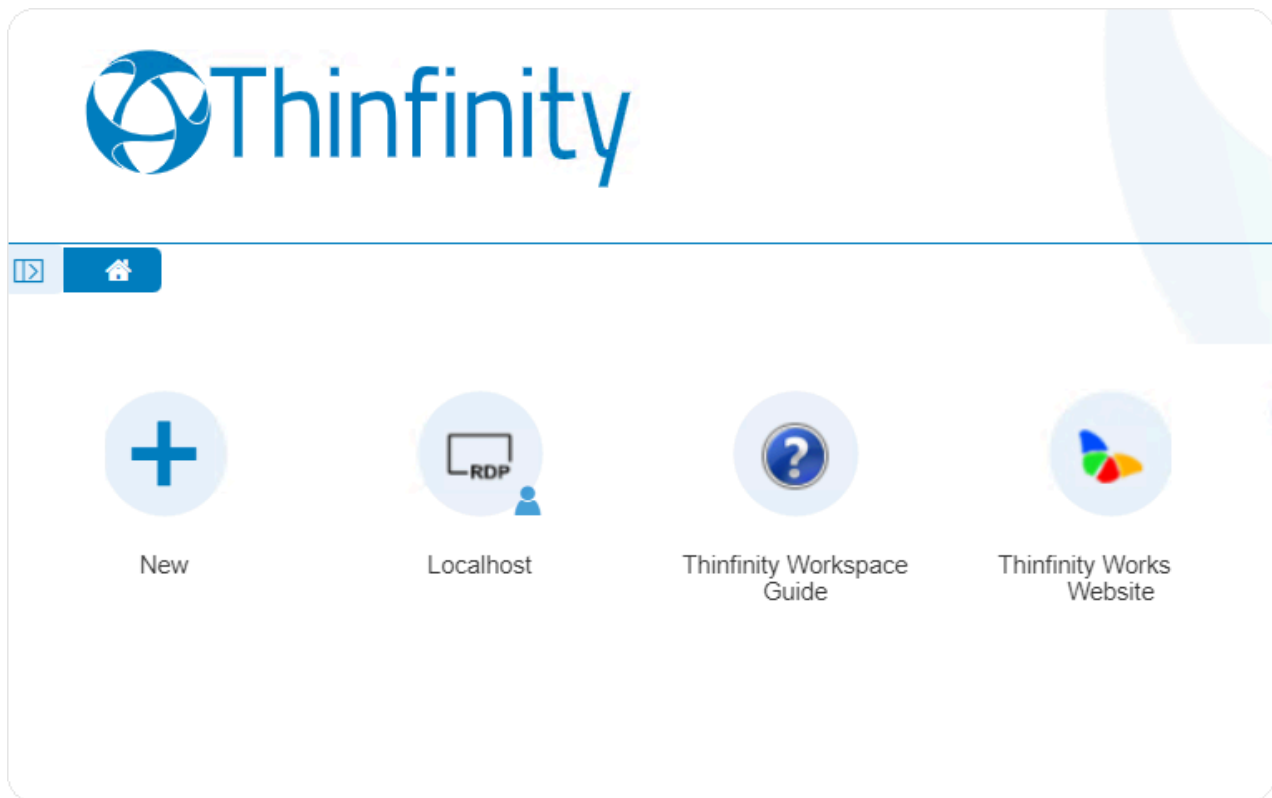
Password:

Remote Desktop

Back

Next

Once the connection is created you'll be able to access it on the landing page with the credentials saved:



Credentials Management

Thinfinity® Remote Workspace allows you to save your credentials on a profile.

To see the stored credentials, you have to click on the little pen icon at the right of the access profile, which will open the following tab:

General

Address

127.0.0.1

Broker Pool

Connection Name

Localhost


Virtual Path

Localhost

Labels

Select

Connection Icon



Enable Wake-on-LAN (WoL)

☐

User Credentials

Username

Password

Read More:

· [User-based Access Profiles](#)

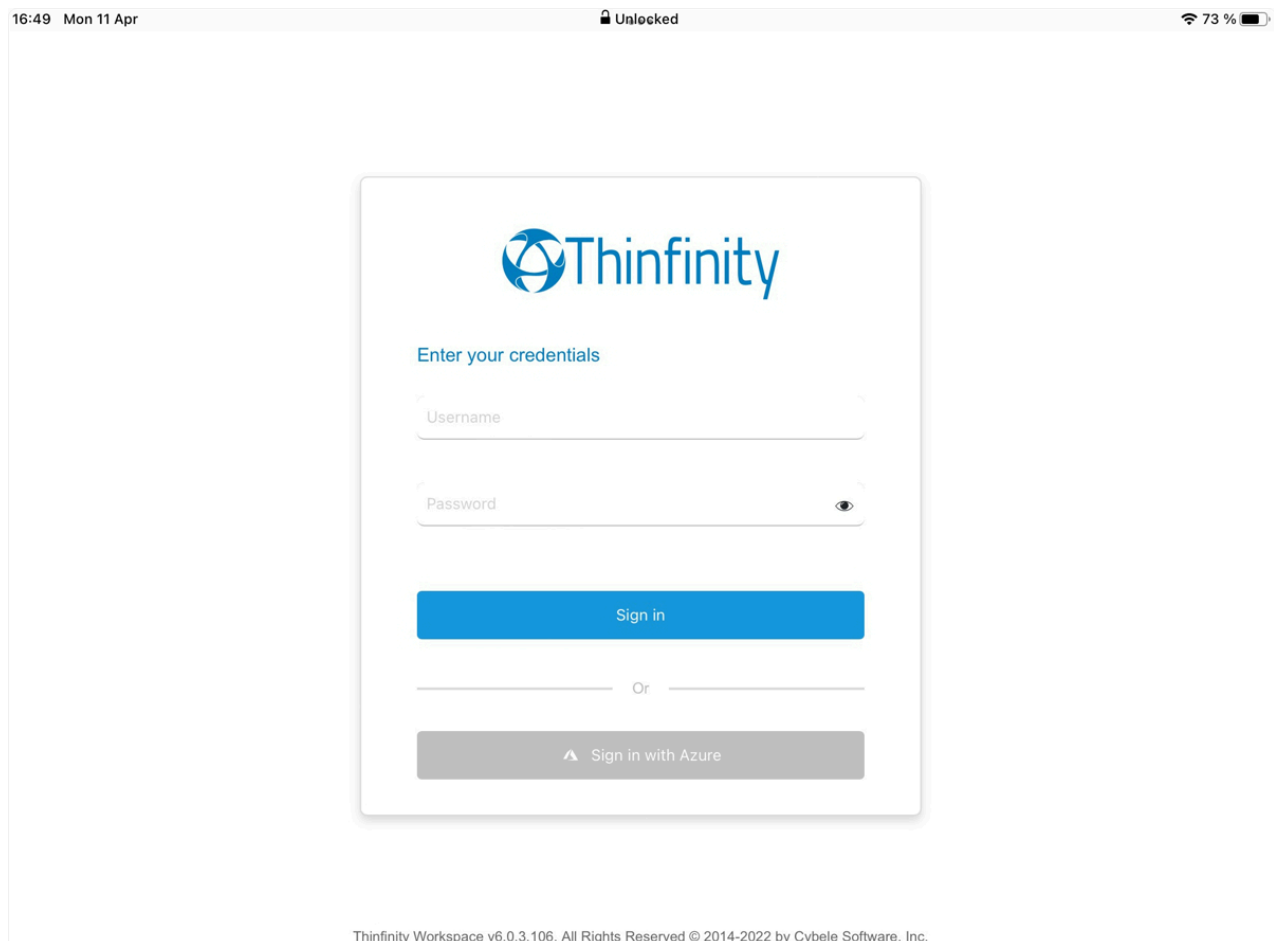
Mobile Devices Section

Mobile Devices

Using Thinfinity® 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, Chromebook and many more.

Access the Thinfinity® app 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 iPad's 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](#).

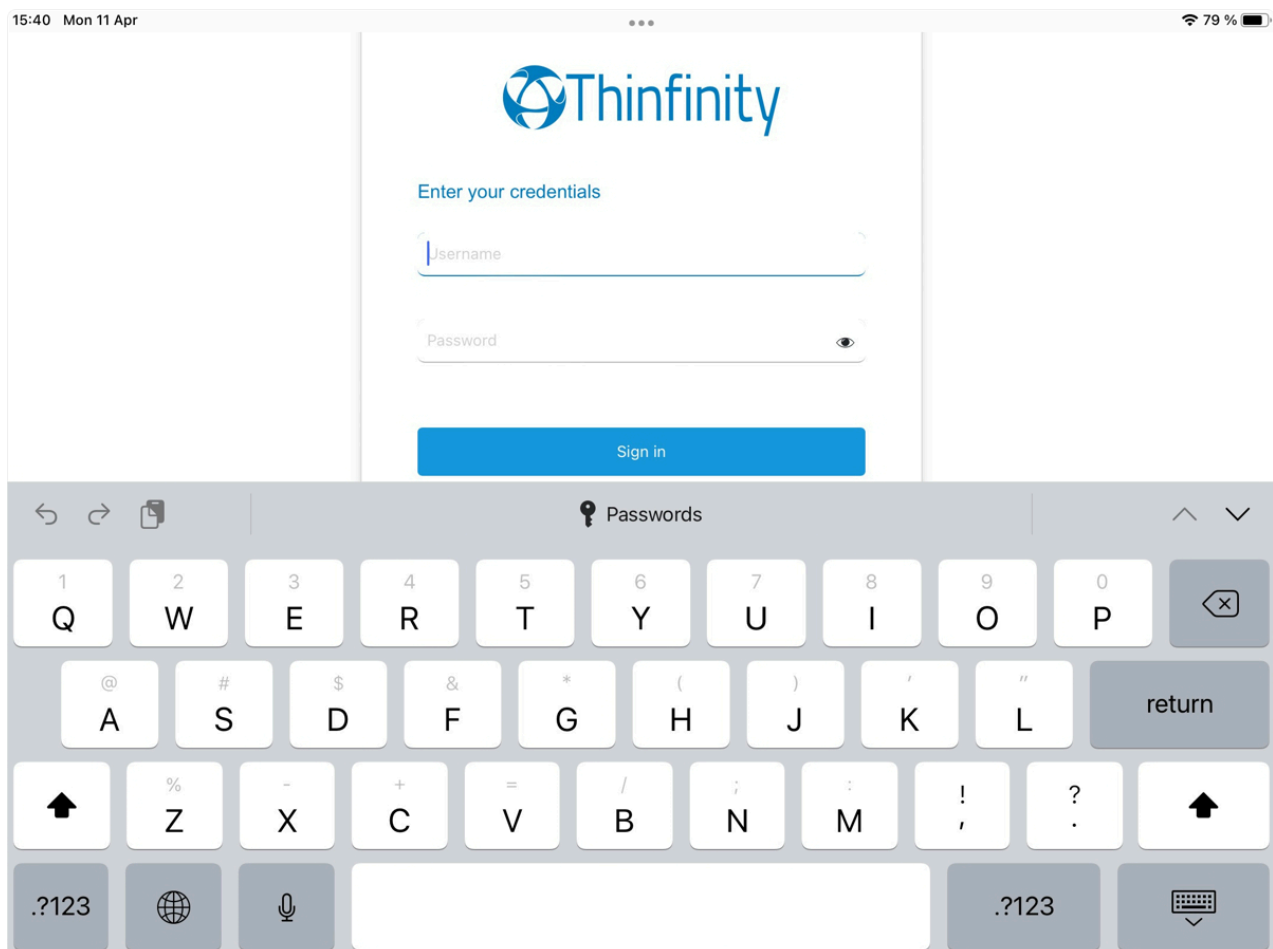
Getting into Thinfinity®

When you access the Thinfinity® app, 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 connected to a desktop or an application, you will have many other navigability options and controls available.

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.

Option	Description	
Moving the mouse around	<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>	
Regular click	<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>	Tap gesture
	Just like on the regular click you need to first position	

Double click	<p>the mouse draw over this element you want to double click.</p> <p>After that give two quick touches on the element.</p>	Double-tap
Right click	<p>When you open a connection through a mobile, Thinfinity® Remote Workspace provides an special 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>	-
Drag and drop	<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. 	Press and drag

Keyboards and Toolbars

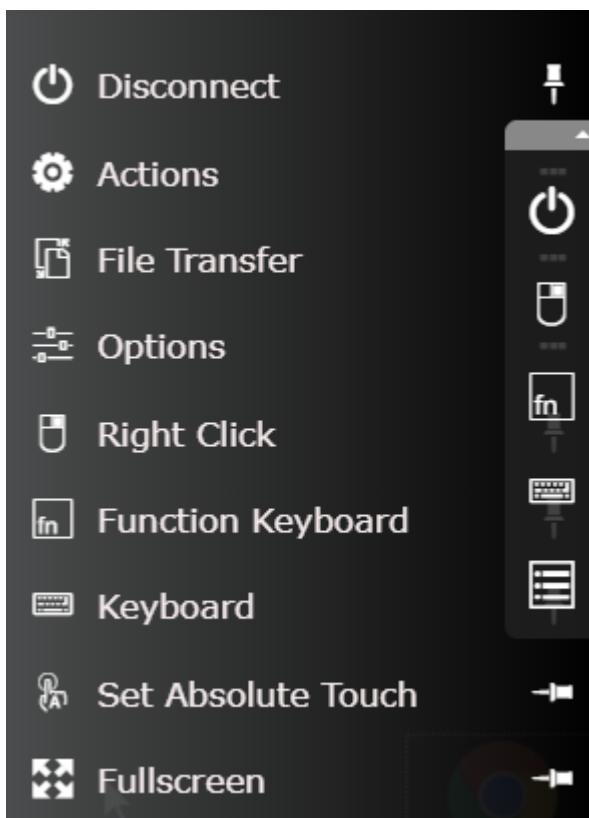
1. Right Side Toolbar

The right side toolbar will be visible from the moment you establish your remote desktop connection. By default it contains the following options :



Option	Description
1	This button disconnects the remote session. You will be prompted for confirmation.
2	This button toggles the remote mouse function to send a right button mouse click or a left button mouse click.
3	This button opens the Thinfinity® Remote Workspace Extended Keyboard. Read more about it below.
4	This button opens the native regular mobile keyboard existing in the device. Read more about it below.
5	This button opens up the toolbar editing menu, allowing for customization of the toolbar buttons.

1. Toolbar Editing Options



Use the pin/unpin buttons to modify the Mobile Toolbar

Option	Description
Disconnect	This button disconnects the remote session. You will be prompted for confirmation.
Actions	This button opens the Actions menu, where you can configure
File Transfer	This button opens the File Transfer menu, for uploading/downloading files from and to the remote connection.
Options	This button opens the Options menu, where you can select the Image Quality of the connection, and enable/disable Shortcuts.
Right Click	This button toggles the remote mouse function to send a right button mouse click or a left button mouse click.
Function Keyboard	This button opens the Thinfinity® Remote Workspace Extended Keyboard. Read more about it below.

Keyboard	This button opens the native regular mobile keyboard existing in the device. Read more about it below.
Set absolute/relative Touch	This button changes the mouse touch behavior between absolute touch and relative touch.
Fullscreen	This buttons sets the RDP connection to

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

a. Enabling the regular keyboard:

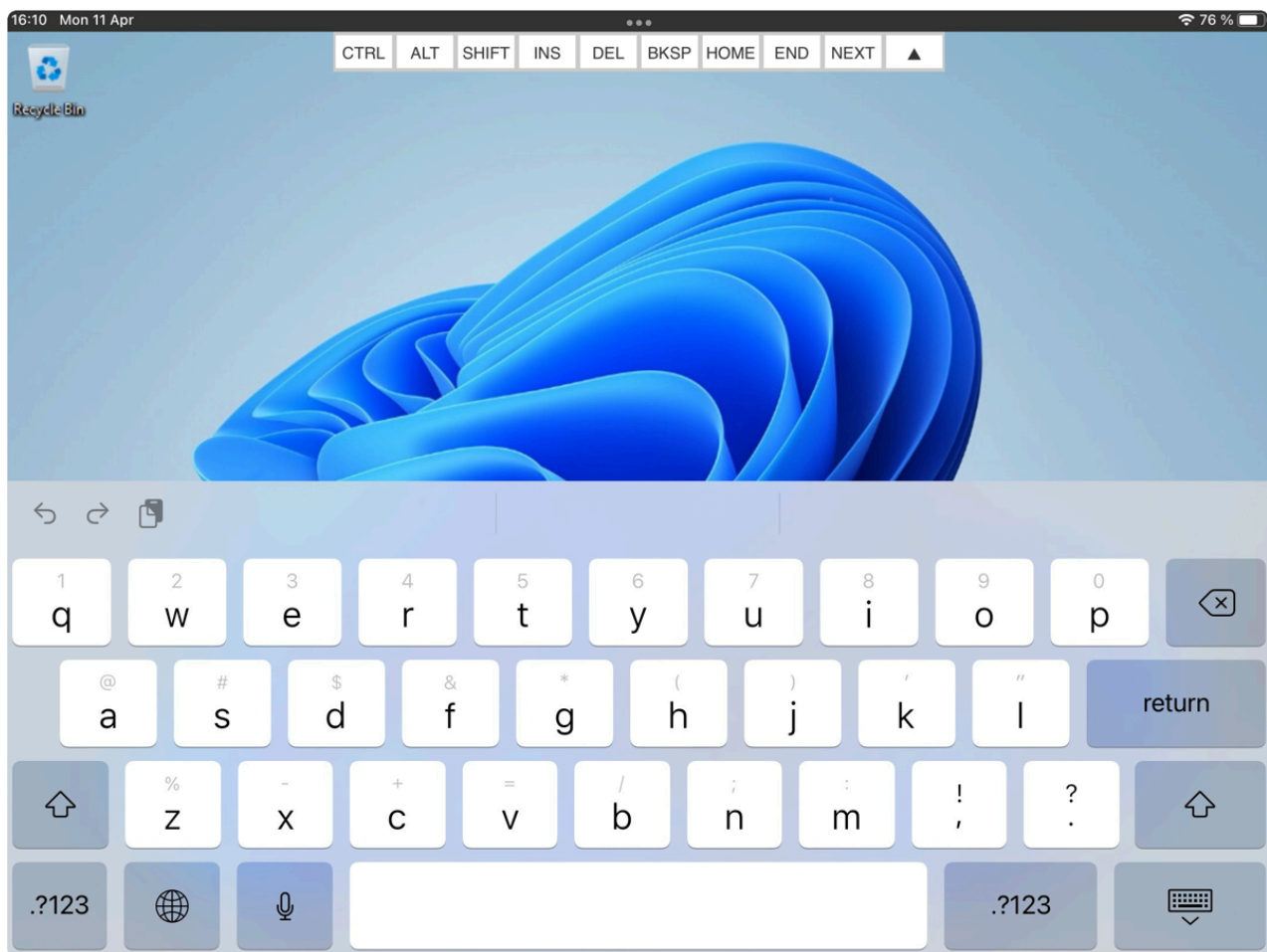
I. If you are on the "Login" or on the "Settings" screen, this keyboard will get automatically enabled every time you enter a text field.

II. Once you get connected to a remote desktop or application, you should touch the last Thinfinity® Remote Workspace 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 draw).

2. Thinfinity® Extended Keyboard

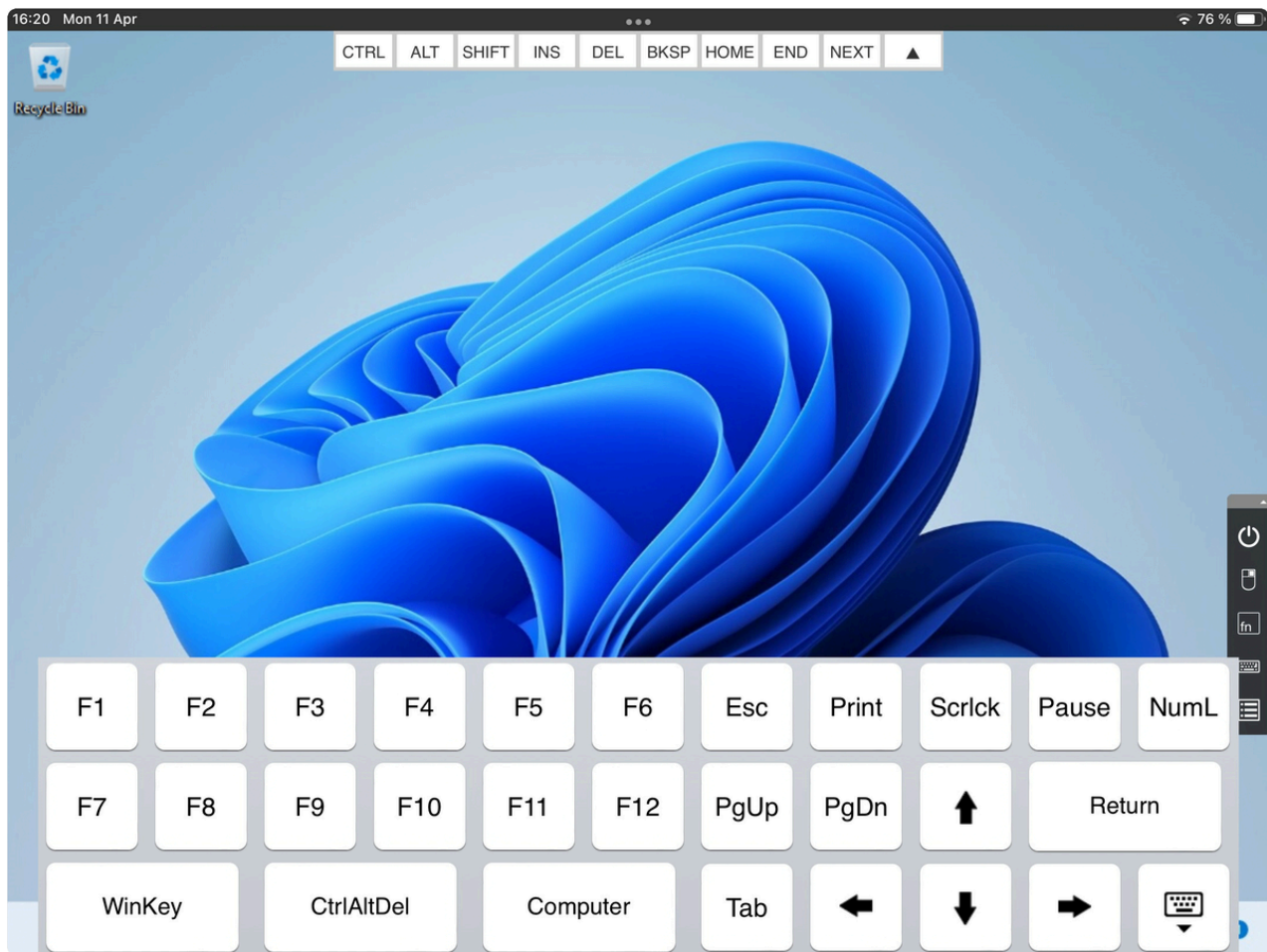
Thinfinity® has two additional keyboards.

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

a. Upper keyboard

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

Gestures

These are the gestures Thinfinity® 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:

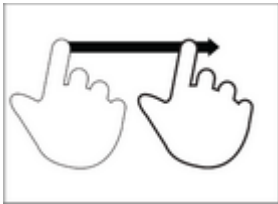


Description	Mouse
Tap Briefly touch surface with fingertip	Mouse correspondent Single-click



Description	Mouse
Double-tap Rapidly touch surface twice with fingertip	Mouse correspondent Double-click

Special gestures:

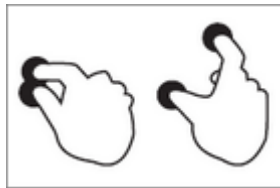


Description	Location
	Where

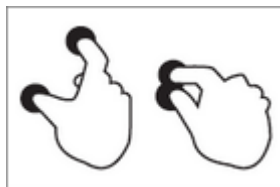
Press and Drag

Move one fingerprint over surface without losing contact

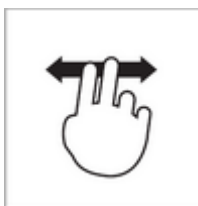
On the Connection Screen you can drag and drop an object using the Press and Drag gesture.

**Description****Location****Spread
(zoom in)****Where**

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

**Description****Location****Pinch
(zoom out)****Where**

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

**Description****Location****Double finger drag**

Move two fingertip over surface without losing contact

Where

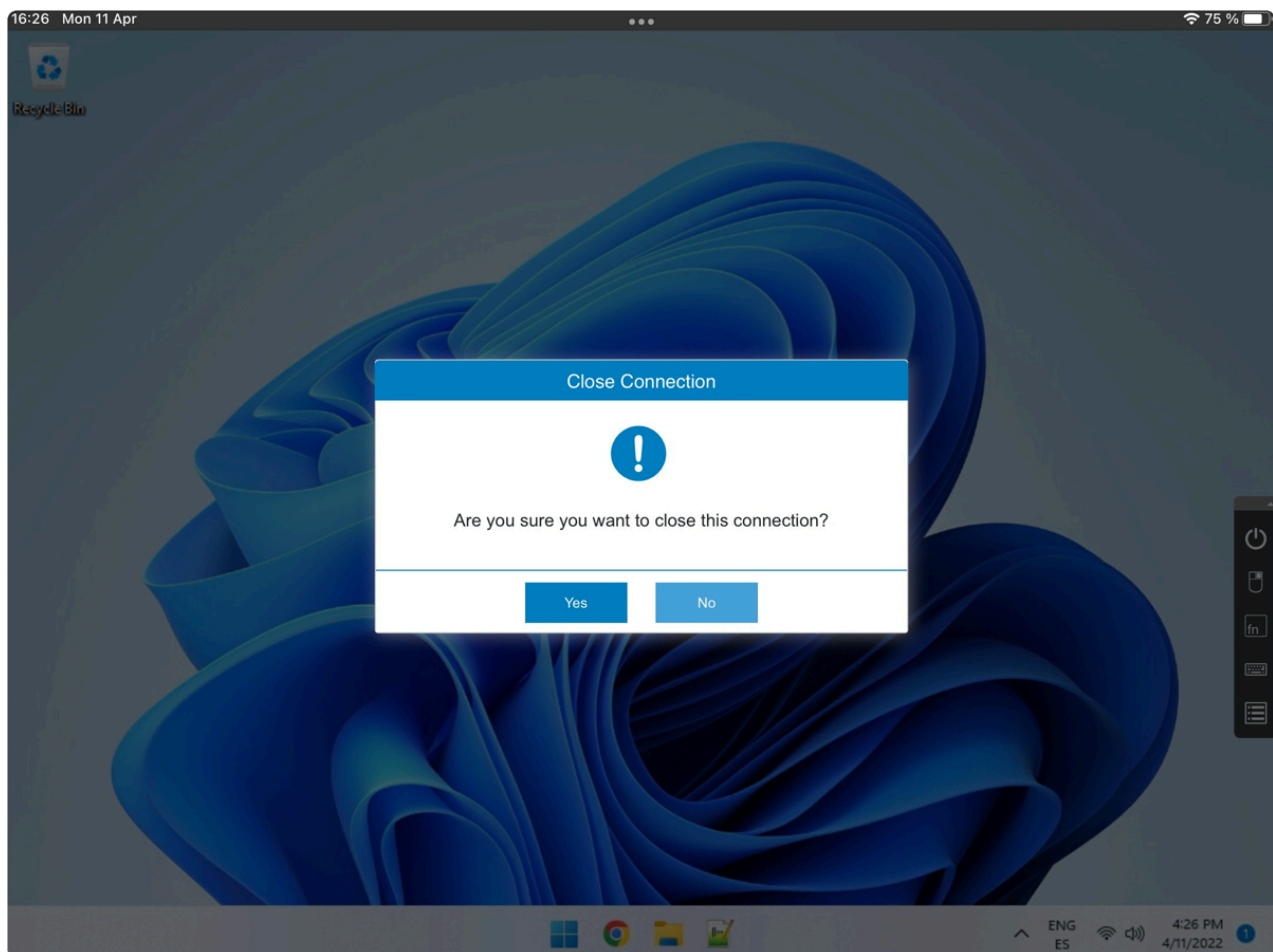
It the Connection Screen is magnified, you can use the "Double finder drag" to scroll the screen in different directions.

Disconnecting from Thinfinity®

1. In order to disconnect from the remote desktop touch the upper button located on the Thinfinity®'s 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".



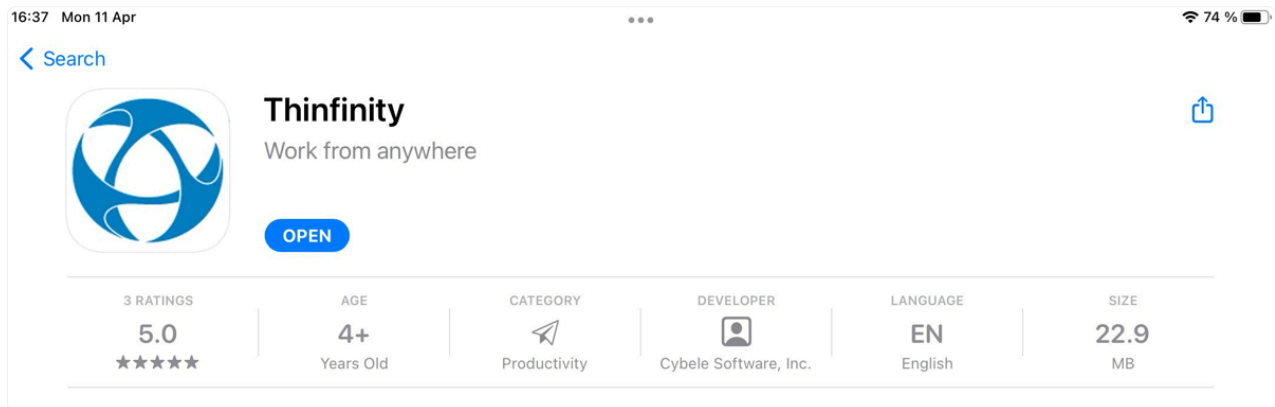
Read more:

· [Disconnecting](#)

iPad Application

Our native Thinfinity® iPad Application provides you with the safest and fastest way to use Thinfinity® on your iPad device.

In order to download it, open the App Store and search for Thinfinity®:



Scaling and Load Balancing Section

Scaling & 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 Workspace 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

Scaling and Load Balancing Configurations

If you arrive to the conclusion that your Thinfinity® Remote Workspace 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.

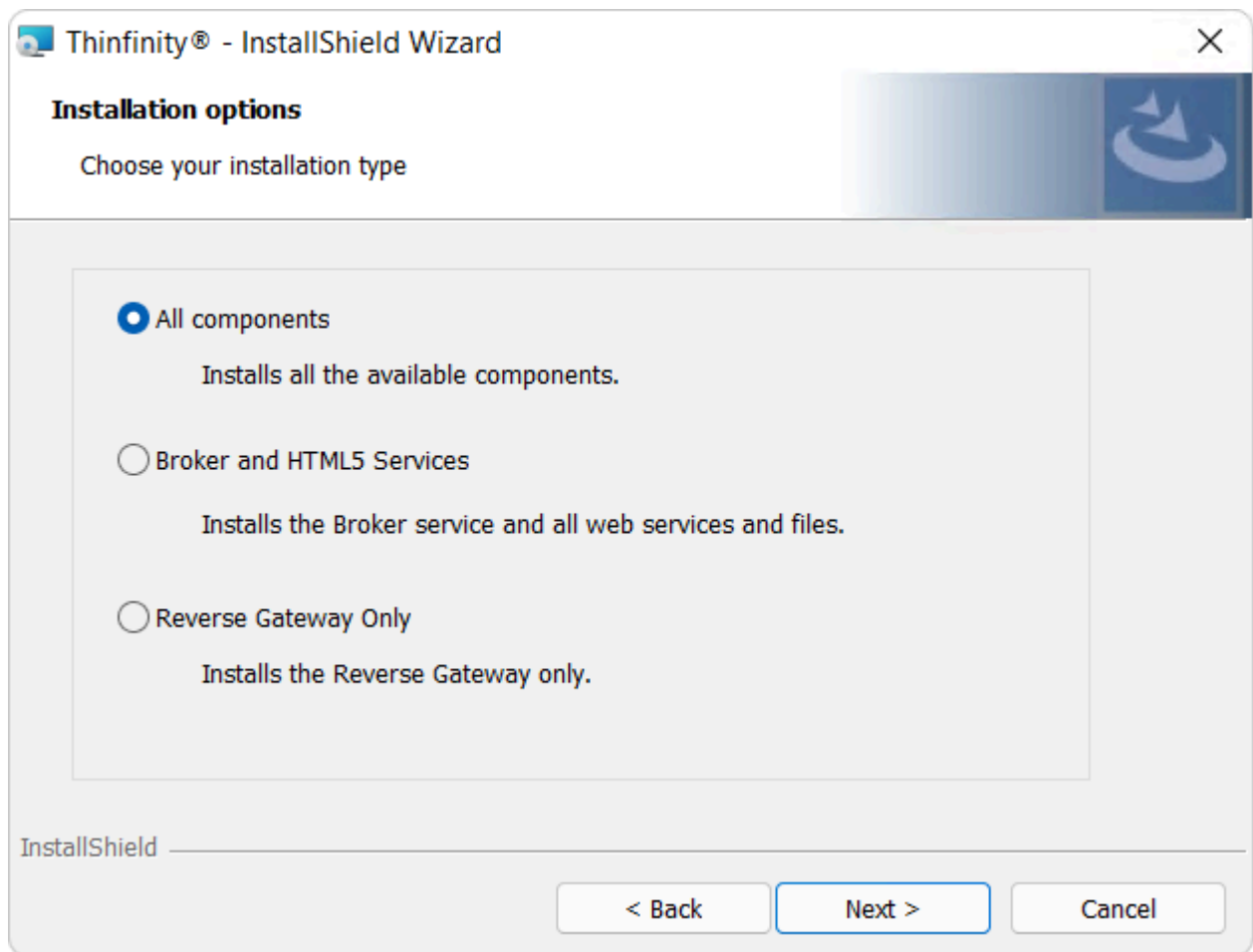
Scenario 2: Multiple Gateways and multiple Servers

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

Installing Components

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

Thinfinity® Remote Workspace has two basic services: the Broker Service and the Reverse Gateway Service.



Broker and HTML5 Services: Under this role, Thinfinity® Remote Workspace only processes forwarded connections. The Broker is responsible for establishing and processing the connections assigned by the Gateway.

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.

Reverse Gateway Service: Under this role, the Thinfinity® Remote Workspace Gateway services respond to all web-page requests and, when a connection is

solicited, it selects the appropriate Server to forward that request to.

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 Workspace Broker 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 Workspace.

Configuring a Load Balancing Scenario

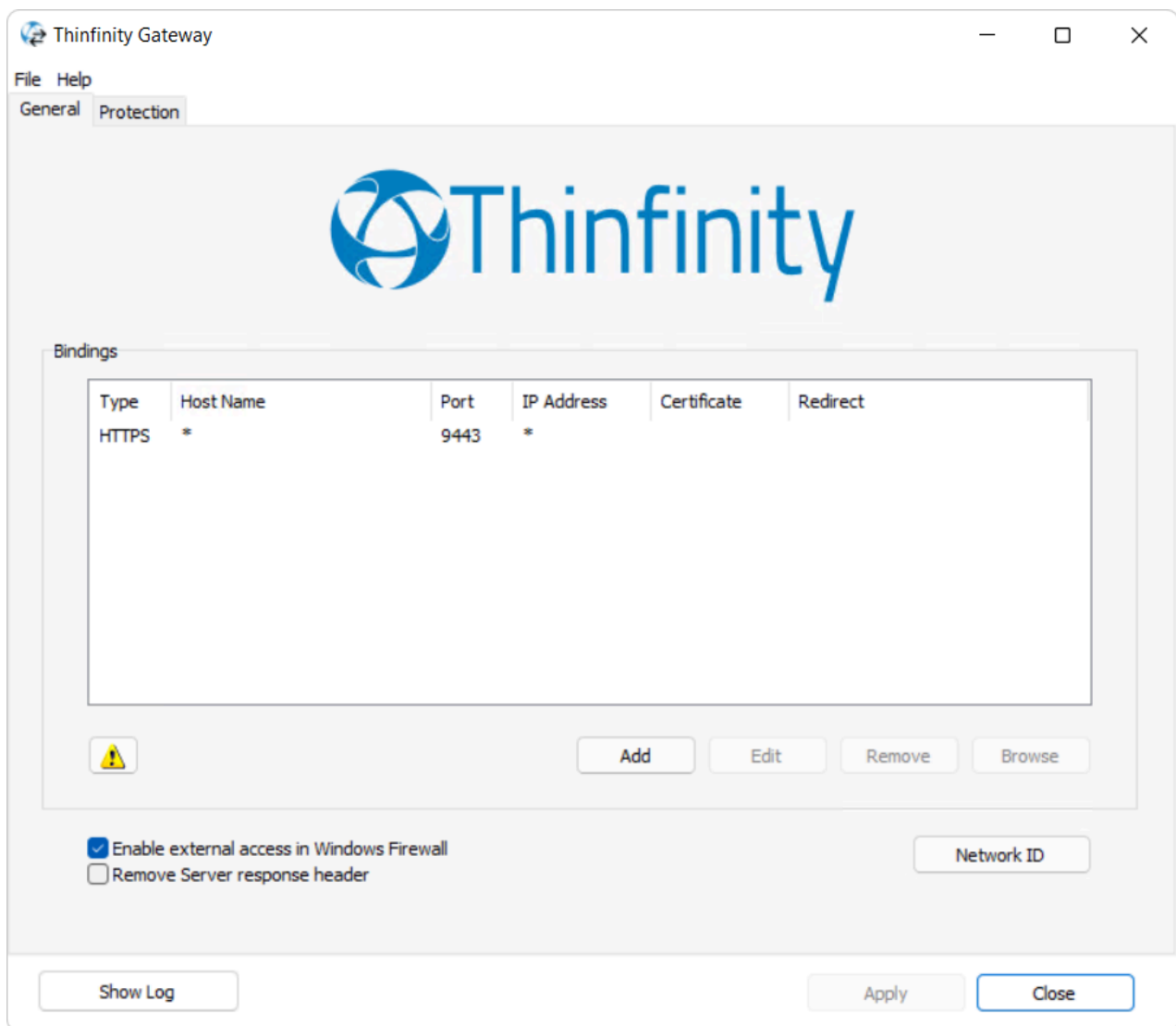
In order to configure a load balancing scenario, you need at least one Gateway installation and two Server installations.

Configuring the Gateway

Under this role, the Thinfinity® 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 Thinfinity® Gateway. 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 Workspace through a web browser.

Configuring the Server

Under this role, the Thinfinity® Remote Workspace Broker only processes forwarded connections. The Server is responsible for establishing and processing the connections assigned by the Gateway.

To configure the Server, open the Thinfinity® Configuration Manager and go the 'Broker' tab.

The screenshot shows the 'Thinfinity Configuration Manager' window with the 'Broker' tab selected. The window has a menu bar with 'File' and 'Help'. Below the menu bar are tabs for 'General', 'Broker', 'Authentication', 'Access Profiles', 'Folders', 'Permissions', 'Protection', 'Services', and 'License'. The 'Broker' tab is active, showing the following configuration options:

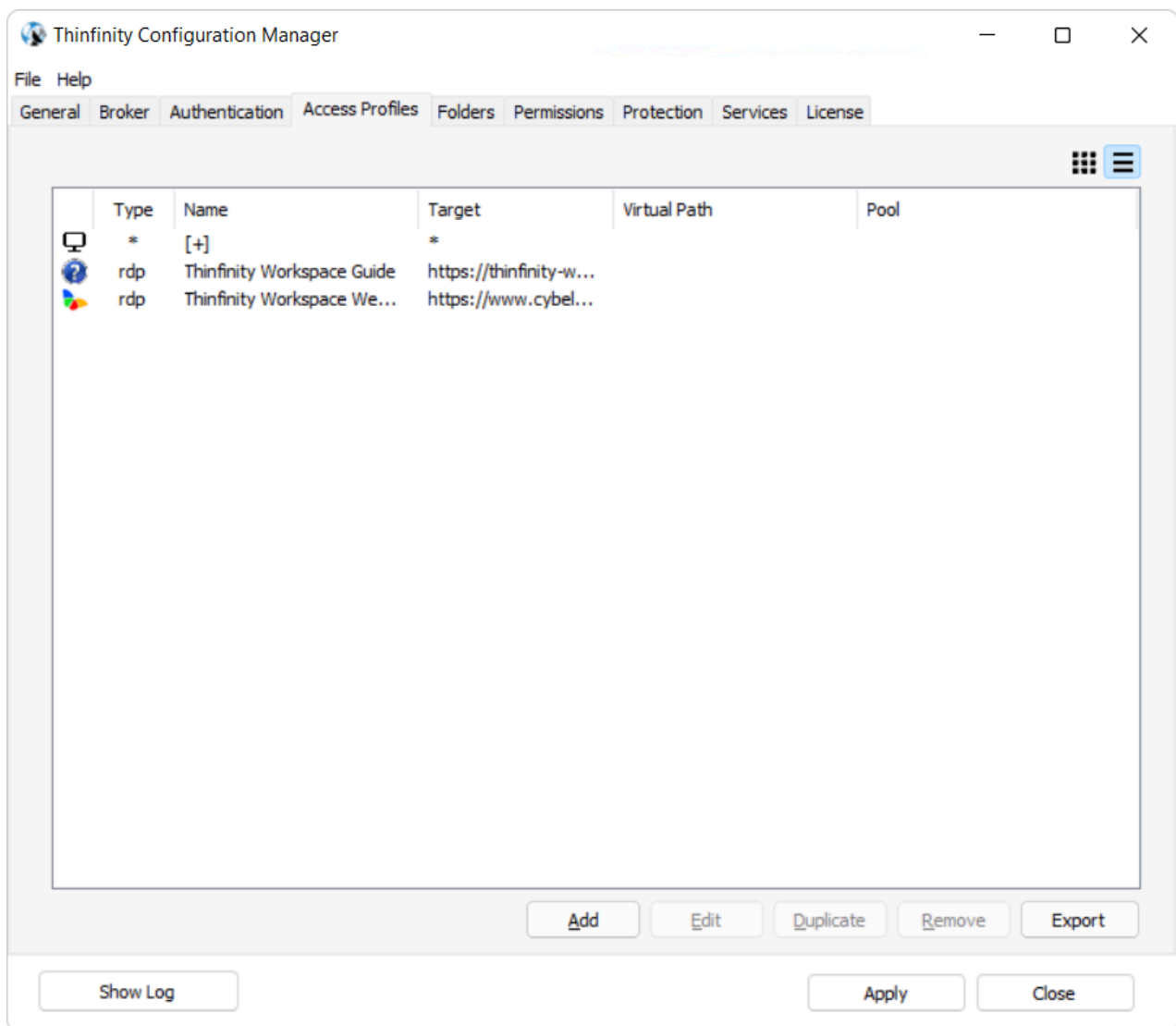
- Primary broker:** A text field with the value '10000' and a dropdown arrow, followed by the text 'per broker'.
- Secondary brokers:** A section containing a 'Pool List' table with columns 'Name', 'Users Limit', 'Load-Balancing', and 'Default'. Below the table are 'Add' and 'Remove' buttons.
- Gateways:** A section containing a 'Network ID' text field with the value '92975761-F5B3-4DC1-AD58-6D759AD30F42' and a 'Gateway List' text field with the value 'https://mygateway:9443/'. Below these fields are 'Add' and 'Remove' buttons.

At the bottom of the window are three buttons: 'Show Log', 'Apply', and 'Close'.

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 Workspace 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 click [here ↗](#) to get more information about the License Server Manager.

Read More:

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

How to configure your license

When installing Thinfinity® Remote Workspace in a Load Balancing environment you will have to install our License Server Manager in order to share you license between all your Thinfinity® Remote Workspace Brokers. Please click [here](#) ↗ to get more information about the License Server Manager.

Secondary Broker Pool

Thinfinity® Remote Workspace Secondary Brokers allow you to distribute the workload across Pools of VMs or bare-metal PCs/Servers, either RDP sessions, RFB/VNC, or SSH/Telnet.

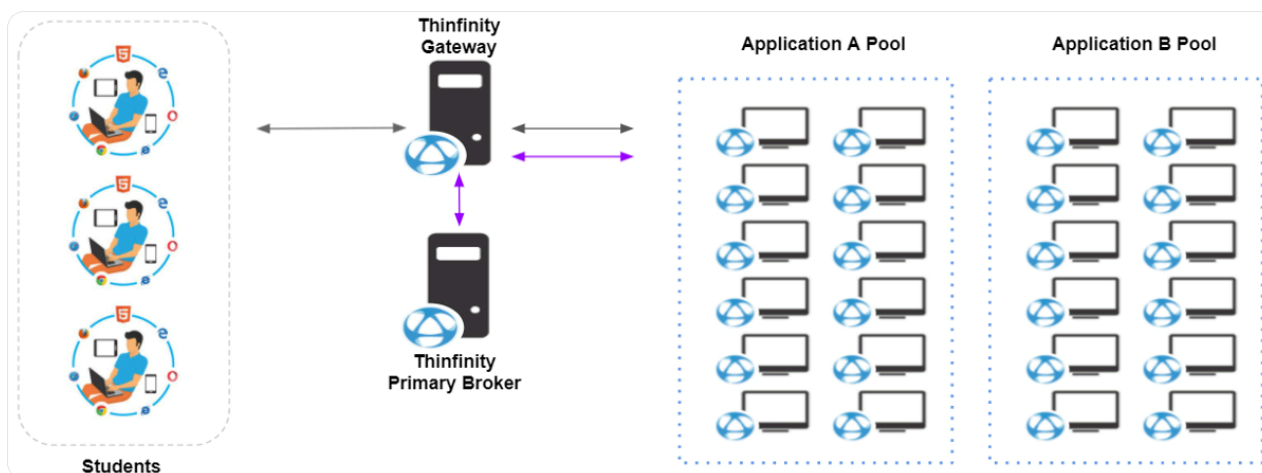
Some of the benefits of load balancing:

- Install on remote sites
- No need to open incoming ports
- Avoids overload by distributing the connections among different servers
- More reliability
- Ideal for Cloud deployments

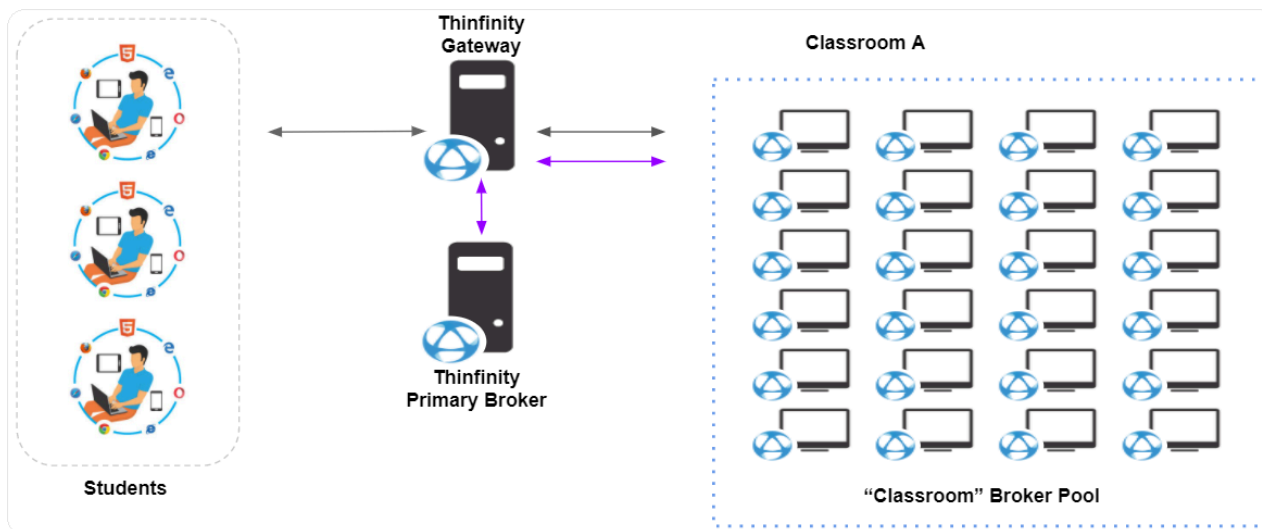
Architecture

Below you'll find some examples of which deployments benefit from using Secondary Brokers:

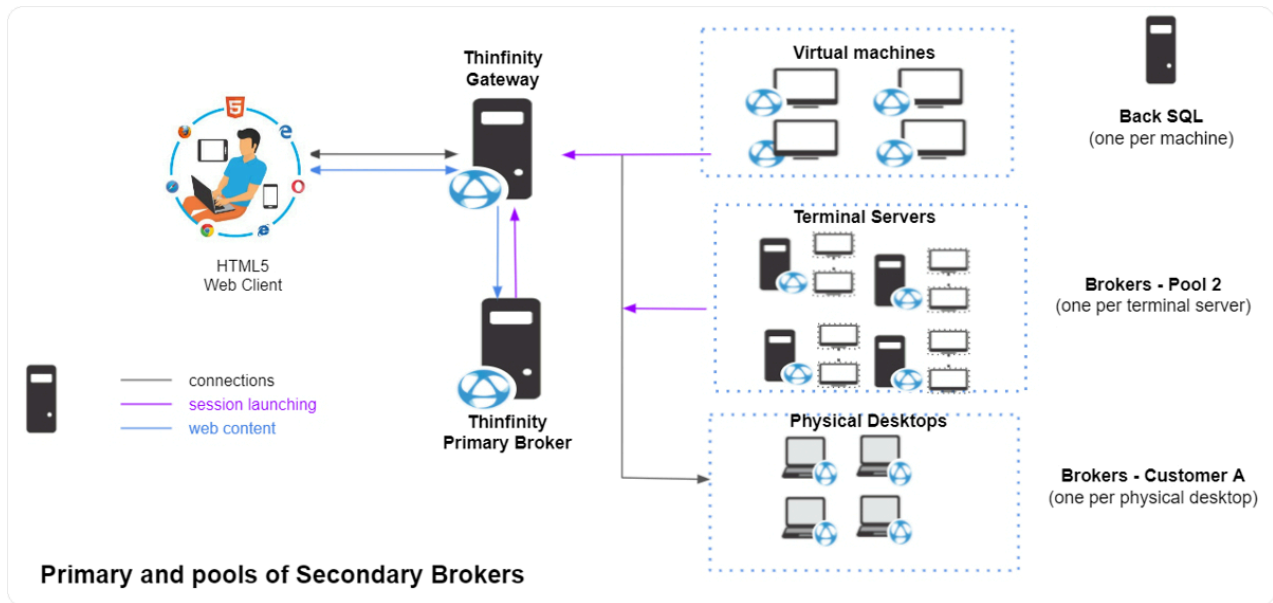
Application 'A' Pool and Application 'B' Pool



'Classroom' Example



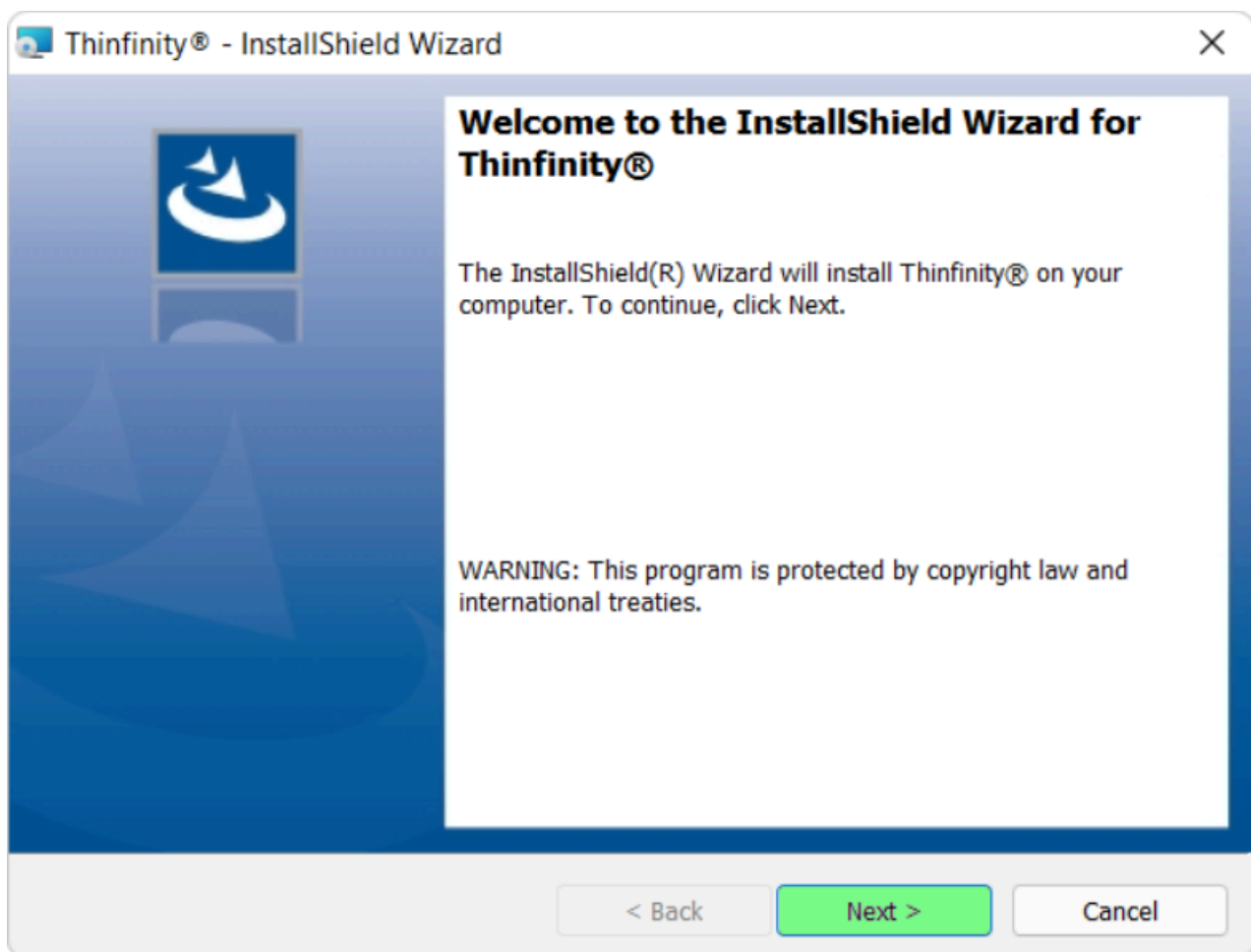
Load balancing with Secondary brokers (Cloud)



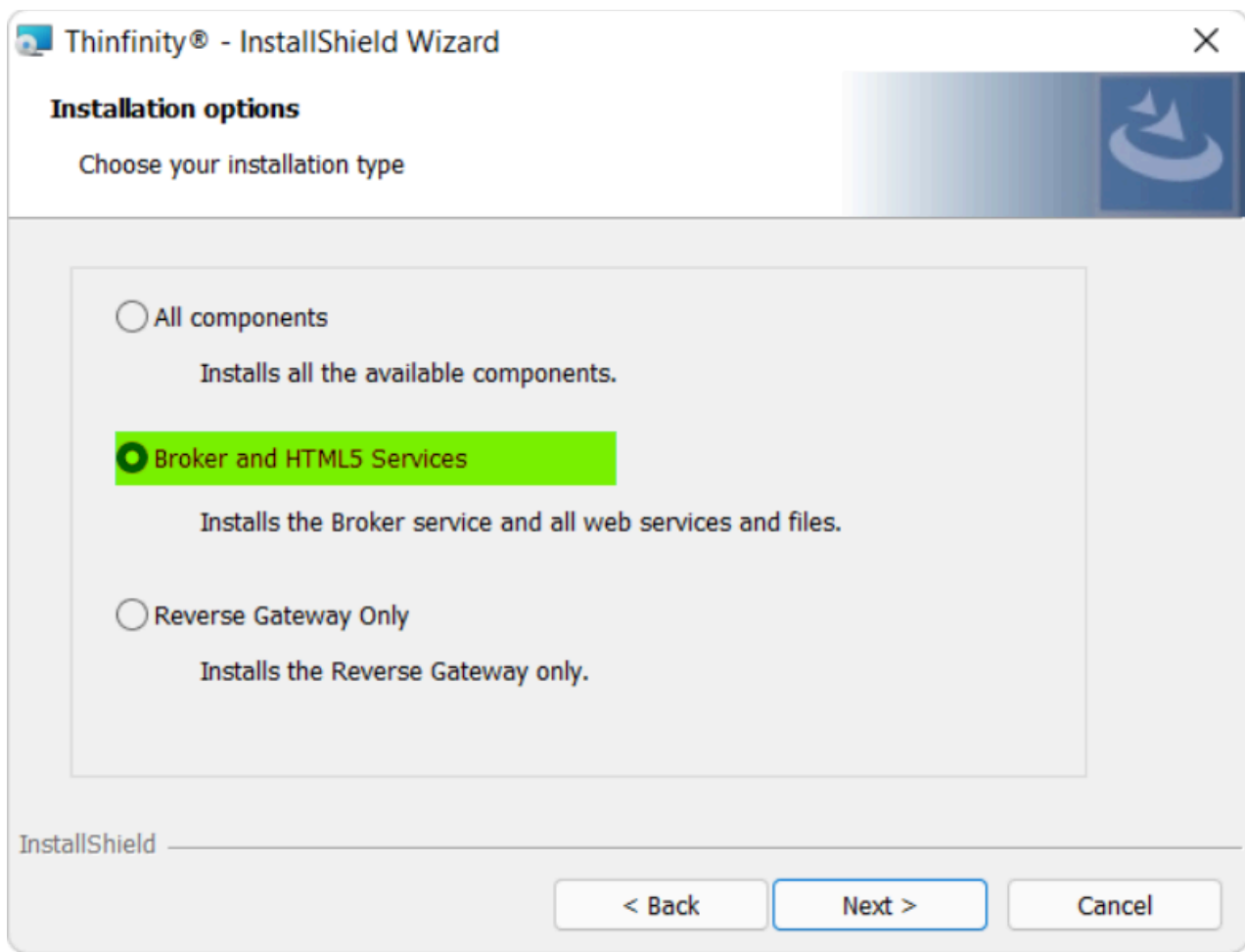
How To Install a Secondary Broker

The secondary broker is triggered by a registry key. You will have to install the broker services first and then edit a registry key to change it's behavior. Below you will find a step by step on how to configure this:

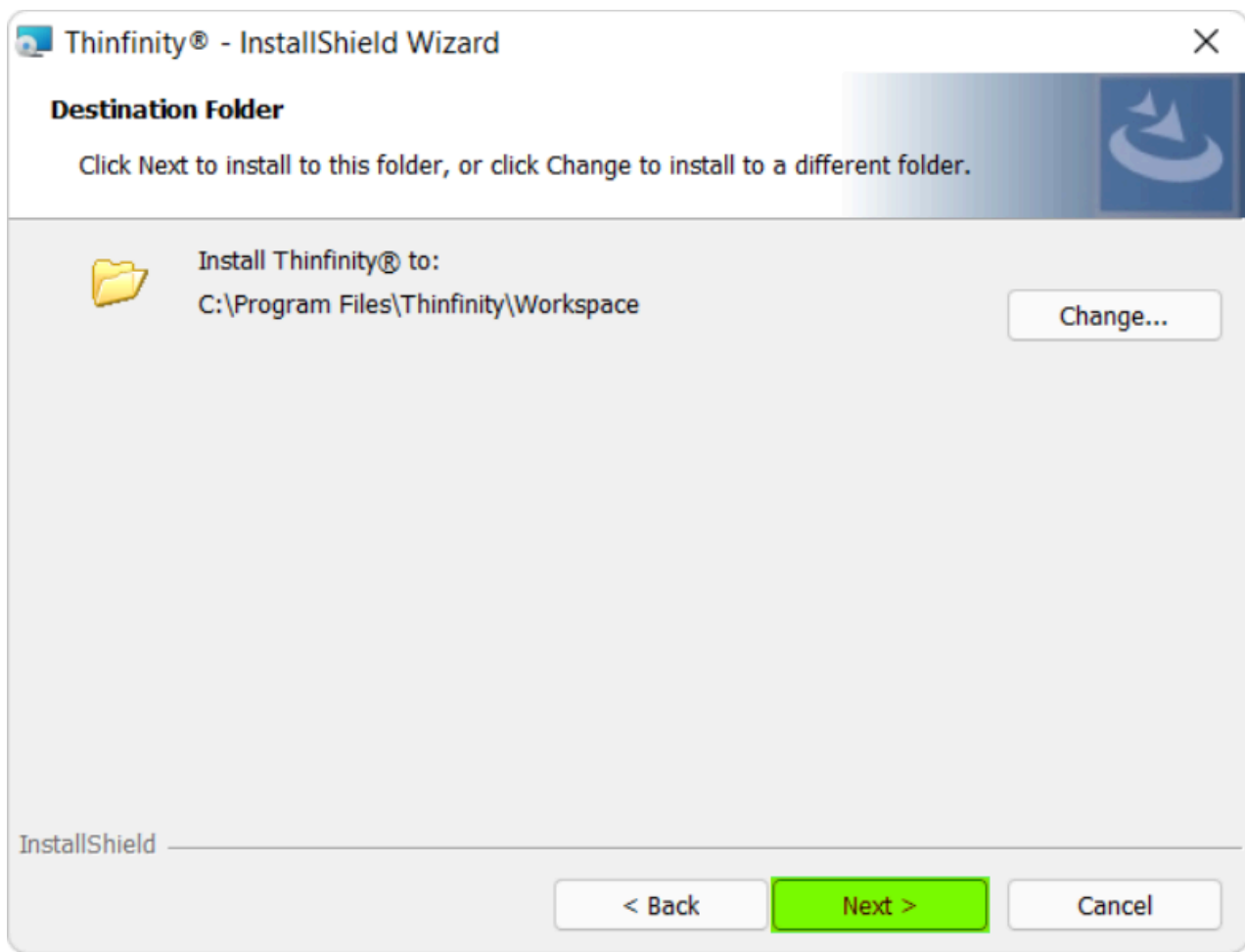
- Execute Thinfinity® Remote Workspace's Installer. Accept the License Agreement, then click on 'Next':



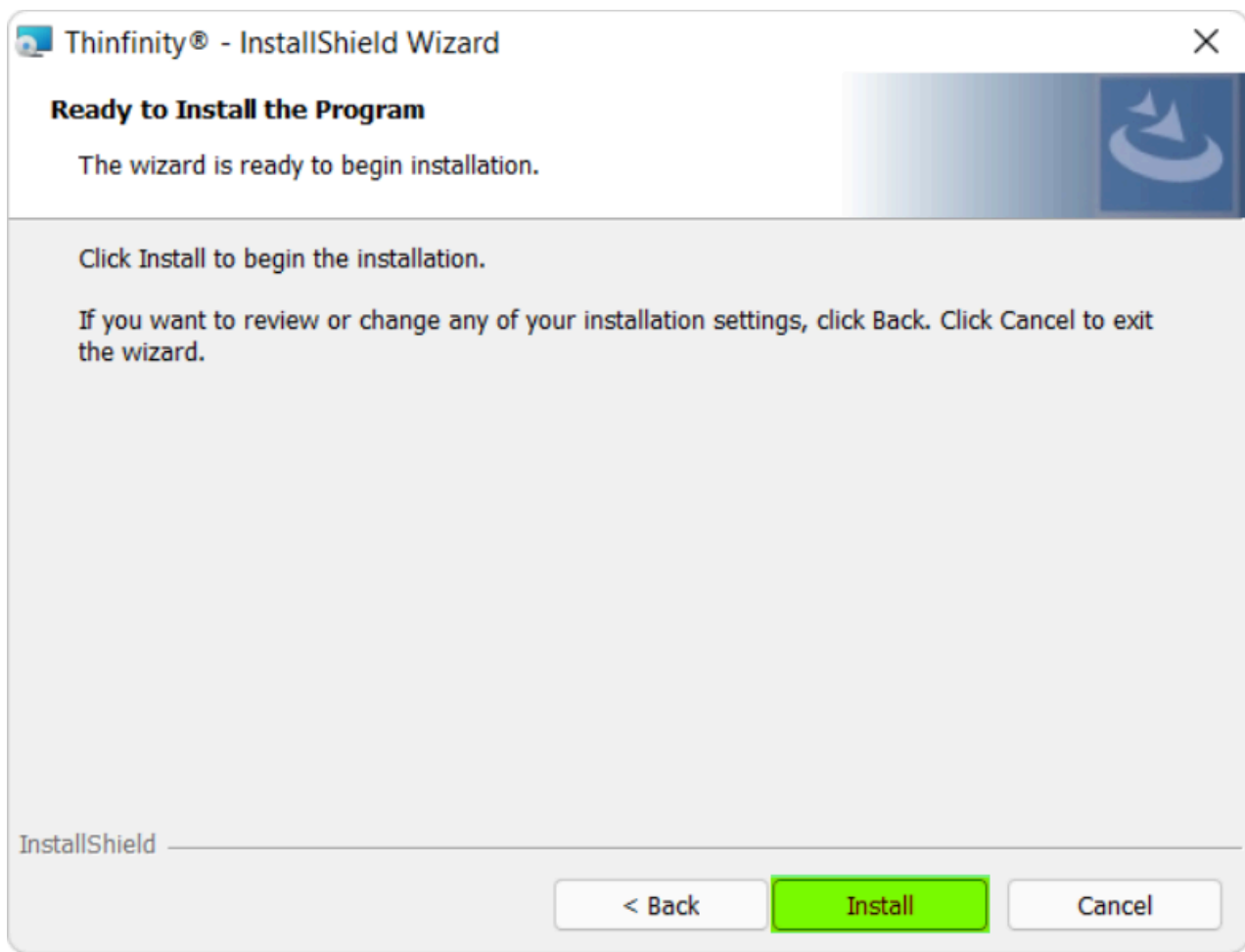
- Select the "Broker and HTML5 Services" option and click on Next:



- Select the Installation destination folder and click on Next:

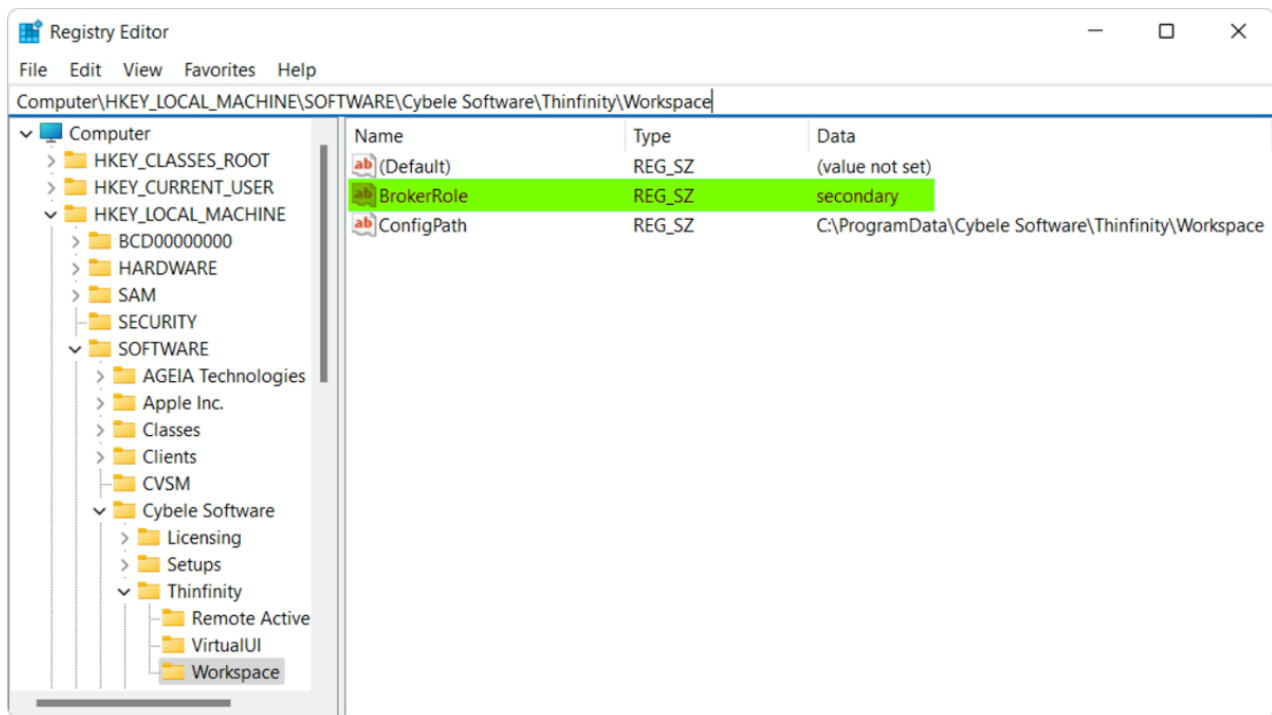


- Now, click on "Install" to install the Thinfinity® Workspace components:



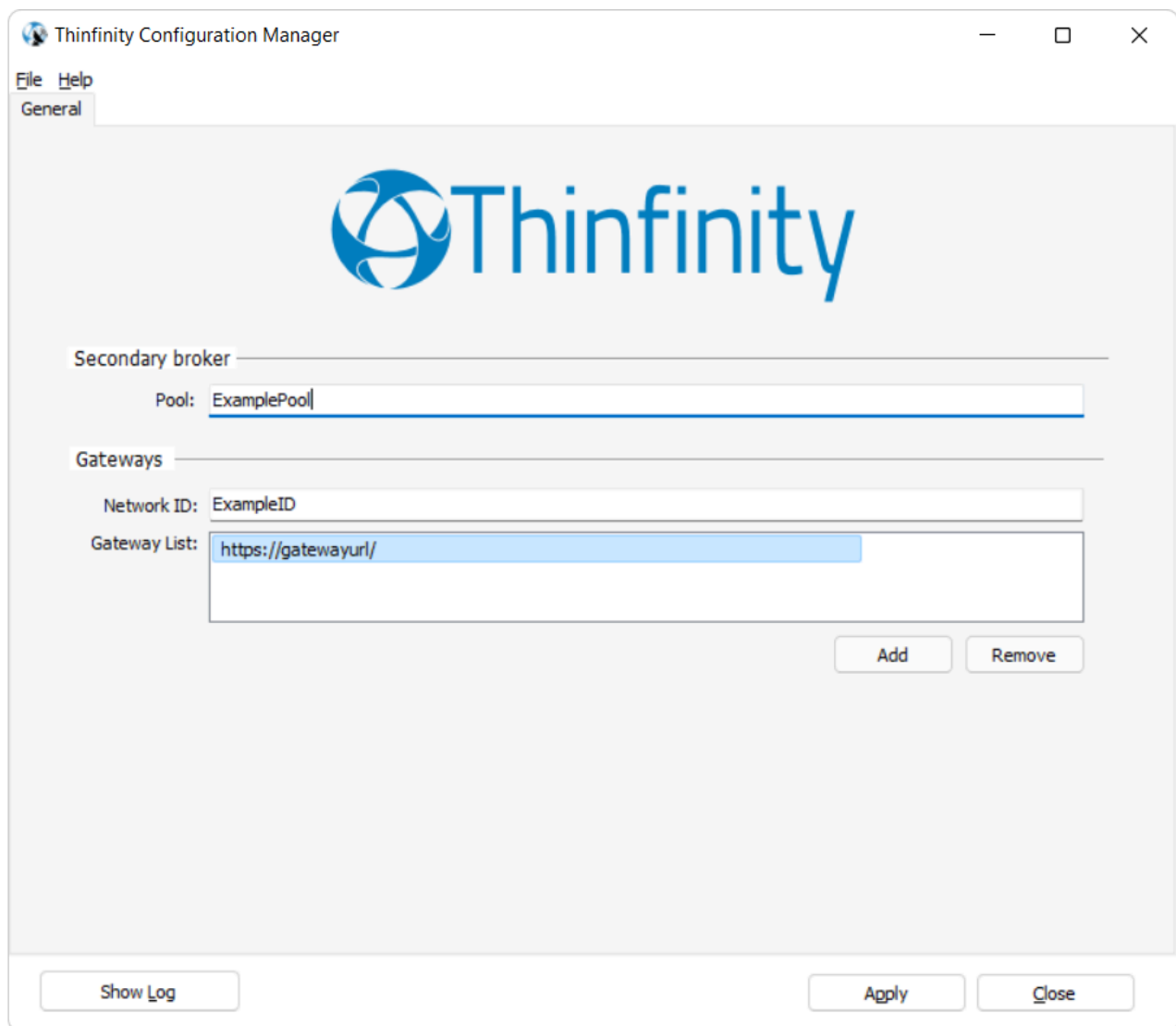
How to Enable Secondary Broker Option

- Open the registry (run: regedit) and search the following directory:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cybele
Software\Thinfinity\Workspace
- Double click on BrokerRole and replace the value primary for secondary:



Configuring Pool, NetworkID, and Gateway

- Open the Thinfinity® Configuration Manager (Start > Thinfinity > Thinfinity Configuration Manager), and configure the required parameters, Pool, NetworkID, and Gateway URL:



The screenshot shows the 'Thinfinity Configuration Manager' window with the 'General' tab selected. The window features the Thinfinity logo at the top. Below the logo, there are three main configuration sections: 'Secondary broker', 'Gateways', and a list of 'Gateways'. The 'Secondary broker' section has a 'Pool' field with the value 'ExamplePool'. The 'Gateways' section has a 'Network ID' field with the value 'ExampleID' and a 'Gateway List' field containing the URL 'https://gatewayurl/'. Below the 'Gateway List' field are 'Add' and 'Remove' buttons. At the bottom of the window are 'Show Log', 'Apply', and 'Close' buttons.

Thinfinity Configuration Manager

File Help

General

Thinfinity

Secondary broker

Pool: ExamplePool

Gateways

Network ID: ExampleID

Gateway List: https://gatewayurl/

Add Remove

Show Log Apply Close

Pool: Use this parameter to specify the pool the secondary broker will use

Network ID: Use this parameter to specify the Network environment that the secondary broker will use

Gateway List: Input the URL of the Thinfinity® Gateway. Click on "Add" and complete the URL information. Always specify the security protocol (HTTP/ HTTPS) and the connection port.

(e.g. https://My_Gateway_DNS:443 ↗)

Finally, click on Apply to save the changes.

How To Add a Pool in the Primary Broker

Firstly open the Primer Broker Server Manager.

In the '*Broker*' you will find a box called '*Secondary Brokers*'. Click '*Add*':

The screenshot shows the 'Thinfinity Configuration Manager' window with the 'Broker' tab selected. The interface includes a menu bar with 'File' and 'Help', and a tab bar with 'General', 'Broker', 'Authentication', 'Access Profiles', 'Folders', 'Permissions', 'Protection', 'Services', and 'License'. The 'Broker' tab contains three main sections: 'Primary broker', 'Secondary brokers', and 'Gateways'. The 'Primary broker' section has a 'Users Limit' of 10000 per broker. The 'Secondary brokers' section features a table with columns 'Name', 'Users Limit', 'Load-Balancing', and 'Default', and an 'Add' button. The 'Gateways' section has a 'Network ID' field with the value 'GW-1280-9031-1220' and a 'Gateway List' table with an 'Add' button. At the bottom, there are 'Show Log', 'Apply', and 'Close' buttons.

Name	Users Limit	Load-Balancing	Default
------	-------------	----------------	---------

Gateway List

General tab:

Secondary Broker Pool

General Folders

Pool name:

Users limit: per broker ☐ Default pool

Load-balancing method

☒ Breadth-First ☐ Depth-First

Breadth-first Load Balancing allows you to evenly distribute user sessions across the session hosts in a broker pool. Depth-first load balancing allows you to saturate a session host with user sessions in a broker pool.

Ok Cancel

Pool name: Add the name of the pool name you assigned to your secondary broker

Users limit: You can assign the maximum amount of users that will be able to connect to this pool

Breadth-First: Will evenly distribute the user sessions across the session hosts in a broker pool

Depth-First: Will saturate a session host with a user session in a broker pool

Folders tab:

The screenshot shows the 'Secondary Broker Pool' configuration window with the 'Folders' tab selected. The window has a title bar with a close button. Inside, there are two tabs: 'General' and 'Folders'. The 'Folders' tab contains two main sections: 'Temporary Folders' and 'Shared Folders'.

Temporary Folders:

- Root Path:** A text field containing the path `C:\Users\Public\Documents\Cybele Software\Thinfinity\Workspace\` with a browse button (three dots) to its right.
- Credentials for network shares only:** A section with two input fields: 'User name:' and 'Password:'. To the right of these fields is a 'Test' button.

Shared Folders:

- A table with three columns: 'Share Name', 'Network Path', and 'User name'. The table is currently empty.
- Below the table are three buttons: 'Add', 'Edit', and 'Remove'.

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

Root Path: Select the directory where the '*Intermediate disk*' (ThinDisk) will be stored

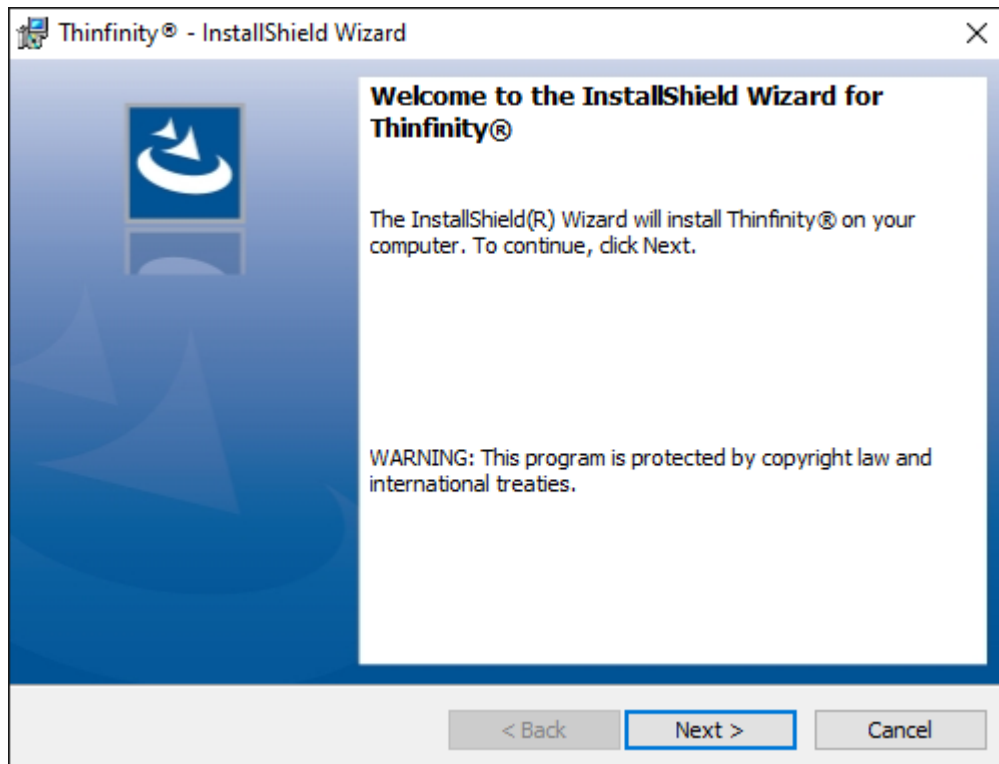
Credentials for network shares only: If you configured a UNC path as the root folder, enter a set of credentials that has access to this path

Shared Folders: Create a shared folder in which all your users will be able to interact with

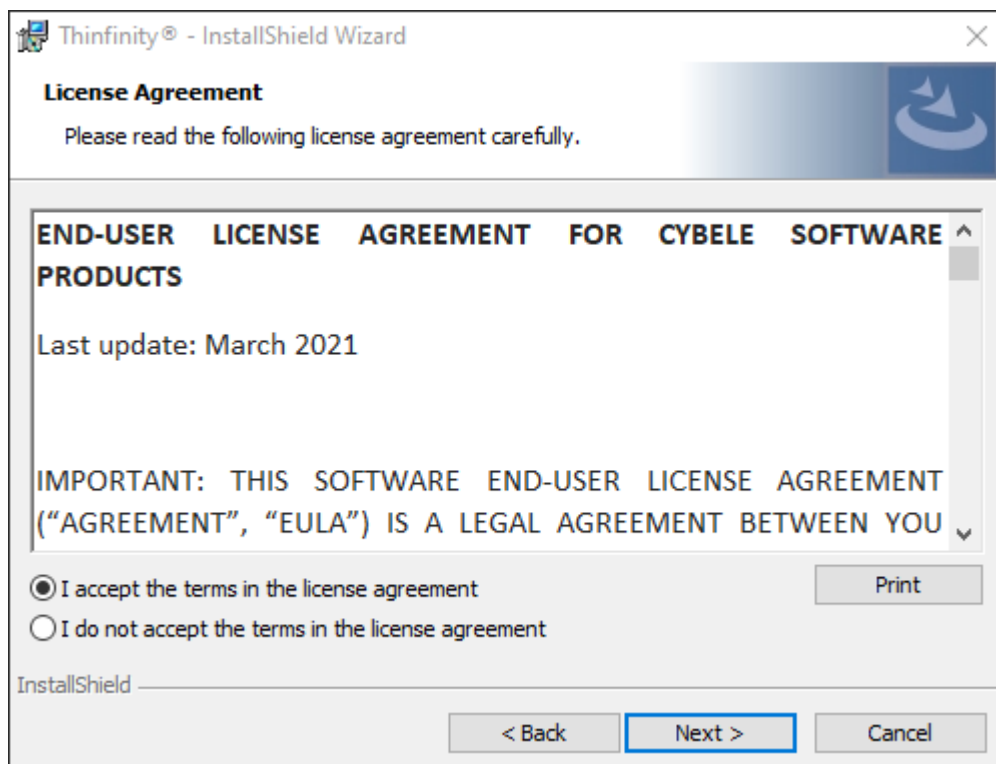
Agent Mode

Installation

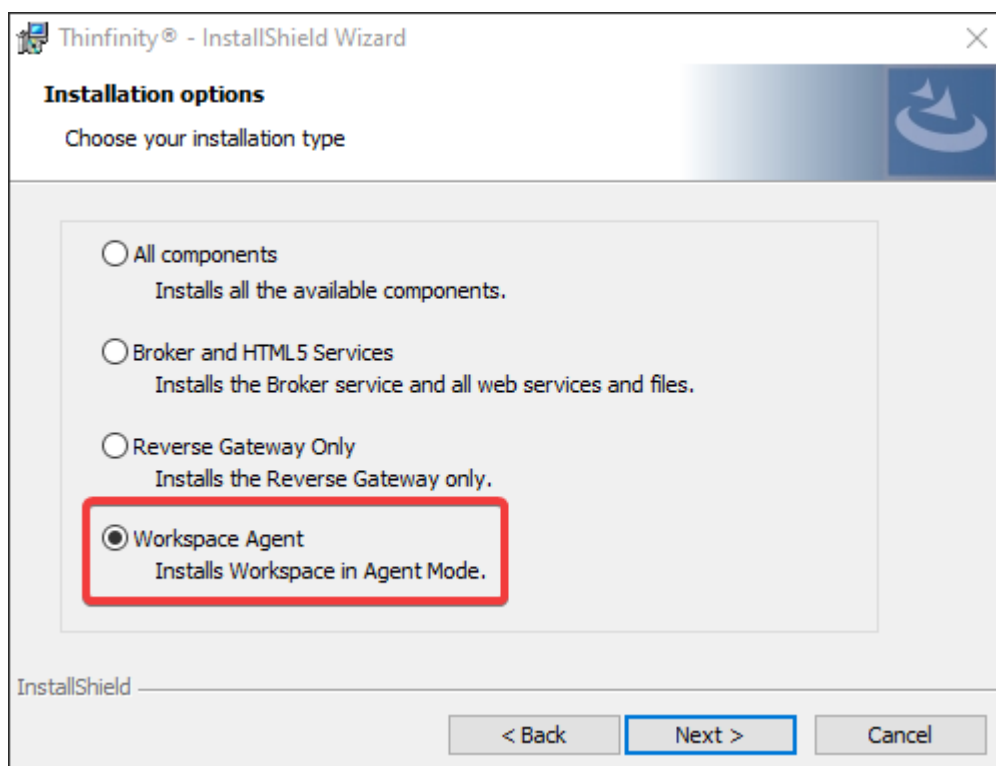
The installation process is similar to the rest of the modes. Firstly, we have to run the installer. You will be welcomed with this screen. We will click on "Next".



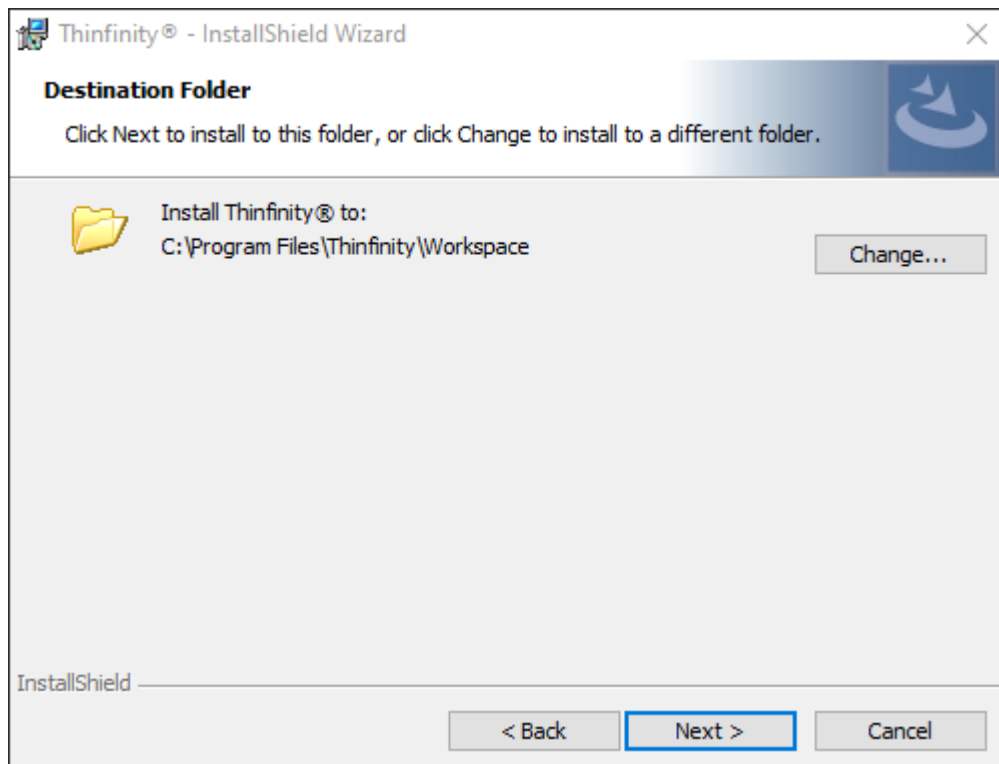
After this, we will be prompted with the License Agreement. Please, read it carefully, and if you accept the terms of the agreement, click on next.



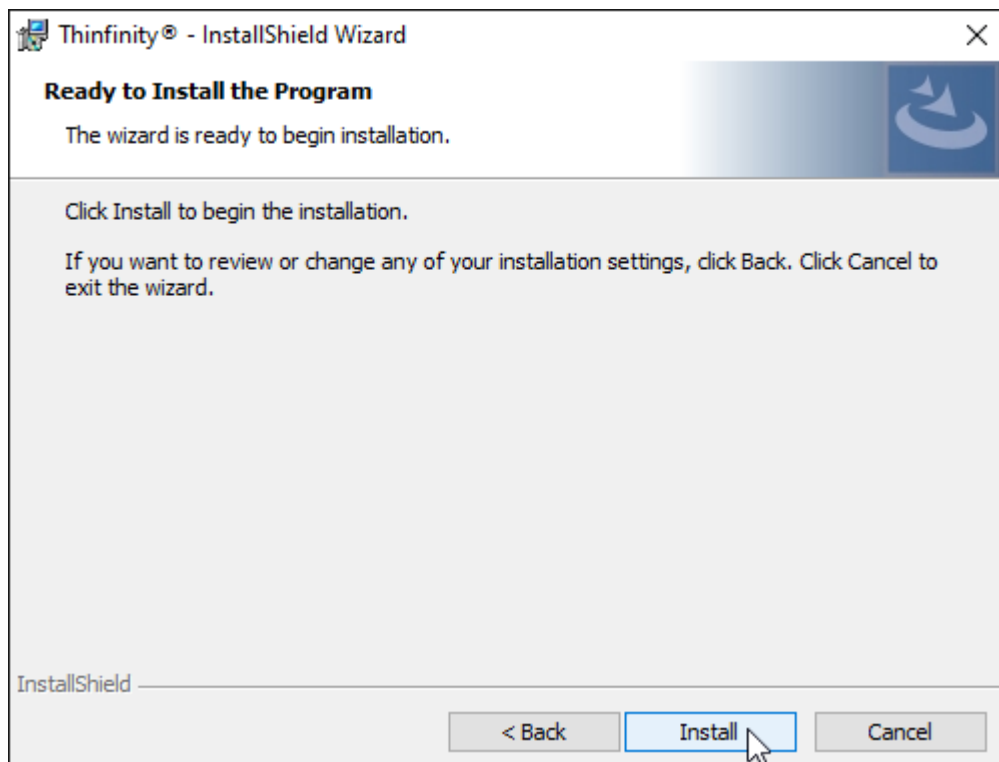
Once we've accepted the agreement, we will need to choose the Installation mode. We have to select "Workspace Agent" and click on next.

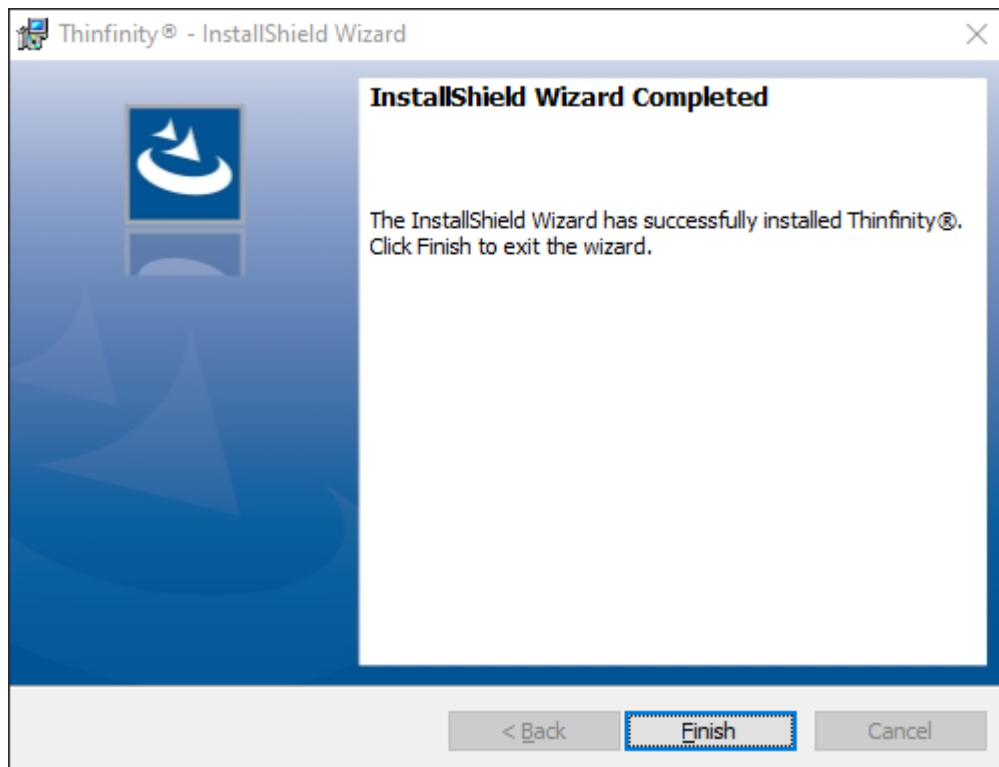


After this, we will select the installation path for the agent. The default path is **C:\Program Files\Thinfinitiy\Workspace**



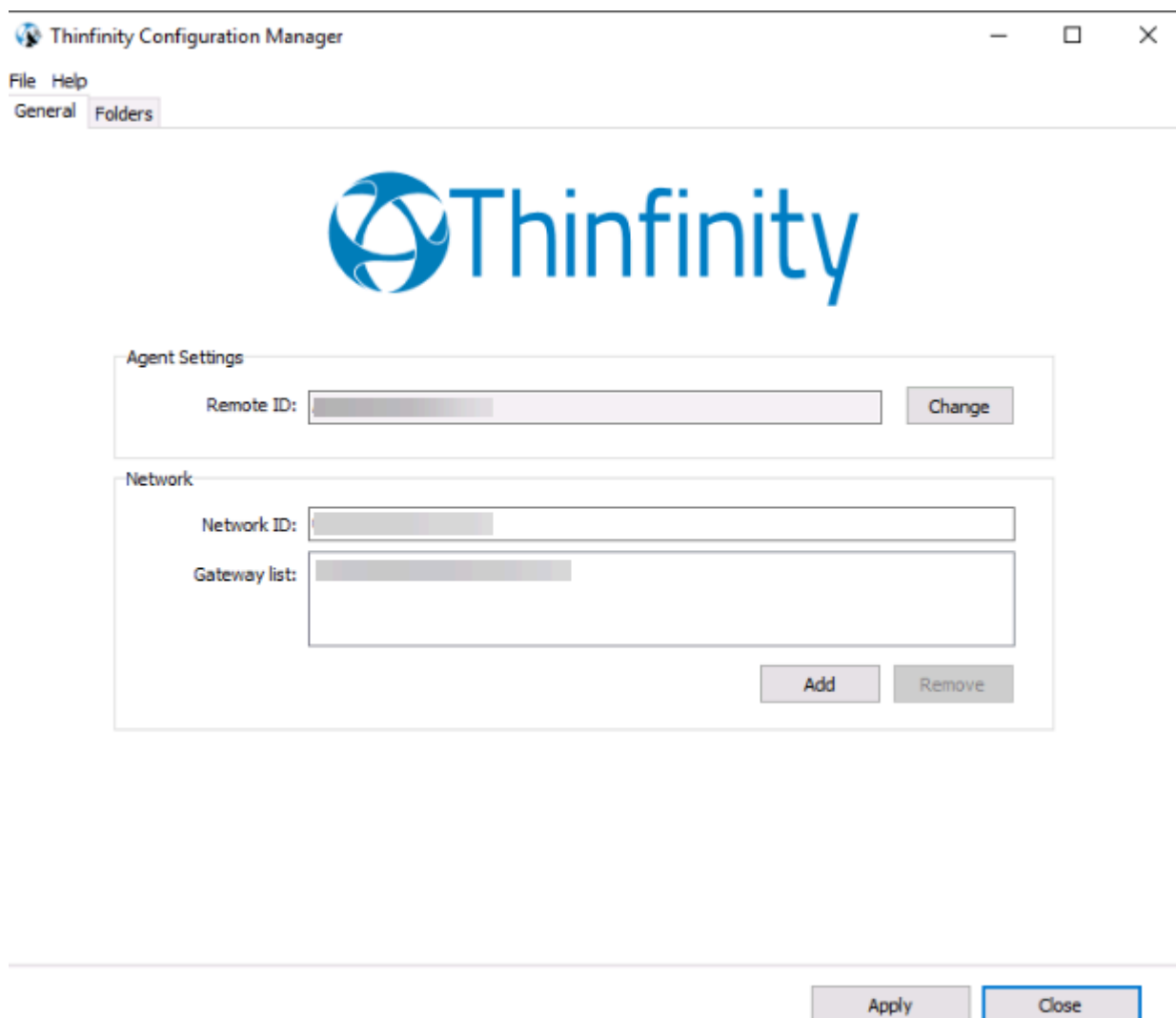
Lastly, we will click on "Install".





Configuration

Thinfinity Remote Workspace Agent allows you to create an RDP connection that doesn't require opening any inbound ports. There are three parameters you will need to configure the Thinfinity Remote Workspace Agent to register it to your main Thinfinity Remote Workspace Broker (Primary).



The screenshot shows the 'Thinfinity Configuration Manager' window. The title bar includes the application name and standard window controls. Below the title bar is a menu bar with 'File' and 'Help'. A tab bar at the bottom of the menu shows 'General' and 'Folders', with 'Folders' being the active tab. The main content area features the Thinfinity logo at the top. Below the logo, there are two sections: 'Agent Settings' and 'Network'. The 'Agent Settings' section contains a 'Remote ID' text field with a 'Change' button to its right. The 'Network' section contains a 'Network ID' text field, a 'Gateway list' text area, and 'Add' and 'Remove' buttons at the bottom right. At the bottom of the window, there are 'Apply' and 'Close' buttons.

REMOTE ID [String]: This value identifies your computer/server (Where the agent is installed). Thinfinity® creates a random ID automatically, it could be modified using *any* alphanumeric value.

NETWORK ID [String]: The Network ID identifies this installation. Any Thinfinity® Remote Workspace servers that want to share their resources through one or more Gateways must match their Network ID.

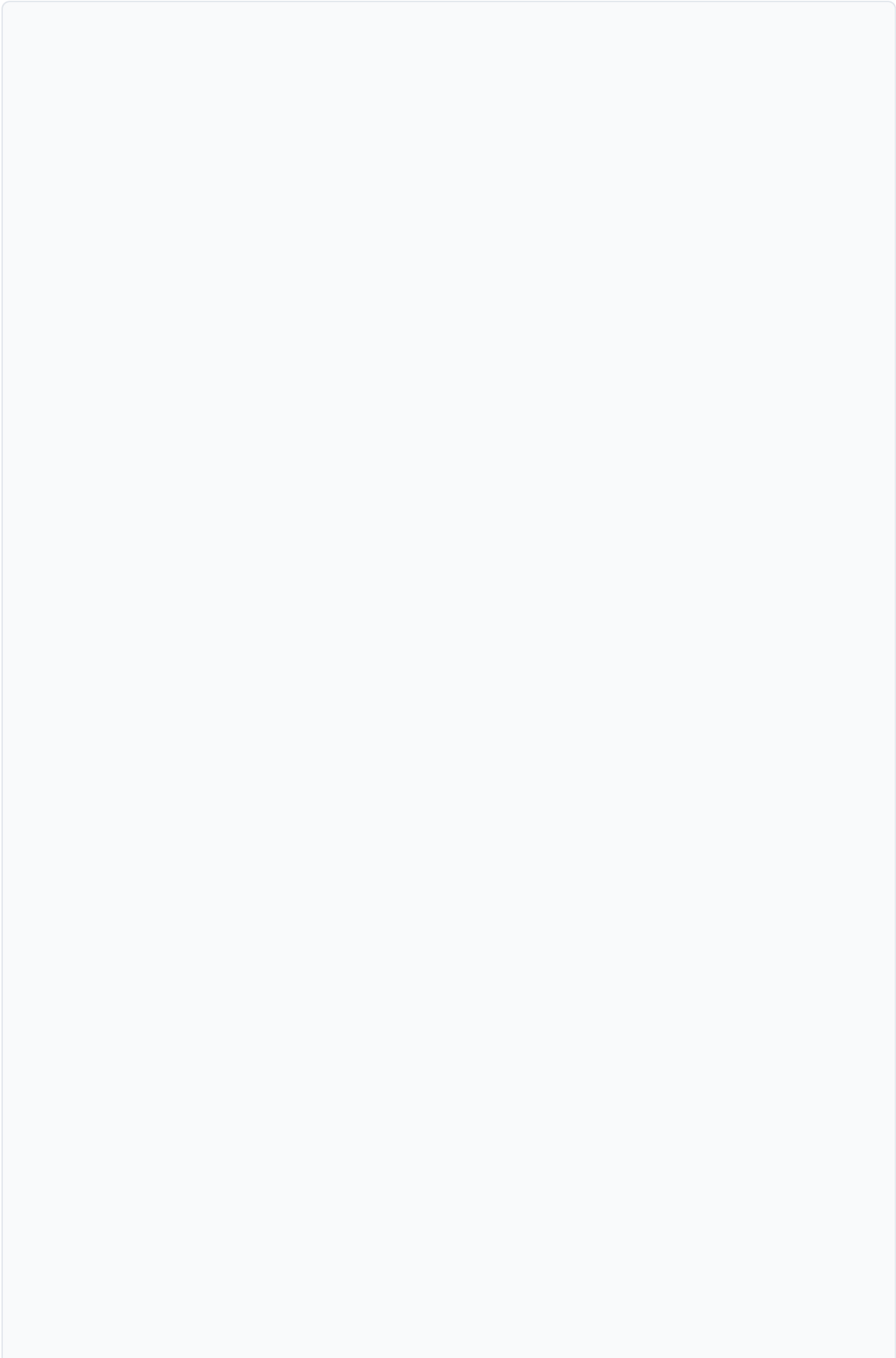
GATEWAY (List) [HTTP(S)://ip:port]: It is the gateway/s URL that the agent will use to generate the connection. You should add at least one gateway URL, or you can add more than one for a redundant environment.

Automation script for parameters configuration

Thinfinity® Remote Workspace Agent allows you to add the parameters required to register that component into a Thinfinity Workspace solution. When you create a Virtual Machine, you will need to add the following script (in the [Custom Data ↗](#)) codified into base 64 in your custom [data: ↗ ↗](#)

```
{
  "thinfinity": {
    "networkId": "networkId",
    "gatewayUrls": [
      "GatewayURL"
    ],
    "agent": {
      "remoteId": "{COMPUTERNAME}@{IPAddress}"
    }
  }
}
```

NetworkId: your deployment's network ID
Gateway URL: your gateway/s URL
Computername: it takes the name and the IP from the ComputerThe format of the JSON file which can be passed as custom data, user data, or as an argument to any of the binaries, is as follows:




```
{
  "thinfinity": {
    "binding": [
      {
        "https": true,
        "ip": "",
        "port": 443,
        "hostName": "127-0-0-1.thinrdp.net",
        "certificateStore": "MY",
        "thumbprint": "ab-cd-ef-gh-ij-kl",
        "redirectUrl": "",
        "redirectCode": 0
      },
      {
        "https": false,
        "ip": "",
        "port": 80,
        "hostName": "127-0-0-1.thinrdp.net",
        "redirectUrl": "https://127-0-0-1.thinrdp.net/",
        "redirectCode": 302
      }
    ],
    "networkId": "set-by-a-script-file",
    "gatewayUrls": [
      "https://127-0-0-1.thinrdp.net/",
      "https://25-95-118-105.thinrdp.net/"
    ],
    "commGatewayUrls": [
      "http://25.87.240.213:8443/",
      "http://25.87.240.214:8443/"
    ],
    "apiKey": "this-is-my-apikey",
    "protection": {
      "bruteForce": {
        "enabled": true,
        "maxAttempts": 3,
        "minutesToReset": 10
      },
      "whiteList": [
        "192.168.1.*"
      ],
      "blackList": [
        "192.168.2.*"
      ]
    },
    "broker": {
      "accessKey": "{InstanceID}-{ComputerName}",
      "master": false,

```

```

        "poolName": "Batch-Pool"
    },
    "agent": {
        "remoteId": "{InstanceID}-{ComputerName}",
        "password": "scripted-agent-password"
    },
    "vnc": {
        "remoteId": "{InstanceID}-{ComputerName}",
        "password": "scripted-vnc-password",
        "options": {
            "enableLanWanAccess": true,
            "certificate": {
                "certificateFile": "",
                "rootCAFile": "",
                "privateKeyFile": "",
                "passPhrase": ""
            },
            "vnc": true,
            "ft": true
        },
        "authentication": {
            "name": "None",
            "username": "",
            "password": "",
            "ntlmUsers": ""
        },
        "permissions": {
            "view": {
                "prompt": true,
                "promptSecsTimeout": 5,
                "inactivityMinsTimeout": 10,
                "allowOnPromptTimeout": true
            },
            "control": {
                "prompt": true,
                "promptSecsTimeout": 5,
                "inactivityMinsTimeout": 10,
                "allowOnPromptTimeout": true
            }
        },
        "protection": {
            "level": 0,
            "password": ""
        }
    }
}

```

In case of using the setup by command line, you have to call the executable in one of the following ways:

1. **`/SetInstance "C:\Thinfinity-config-JSON-Path\Thinfinity.json"`**
2. **`/SetInstance json-element-1-path=element-1-value ... json-element-N-path=element-N-value`**

Examples:

- `/SetInstance network.id=my-secret-network-id`
`"gatewayUrls=https://gw1.domain.com;https://gw2.domain.com ↗"`
`binding.https=false binding.port:8080`

In this case, you can also add one binding. Instead, using a file, you can add more than one since it is an array of bindings.

- `/SetInstance network.id=my-secret-network-id`
`"gatewayUrls=https://gw1.domain.com" broker.id={InstanceID}`
`broker.master=false broker.poolName=PrivatePool-1`

This sets the broker as secondary and named **PrivatePool-1**, connecting to the gw1.domain.com ↗ gateway using the networkID **my-secret-network-id**

Integrating Thinfinity® Remote Workspace Section

Integrating Thinfinity® Remote Workspace

Thinfinity® Remote Workspace was designed to interoperate with many different applications.

Find below the ways you can integrate Thinfinity® Remote Workspace with other applications:

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

[Integrating Thinfinity® Remote Workspace 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 Workspace 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.

External Authentication

Thinfinity® Remote Workspace 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 Workspace.

How to authenticate against Thinfinity® Remote Workspace from external applications:

The authentication against Thinfinity® Remote Workspace can be done using:

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

Every time you call Thinfinity® Remote Workspace, 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`

Encryption:

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

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

[OAuth/2](#)

ApiKey

The ApiKey is a secret value, known only by Thinfinity® Remote Workspace 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 Workspace 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 Workspace ini configuration file. The location of this file depends on the Windows version Thinfinity® Remote Workspace is running at:

C:\ProgramData\Cybele Software\Thinfinity\Workspace\DB\settings.ini

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

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

You should use a personal value for the ApiKey setting, as long as it follows the pattern shown above in the 'Key' parameter and matches the value sent by the external application.

Do not use the example value shown above, as this content is public on the internet.

Filter access. Grant access to a set of desired ips by adding them in the 'Ips' parameter. This will restrict the rest of ips from connecting.

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

Customizing the Web Interface

Customizing the Web Interface

Thinfinity® Remote Workspace 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.

Changing the Logo

Modifying the application logo can be as simple as copying the new logo image and telling Thinfinity® Remote Workspace application where it is located:

1. Create a folder called "BrandingFiles", if it doesn't exist yet, in the 'web' folder located inside the Thinfinity® Remote Workspace installation directory (C:\Program Files\Thinfinity\Remote Workspace\web)

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

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

A. Create a file called "WebAliases.ini" in the following directory :

C:\Program Files\Thinfinity\Remote Workspace\bin64.

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.

Customizing the Web Files

Modifying the application logo can be as simple as copying the new logo image and telling Thinfinity® Remote Workspace application where it is located:

1. Create a folder called "BrandingFiles", if it doesn't exist yet, in the 'web' folder located inside the Thinfinity® Remote Workspace installation directory (C:\Program Files\Thinfinity\Remote Workspace\web)

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

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

A. Create a file called "WebAliases.ini" in the following directory :

C:\Program Files\Thinfinity\Remote Workspace\bin64.

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.

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 web structure. Read next, how each option will behave differently.

Inside the web :

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 web 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](#).

« Remote Desktop Server » web ↕ ↺ 🔍 Search web

Name	Date modified	Type	Size
BrandingFiles	10/21/2020 11:13 ...	File folder	
common	10/15/2020 10:38 ...	File folder	
css	10/15/2020 10:38 ...	File folder	
css.m	10/15/2020 10:38 ...	File folder	
images	10/15/2020 10:38 ...	File folder	
js	10/15/2020 10:38 ...	File folder	
rdp	10/15/2020 10:38 ...	File folder	
rfb	10/15/2020 10:38 ...	File folder	
smb	10/15/2020 10:38 ...	File folder	
themes	10/15/2020 10:38 ...	File folder	
zsc	10/15/2020 10:38 ...	File folder	
401.html	10/10/2020 8:06 PM	Chrome HTML Do...	2 KB
402.html	10/10/2020 8:06 PM	Chrome HTML Do...	2 KB
403.html	10/10/2020 8:06 PM	Chrome HTML Do...	2 KB
404.html	10/10/2020 8:06 PM	Chrome HTML Do...	2 KB
409.html	10/10/2020 8:06 PM	Chrome HTML Do...	2 KB
500.html	10/10/2020 8:06 PM	Chrome HTML Do...	2 KB
admin.html	10/10/2020 8:10 PM	Chrome HTML Do...	6 KB
admin.min.js	10/10/2020 8:09 PM	JavaScript File	621 KB
browser.capabilities.min.js	10/10/2020 8:09 PM	JavaScript File	149 KB
browserCapabilities.html	10/10/2020 8:10 PM	Chrome HTML Do...	2 KB
customSettings.js	10/10/2020 8:09 PM	JavaScript File	1 KB
customSettings.rdp.js	10/10/2020 8:09 PM	JavaScript File	3 KB

Outside the web:

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
```

Web Services API

The Web Services API is intended to allow external applications to access and manipulate some of Thinfinity® Remote Workspace data and settings.

Thinfinity® Remote Workspace has two different Web Services available:

a. Profiles Web Service:

If you need to manipulate Thinfinity® Remote Workspace 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 at the section that explains its use and behavior.

b. Analytics Web Service:

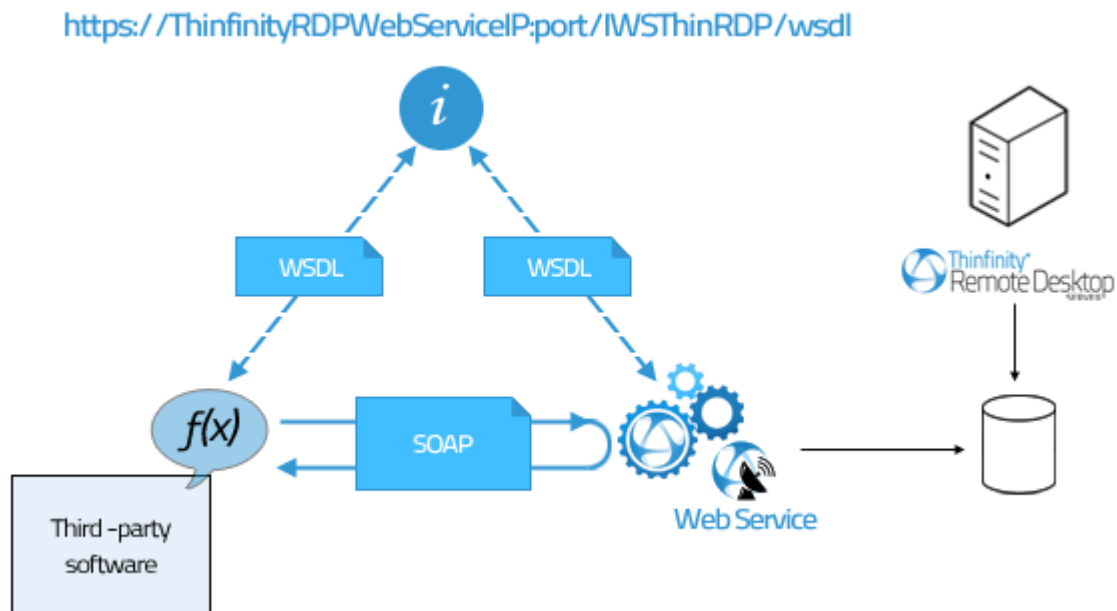
The Thinfinity® Remote Workspace Analytics feature is included since version 2.0.0.16. This feature keeps statistic data of Thinfinity® Remote Workspace logins, sessions, connections and used browsers. The [Analytics Web Service](#) allows external applications to access this information.

Requirements for the Web Service API:

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 Workspace Web Service interface.

Architecture

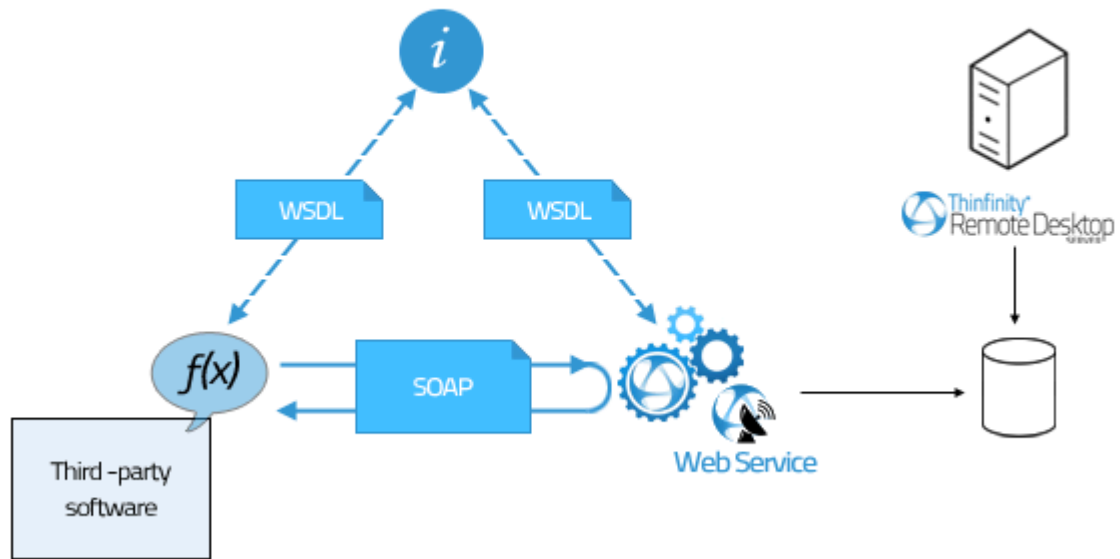
The Thinfinity® Remote Workspace Web Service architecture is illustrated in the image below:



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 Workspace on the following address, once the Web Service is installed:

<https://ThinfinityRDPWebServiceIP:port/IWSThinRDP/wsdl>

<https://ThinfinityRDPWebServiceIP:port/IWSThinRDP/wsdI>



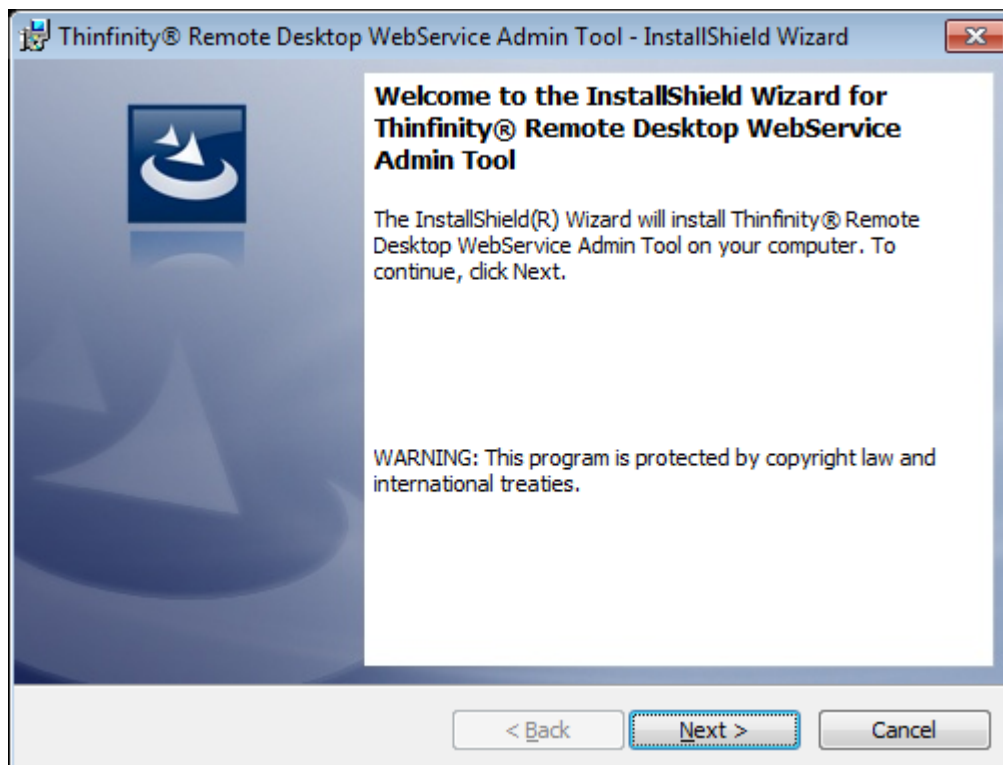
Installing the Web Service

The first step to start developing the integration with Thinfinity® Remote Workspace 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 Workspace is installed.



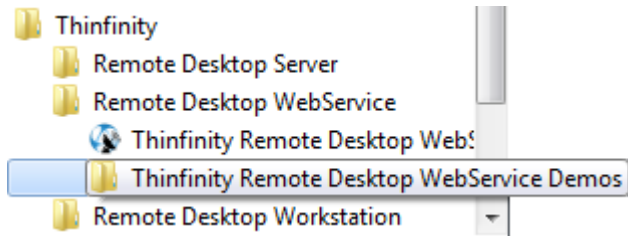
3. Besides installing the Web Service, the installer will also:

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

* 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.



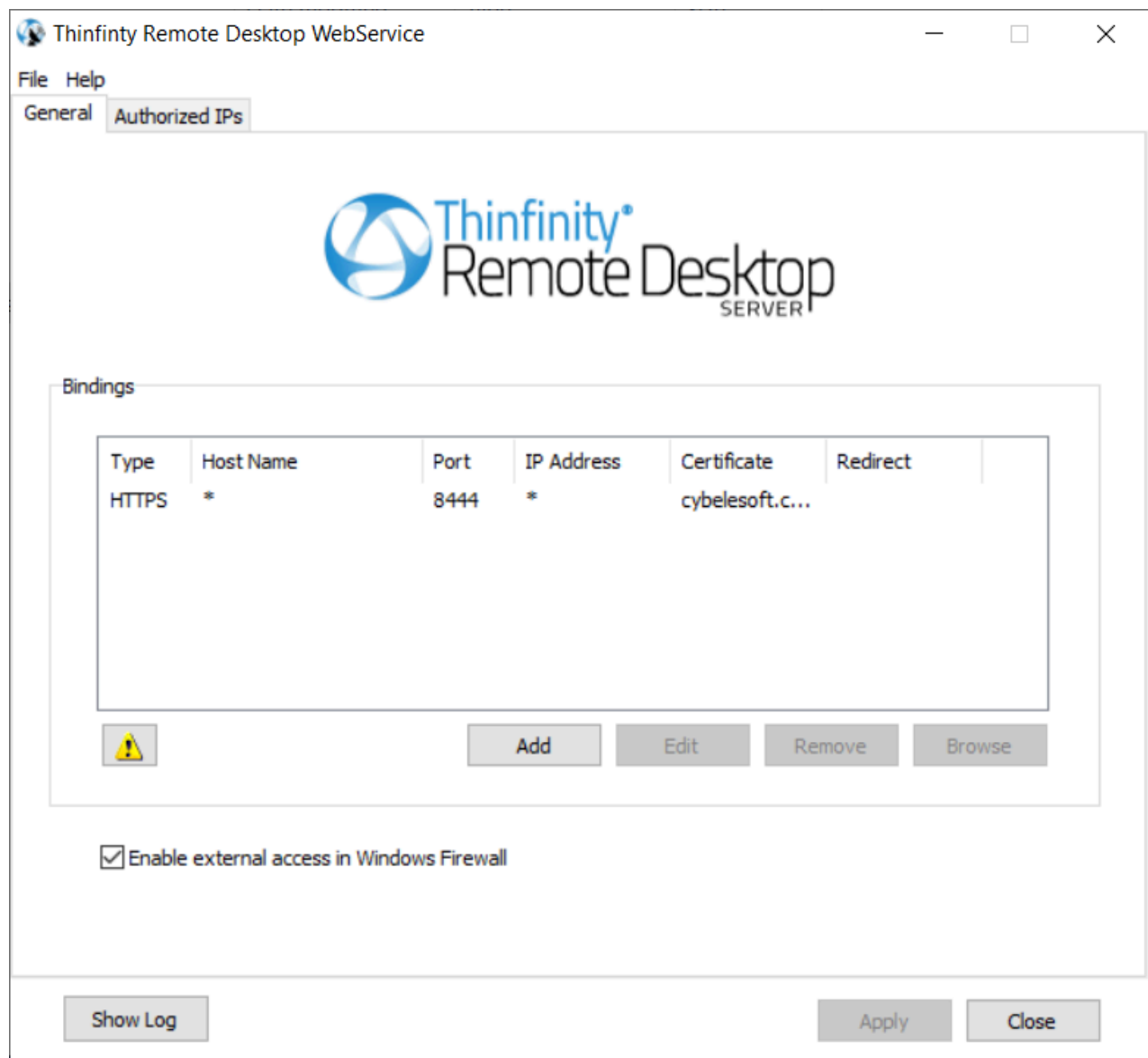
Setting up the Communication Settings

Setting up the Communication Settings

Open the "WebService Admin Tool" from the Windows start menu.

General tab:

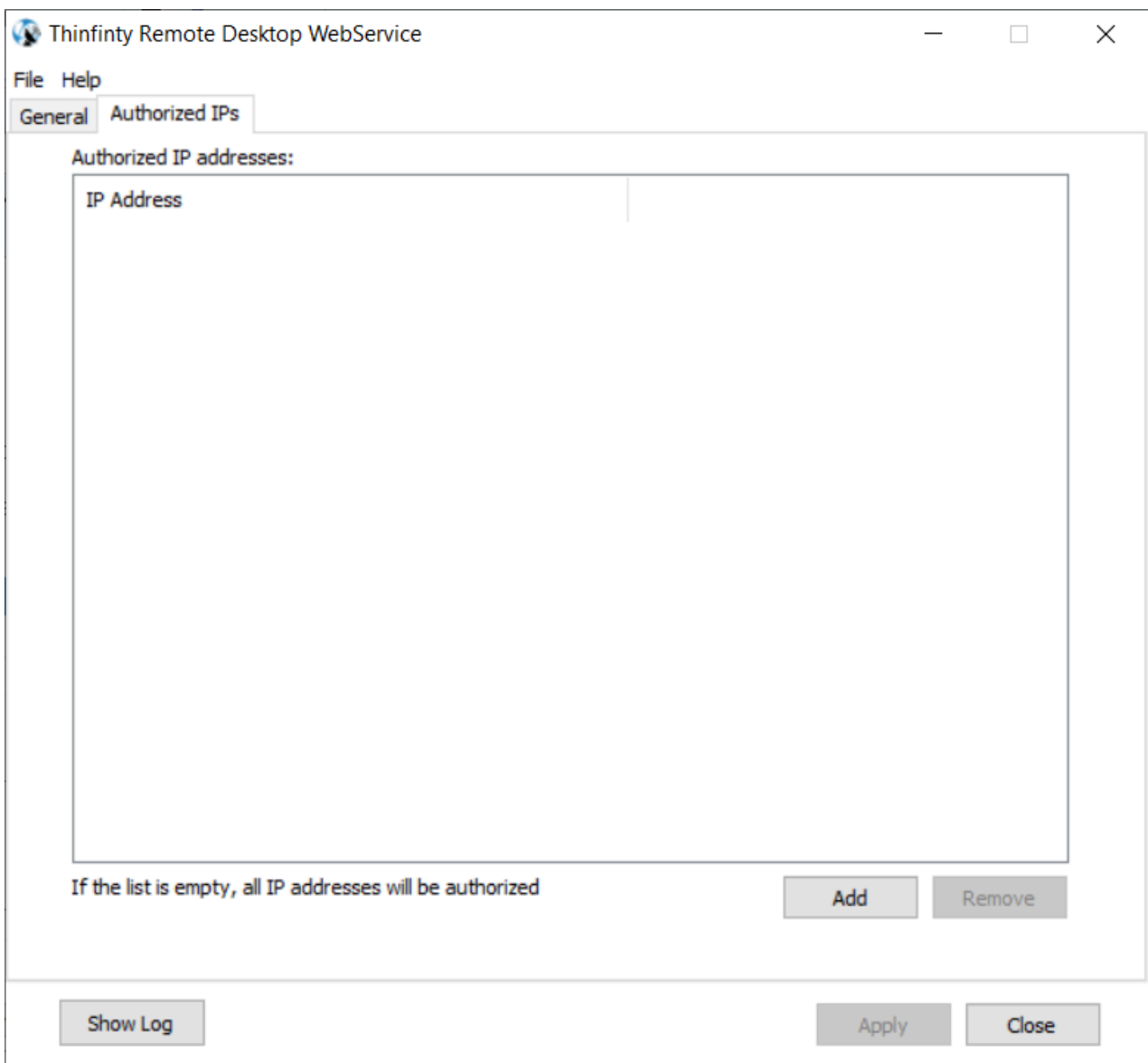
1. By default, the WebService listens to HTTP and port 8444.



4. You can change this

Authorized IPs tab:

1. Go to the "Authorized IPs" tab.
2. If you don't want to restrict the IP addresses that will access the Web Service, leave the list empty.
3. If you want only determined IPs to access the Web Service, click on "Add" and add 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.

Profiles Web Service

The Access Profiles Web Service integration allows external applications to:

1. Retrieve any information from the profiles configured in Thinfinity® Remote Workspace
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.

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 Workspace	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.
				If there is are no profiles

FindByUserName	Returns all profiles assigned to the user.	string: username	<u>WSProfileArray:</u> user granted profiles.	associated with the user, returns a WSProfileArray with length = 0.
CreateProfile	Creates a new profile.	<u>WSProfile:</u> profile to be created	<u>WSProfile:</u> 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.	<u>WSProfile:</u> profile to be updated with the new data already loaded in its structure.	int: returns 0 if the profile was updated successfully. Any value different from 0 means the update could not be performed.	If there is no profile matching the WSProfile ID, returns a value <> 0.
NewPublicKey	Generates a new public key for an existing profile.	string: profile ID	<u>WSProfile:</u> profile carrying the new Public Key.	If there is no profile matching the WSProfile ID, returns null.
Commit	Commits all the performed methods since			

Rollback	the last commit or rollback. Rollbacks all the performed methods since the last commit or rollback.			
----------	---	--	--	--

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 WSProfile type represents one profile. It has all the attributes that describe a profile.	
WSProfileArray	Complex	The WSProfileArray is an array of WSProfile . It is used mostly as a parameter for methods that retrieve more than one profile from the server.	
TRdpCredentials	Simple	This type is used to describe the kind of authentication the WSProfile will perform. "crAuthenticated" means no username and password will be required. "crAsk" will use the username and password configured inside the profile. When "crSaved" is set up, the profile will authenticate	"crAuthenticated" "crAsk" "crSaved"

		automatically using the same application credentials.	
TRdpScreenBPP	Simple	<p>Color Depth: sets the WSPProfile remote desktop screen number of bits per pixel .</p> <p>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)</p>	<p>"bpp8",</p> <p>"bpp15",</p> <p>"bpp16",</p> <p>"bpp24",</p> <p>"bpp32"</p>
TRdpScreenResolution	Simple	<p>WSPProfile remote desktop screen resolution.</p>	<p>"srCustom",</p> <p>"srFitToBrowser",</p> <p>"srFitToScreen",</p> <p>"sr640×480",</p> <p>"sr800×600",</p> <p>"sr1024×768",</p> <p>"sr1280×720",</p> <p>"sr1280×768",</p> <p>"sr1280×1024",</p> <p>"sr1440×900",</p> <p>"sr1440×1050",</p> <p>"sr1600×1200",</p> <p>"sr1680×1050",</p> <p>"sr1920×1080",</p> <p>"sr1920×1200"</p>

TRdpImageQuality	Simple	WSProfile remote desktop image quality.	"iqHighest", "iqOptimal", "iqGood", "iqFaster"
TRdpAppMode	Simple	<p>The application mode is used to determine if Thinfinity® Remote Workspace will open a specific application and the mode it will use to do it.</p> <p>The "amNone" value will show the whole desktop mode. The "StartApp" and "RemoteApp" are the two possible modes of connecting to a remote application.</p>	"amNone", "amStartApp", "amRemoteApp"
		This type is used to describe the	"ccDoor"

The WS Profile type

The WSProfile type

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

Attribute name

Type	Description	Modifiable	
ID	string	Profile ID	no
Name	string	Profile name	yes
Enabled	boolean	Set false if you want the profile to be disabled	yes
Unrestricted	boolean	Only the [any computer] profile has this property set to true. It means that the profile will enable the users to choose the computer they will access entering the IP, port and credentials on the connection moment.	no
GuestAllowed	boolean	Set true to make the profile public	yes
IsBuiltIn	boolean	This attribute identifies the [any computer] profile. Only this profile has this attribute set to true.	no

PublicKey	string	Key that identifies a profile .	no
Computer	string	The remote desktop IP and port to connect to	yes
Credentials	TRdpCredentials	Configures the credential mode Thinfinity® Remote Workspace will operate on.	yes
LogonUserName	string	If the credential mode is set to "crAsk", will use this Username to log in into the computer.	yes
LogonPassword	string	If the credential mode is set to "crAsk", will use this Password to log in into the computer.	yes
ScreenResolution	TRdpScreenResolution	Sets the remote desktop resolution.	yes
ScreenWidth	int	Remote desktop screen width.	yes
ScreenHeight	int	Remote desktop screen height.	yes
BPP	TRdpScreenBPP	Color Depth: sets the number of bits per pixel	yes
ImageQuality	TRdpImageQuality	Remote desktop image quality.	
UnicodeKbd	boolean	Allows for full unicode keyboard charsets. Set to	yes

		false to connect to xRDP servers. Set to true to connect to the console session. This requires confirmation from the logged on user and will log out the current session.	
ConsoleSession	boolean		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	yes

PrinterEnabled	boolean	will present many visual effects Visual Effects option to disable Thinfinity® Remote Workspace PDF printer.	yes
PrinterSetAsDefault	boolean	Mark this option to make Thinfinity® Remote Workspace 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	<p>This is the driver to be used by Thinfinity® Remote Workspace in order to print the remote documents.</p> <p>The "<i>HP Color LaserJet 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. 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.</p>	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® Workspace 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 Workspace will use to reproduce the remote sound. The highest the quality,	yes

Users	string	the more resources it will require. Windows Authentication Users or Groups that will be granted access to this profile. Separate each user or group	yes
-------	--------	---	-----

The Demo Applications

We have packed with the Thinfinity® Remote Workspace installation two example applications that use Thinfinity® Remote Workspace Web Service to manipulate Access Profiles.

If you have already [installed Thinfinity® Remote Workspace WebService](#), you can access the demos from the Windows Start menu: All Programs/Thinfinitiy/Thinfinitiy Remote Workspace 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 Workspace application, until you call the **Commit** method on the Web Service.

Analytics Web Service

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

Methods

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

Method name	Method description	Input params	Output params	Exceptions
Count	Returns an integer value with the count of the records that satisfy the search criteria sent on the QueryType parameter.	QueryType: WSQueryType	Integer	
List	The list method returns an array containing all the records that satisfy the search criteria sent on the QueryType parameter.	QueryType: WSQueryType	WSDBRecordArray	If the search does not match any record, the result will be a WSDBRecordArray with length = 0.
RangeList	The RangeList method returns an array containing all the records that satisfy the search criteria sent on the QueryInfo parameter. The QueryInfo is composed by the QueryType and also a date range to filter	QueryInfo: WSQueryInfo	WSDBRecordArray	If the search does not match any record, the result will be a WSDBRecordArray with length = 0.

	the records (QueryRange).			
LoginList	The LoginList method returns an array containing all the records that satisfy the search criteria which is composed by a QueryRange and the login type (successful logins and failed logins).	Range: WSQueryRange ; Successful: Boolean Failed: Boolean	WSDBRecordArray	If the search does not match any record, the result will be a WSDBRecordArray with length = 0.

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.	
		This type is a generalization interface of all	

WSDBRecord	Simple	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.	

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

WSQueryRange

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

Attribute name	Type	Description	Modifiable
dateFromField	dateTime	Lower dateTime limit from where the records should be searched.	yes
dateToField	dateTime	Upper dateTime limit until where the records should be searched.	yes

WSDBLoginRecord

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

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

WSSessionRecord

The WSDBSessionRecord type describes how a Session record is structured.

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

WSDBConnectionRecord

The WSDBConnectionRecord type describes how a Connection record is structured.

Attribute name	Type	Description
userField	string	User that established the connection.
sourceIPField	string	IP Address from which the connection was established.
hostField	string	Host Name to which the connection was established.
connStartField	string	Date and time when the Connection was Started.
connEndField	string	Date and time when the Connection was Ended.

WSDBBrowserRecord

The WSDBSessionBrowser type describes how a Browser record is structured.

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

The Demo Application

We have packed —along with the Thinfinity® Remote Workspace installation— one example that uses analytics for Thinfinity® Remote Workspace WebService to show the application usage data.

If you have already [installed Thinfinity® Remote Workspace WebService](#), you can access the demos from the Windows Start menu All Programs/Thinfinity/Thinfinity Remote Workspace Demos.

The application was developed in C# and was designed to present you an integration possibility the Web Service provides you.

In order to compile this application, you can use the Microsoft Visual C# Studio 2010 Express. Download it [here ↗](#).

ThinRDPWS-Query application example:

This application is an example of an external application integrating each available Web Service method.

Observe that the upper radio buttons are different date ranges used to filter the statistic records.

Select one of the date options, go to a specific tab (Logins, Sessions, Connections or Browsers) and click on the Refresh button.

The analytics data will be displayed on the tab grid.

[illegible]

One-Time-URL

Thinfinity® Remote Workspace 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 Workspace 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 '**Allow Anonymous Access**'.
- b. Generating a temporary access to a desktop.
- c. Integrating Thinfinity® Remote Workspace on a Single-Sign-On Scheme along with external applications.

How it works:

1. First you need to ask Thinfinity® Remote Workspace to generate the URL for you. Call Thinfinity® Remote Workspace server following this URL format:

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

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

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

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

Parameter	Description
apiKey	The ApiKey is a secret value, known only by Thinfinity® Remote Workspace and the corporate application. Find out more about it on the ApiKey topic .
apiuser	Use this parameter to identify the user within Thinfinity® Remote Workspace. The value should be the user or email registered in your website. The users are seen in the Analytics Web Service .
model	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.
plen	The plen parameter carries the password length.
expires	Through this parameter you can set an expiration(in minutes) for the URL. Expires = 30 means that the URL won't work anymore after 30 minutes from the URL generation.

On the next topics you can find out other parameters you can use to [Configure the connection](#) and [Enable features](#).

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

```
/oturl.html?
key=w7NJNschBdJD9e6G6luWh0Ca1M$oFW7guqC6jE1IQah3AJm3&pass=B0WZB8FG
```

Concatenate the Thinfinity® Remote Workspace address to the generated URL, following this format below:

```
http(s)://Thinfinity:Port/oturl.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](#)

Configuring the Connection

Besides the basic parameters required to establish a connection, you can send additional settings parameters to customize the connection the way you want.

There are three ways to customize the one-time-url connection:

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

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

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

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

Mode 2. Overriding the profile settings:

Parameter	What it means	Type/format	Default
	Set this property to true, to have the Profile settings overridden by the parameters sent on the queryString. Then configure the		

overrideDefaults	<p>individual settings you want to add to the Profile connection template</p> <p>If you send this parameter as false, only the profile configuration will be taken.</p>	<p>boolean</p> <p>true,false</p>	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 Workspace setting individually.

Find below the list of the parameters you can configure manually:

Parameter	What it means	Type/format	Default
computer	<p>The remote desktop IP and port to connect to.</p> <p>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.</p>	<p>string</p> <p>IP:Port</p>	
username1	<p>The username to authenticate against the remote machine. If this parameter is not sent, Thinfinity® Remote Workspace</p>	<p>string</p> <p>username</p>	

	will prompt the user for this information. The password to authenticate against the remote machine. If this parameter is not sent, Thinfinity® Remote Workspace will prompt the user for this information.		
password1		string password	
startprg	If you will use the OneTimeURL to start a specific application, you should change this and the following three fields. Set it to 0 for the "Do nothing" option; 1 for the "Start a program" option; 2 for the "Launch RemoteApp" option.	integer 0,1 or 2	0
command	Full remote application path that should start upon connection establishment.	string app path	
directory	Initial context directory to be used by the application set on command parameter described above.	string dir path	
cmdargs	Arguments to start the application specified on the "command" property.	string app args	
	Color Depth: sets the number of bits		

bpp	per pixel. Set 8 for 256 colors; 15 for True Color (15 bit); 16 for True Color (16 bit) ; 24 for True Color (24 bit)	integer 8,15,16 or 24	16
resolution	"fittobrowser", "fittoscreen", "fixed". When "fixed", the 'width' and 'height' parameters will be considered.	string toolbar size	"fittobrowser"
width	Remote desktop screen width. It will only be considered when the resolution parameter is set to "fixed".	integer pixels	Desktop width
height	Remote desktop screen height. It will only be considered when the resolution parameter is set to "fixed"	integer pixels	Desktop height
imagequality	Specifies the image quality/compression. Set 0 for "Highest"; 1 for "Optimal"; 2 for "Good"; 3 for "Faster"	integer 0,1,2 or 3	1
desktopbackground	Set to true to show the original remote desktop background.	boolean true,false	false
	Set to true to change the start	boolean	

visualstyles	menu and other windows features style.	true,false	false
menuwindowanimation	Set to true to show an animation on the Start menu.	boolean true,false	false
fontsmoothing	Set to true to make text easier to read, especially magnified text.	boolean true,false	false
showwindowcontent	Set to true to show windows contents while dragging them.	boolean true,false	false
desktopcomposition	Set to true to configure the DWM to redirected the desktop drawing to off-screen surfaces in video memory. The desktop will also present many visual effects.	boolean true,false	false
unicodekeyboard	Allows for using full unicode keyboard charsets. Set to false to connect to xRDP servers.	boolean true,false	true
keyboardlayout	Allows to specify the keyboard layout when unicode keyboard is disabled.	string Keyboard identifier (hexadecimal)	"00000409 (US)
console	Forces the connection to connect to the remote console session.	boolean true,false	false

wscompression	Set to true to enable the compression for the exchanged Websocket data and have the application performance improved.	boolean true,false	true
disablenla	Set the option disableNLA if you use a CredSSP other than Microsoft.	boolean true,false	false
desttype	Set the desttype to "VMID" in case you want to establish a connection to a Hyper-V Virtual Machine or set "RDS" if you want to create a connection to an RDS Collection VM. The connection will act as a regular connection in case you don't inform this property of inform any value different from "VMID" and "RDS".	string VMID or RDS	
destinfo	Inform the Virtual Machine ID, for Hyper-V Virtual Machine connections or inform the TSV URL for RDS Collection Virtual Machines.	string Virtual Machine ID or TSV URL	

diskenabled	Set to true to have an intermediate disk available on the connection.	boolean true,false	true
diskname	Identify the intermediate disk among the other remote desktop disks.	string name	"ThinDisk"
	Set to true to		

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 supposed 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...

Enabling Features

You can also send some parameters on the queryString to enable Thinfinity® Remote Workspace features.

Find below the parameters you can send in order to enable and configure Thinfinity® Remote Workspace features for the One-Time-URL connection:

Clipboard:

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

Printer:

Parameter	What it means	Type/format	Default
printerenabled	Set to true to enable Thinfinity® Remote Workspace PDF printer.	boolean true,false	false
printersetasdefault	Thinfinity® Remote Workspace printer as the remote default printer.	boolean true,false	true
printername	Specify the printer name that you want to be shown on the remote machine's printer list.	string name	
	Mark this option to set Thinfinity® Remote Workspace	string	

printerdriver

printer as the
remote machine
default printer.

driver

Sound:

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

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

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

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

Thinfinity® RemoteAD API reference

Thinfinity® REST API Reference

For more details regarding the REST API, please visit:

<https://api-workspace-docs.cybelesoft.com/> ↗

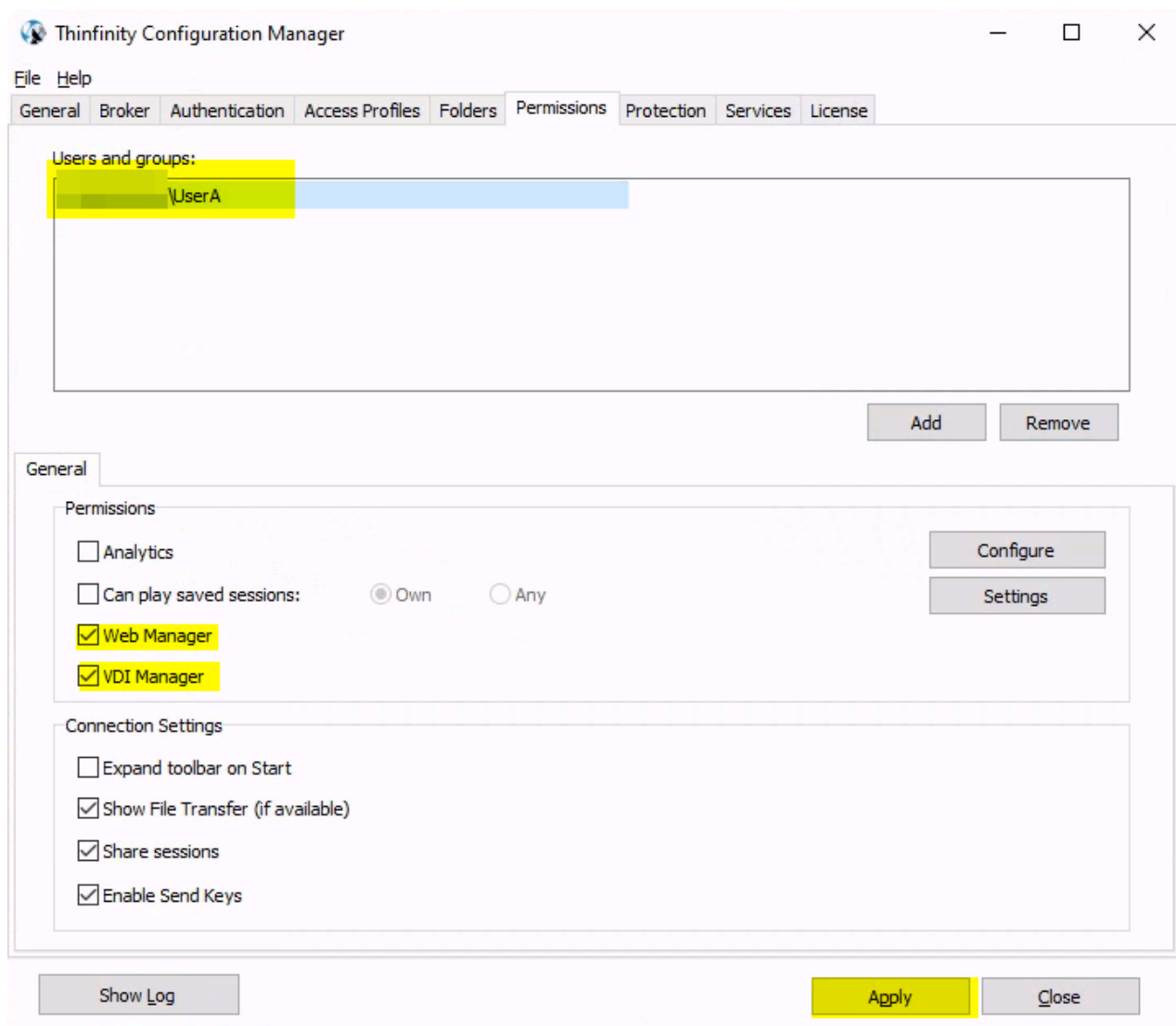
Cloud Automation

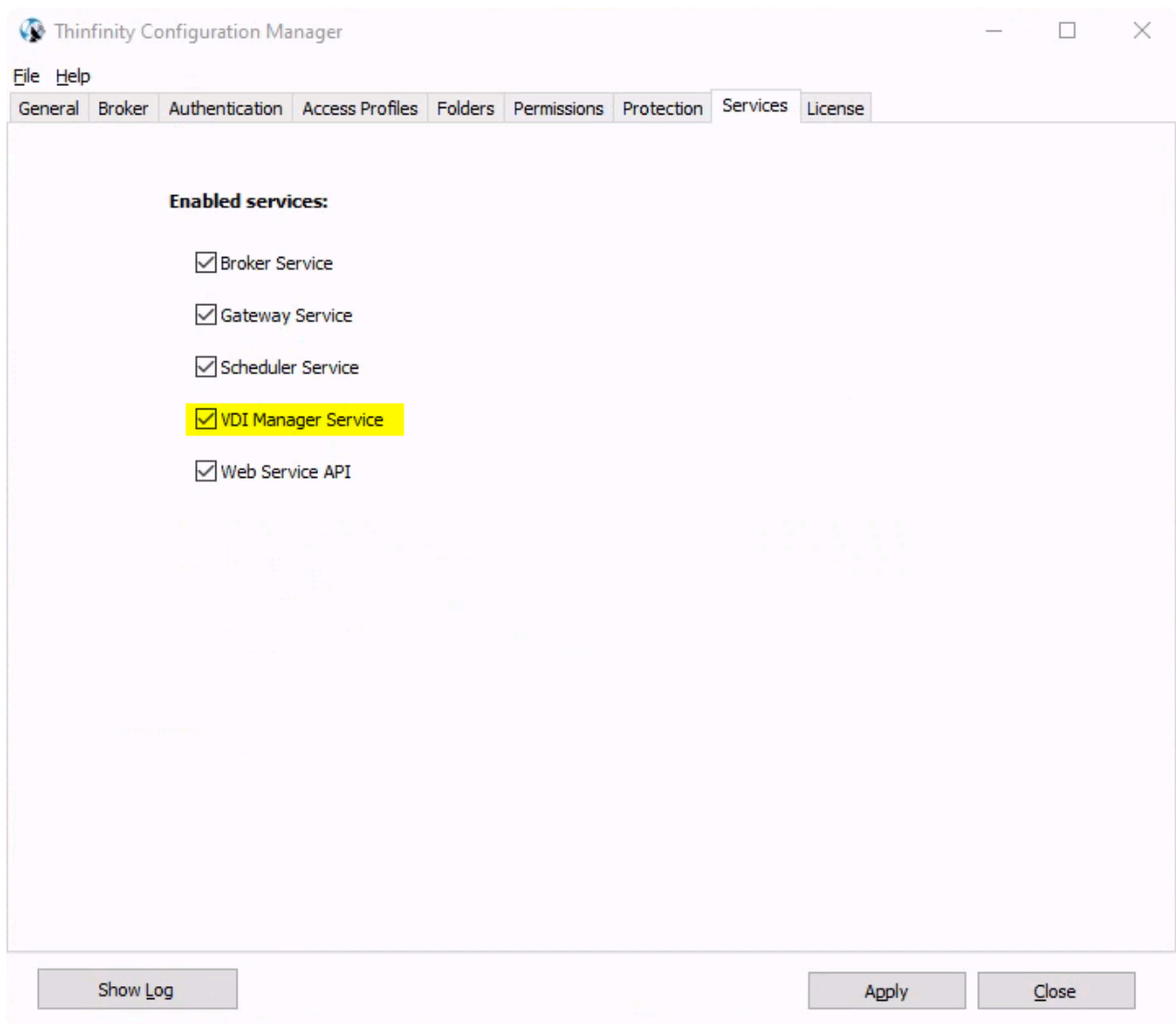
How to enable the VDI Manager

To enable cloud automation we need to add a user with the right permissions to have access to Cloud Automation Manager

To do so, first we have to go to the permissions tab of the configuration manager and enable the "web manager" the "cloud on demand" features, and then hit apply

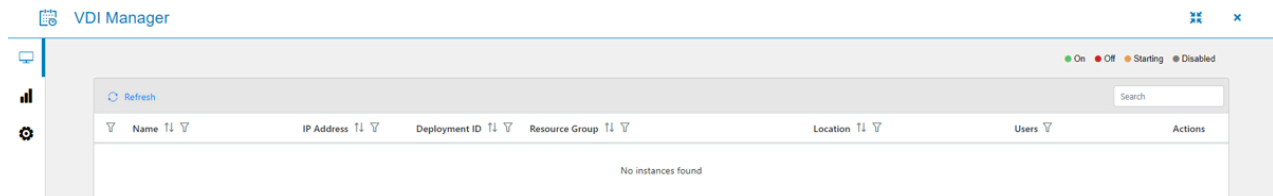
After that, we have to go to the services tab, and make sure that the VDI Manager Service services are enabled





Instances

In the Instance section, you will be able to manage, check the status of your Virtual Machines, and have a quick overview of the deployment.



Status

On: When the VM is on, it will show a 'green' status.

Off: When the VM is off, it will show a 'red' status.

Starting: When the VM is starting, it will show an 'orange' status.

Disabled: When the VM is disabled, it will show a 'gray' status.

Instances

Refresh Button: This button will force refresh of the status page.

Search: Use this to search a specific VM

Name: Name of the VM

IP Address: IP Address of the VM

Deployment ID: Deployment ID this VM was based on.

Resource Group: The Resource Group it belong to in Azure

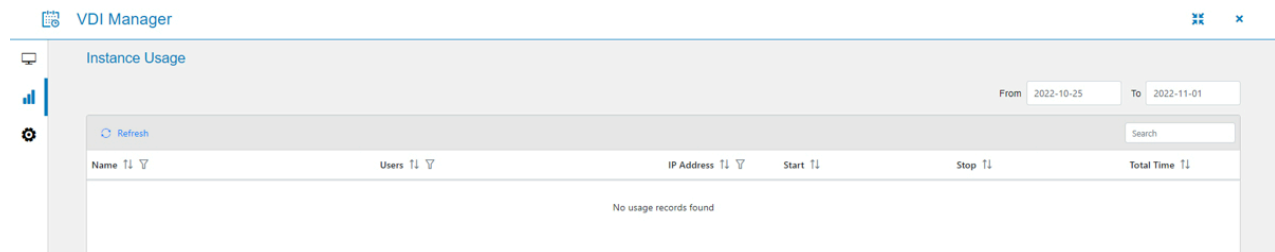
Location: The Azure Region the VM is located.

Users: The user that has access to this VM

Actions: Here you will be able to manage the VM. You can either start, stop or delete this VM.

Instance Usage

From the Instance Usage page, you will be able to access the log of usage of your VMs.



Description

Name: Name of the VM

Users: The user that has acced the VM

IP Address: IP Address of the VM

Start: Time the VM started.

Stop: Time the VM stopped.

Total Time: The total time the VM was on.

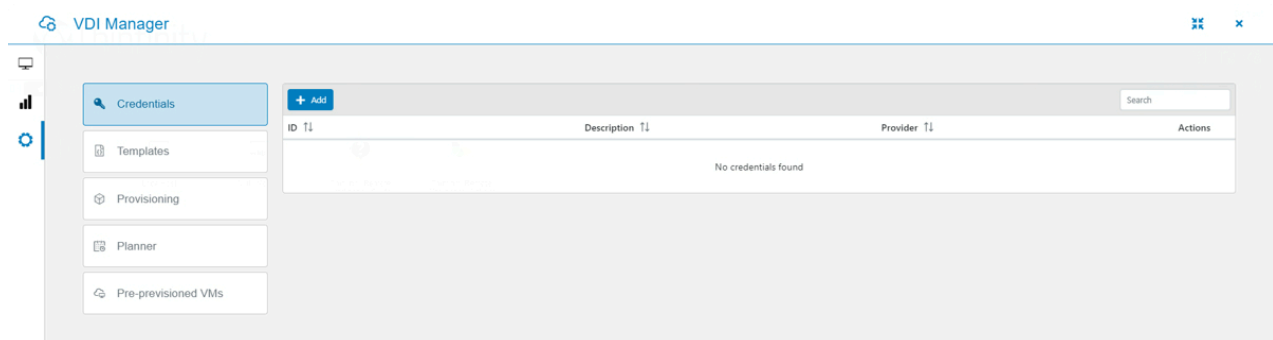
Configuration

In the Configurations pane you will be able to configure the settings related to your Azure account and resources.

Credentials

In the Credentials tab, you will be able to configure the App Registration in your Azure Active Directory you want to use.

Search: Use this to search for the set of credentials (App Registration)



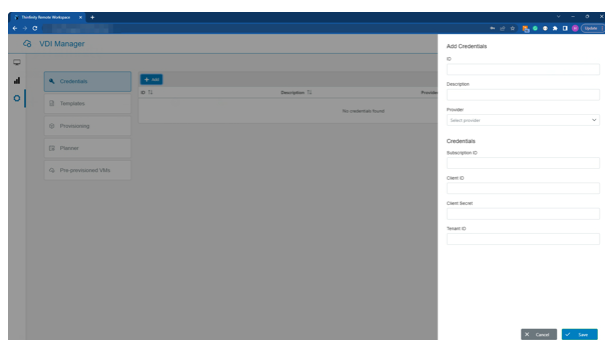
ID: Credential's ID.

Description: Description provided when the Credentials were created.

Provider: Cloud provider of the Credentials.

Actions: Here you can edit or delete the Credentials.

Adding Credentials



ID: Provide a name/ID for the Credentials.

Description: Provide a description for the Credentials.

Provider: Select the Cloud Provider.

Credentials

Subscription ID: Insert the Subscription ID your Azure's App Registration belongs to.

Client ID: Insert the Client ID of your App Registration.

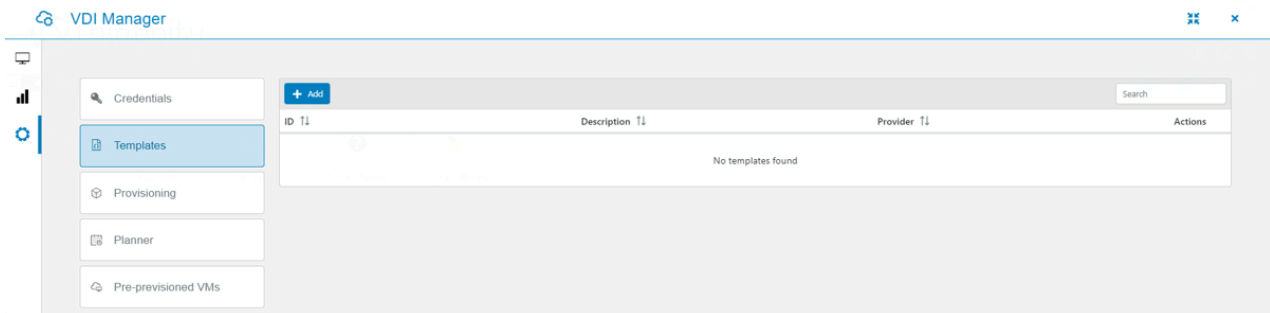
Client Secret: Insert the Client Secret for the Client ID.

Tenant ID: Insert the Tenant ID of Azure.

Templates

In this pane you will be able to add your VM Templates from Azure.

Search: Use this to search for a specific Template



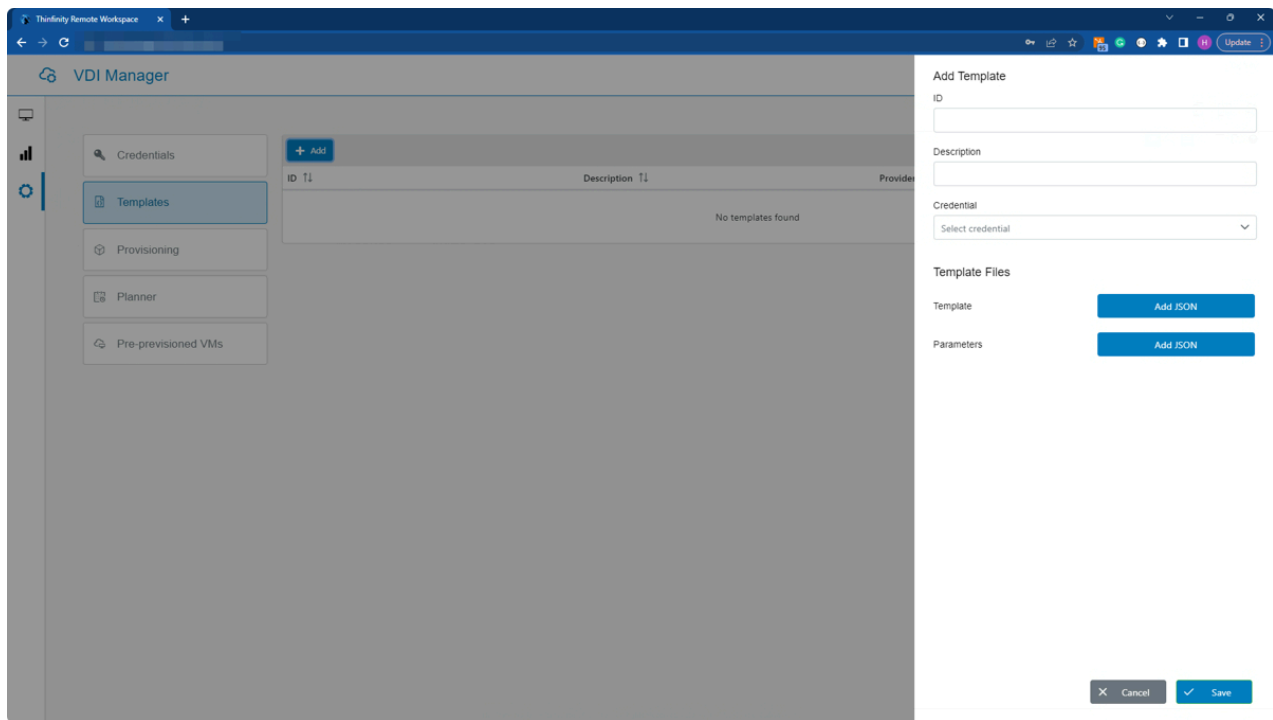
ID: Name of the Template

Description: Description of your Template

Provider: Your cloud Provider

Actions: Here you can edit or delete the Templates.

Adding Templates



ID: Add a name/ID for the Template.

Description: Add a description for the Template.

Credential: Select a set of credentials (App Registration)

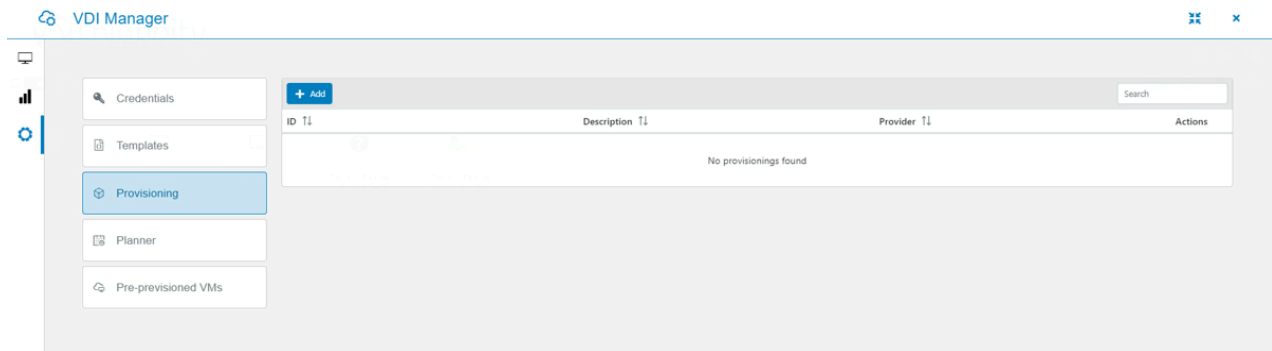
Template Files

Template: Input the Template JSON file of the VM

Parameters: Input the Parameters JSON file of the VM

Provisioning

ID: Name/ID of the Deployment(s)



Description: Description of the Deployments.

Provider: Cloud provider of the Deployment.

Actions: Here you can edit or delete the Deployment.

Adding Deployments

ID: Input a name/ID for the Deployment.

Description: Input a description for the Deployment.

Credential: Select the credentials from the combo box (App Registration)

Template: Select a template from the combo box.

Group: Input Azure's Resource Group for these VMs

-Append Location to Group: Check this box if you wish to append the location to the Resource Group.

Locations: Select the Region.

Parameters:

-Key: Search for a key parameter (for instance, adminPassword, adminUsername, etc)

-Value: Input the value for the Key.

Instancing Modes:

-On Demand: Select this option to create create/start the VMs on-demand.

-Scheduled: Select this option to create/Start the VMs based on a Schedule

Stop After Disconnect: Input the number (minutes) it will take to deallocate the VM after disconnecting.

Estimated Provisioning Time:

Pool Mode:

-None: If selected, pool mode won't be used.

-Breadth First: Will evenly distribute user sessions across the session hosts in a broker pool.

-Depth First: Will saturate a session host with user sessions in a broker pool.

Connection Mode:

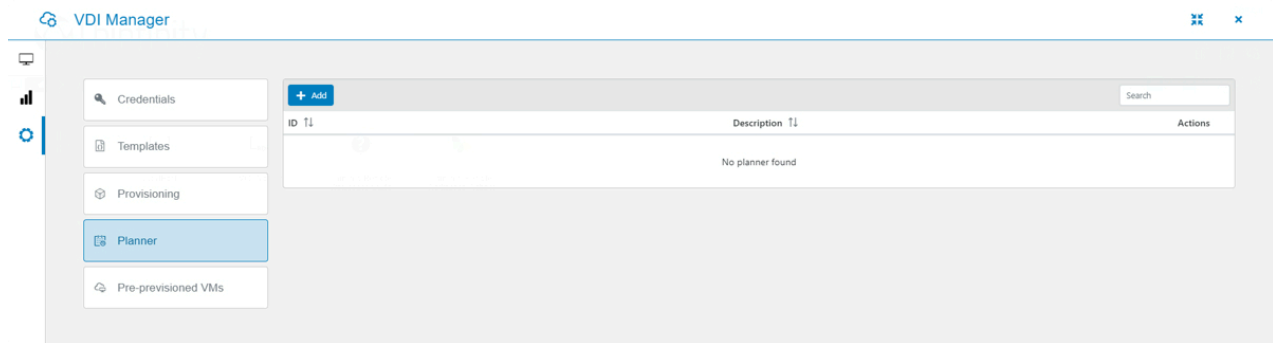
-Public IP: Select this option to connect to a VM through its external IP.

-Private IP: Select this option to connect to a VM through its internal IP.

-Agent IP: Select this option to connect to a VM using the remote ID of the Agent.

Planner

The Deployment Schedules will allow you to automate the start/Create and stop/destroy of you VMs. This will save time to your users

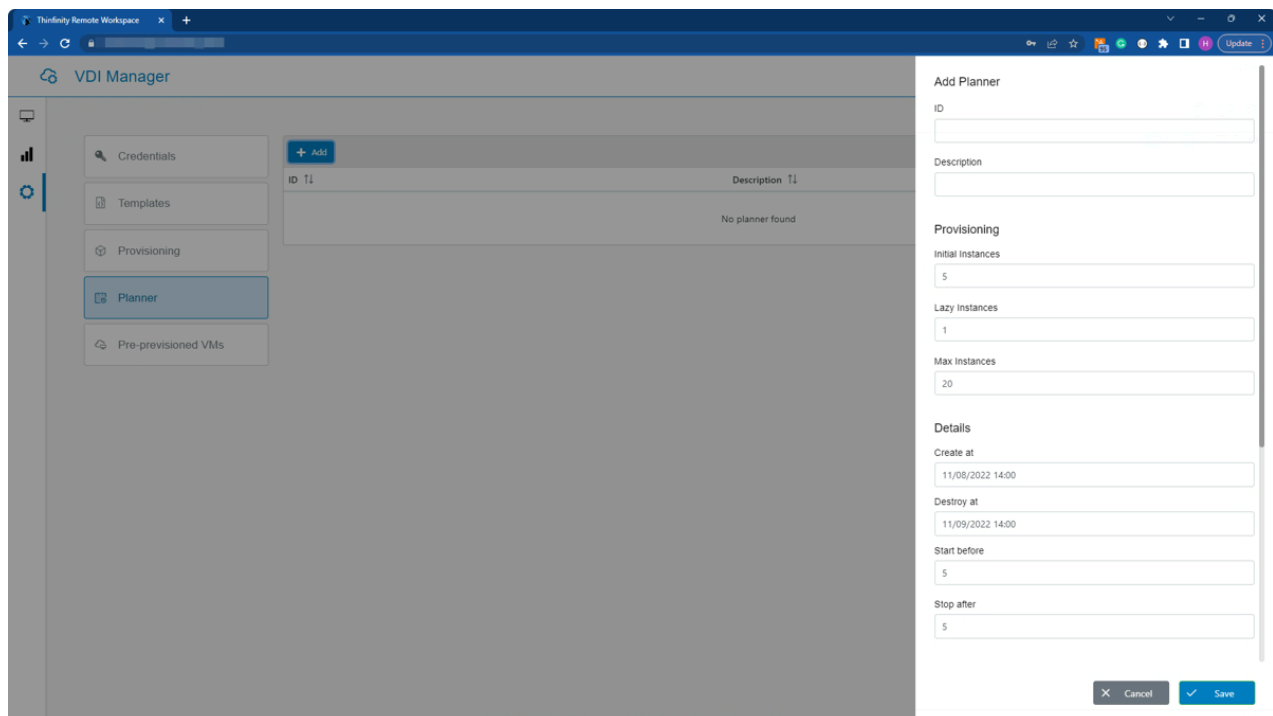


Search: Use this to search for a Schedule

Description: Description of the Deployment Schedule.

Actions: Here you can edit or delete the Deployment Schedule

Adding Deployment Schedules



ID: Add a name/ID for the Deployment Schedule.

Description: Add a description for the Deployment Schedule.

Provisioning

Initial instances: Initial number of VMs Thinfinity will spawn.

Lazy Instances: Number of instances that will spawn and keep idle when all initial instances are in use.

Max Instances: Maximum number of instances Thinfinity will spawn.

Details

Create/Destroy: Select the duration for the Deployment Schedule.

Start Before: Select how many minutes in advanced the VM will start.

Stop After: Select how many minutes after the session is disconnected to deallocate the VM.

Hours

Mode:

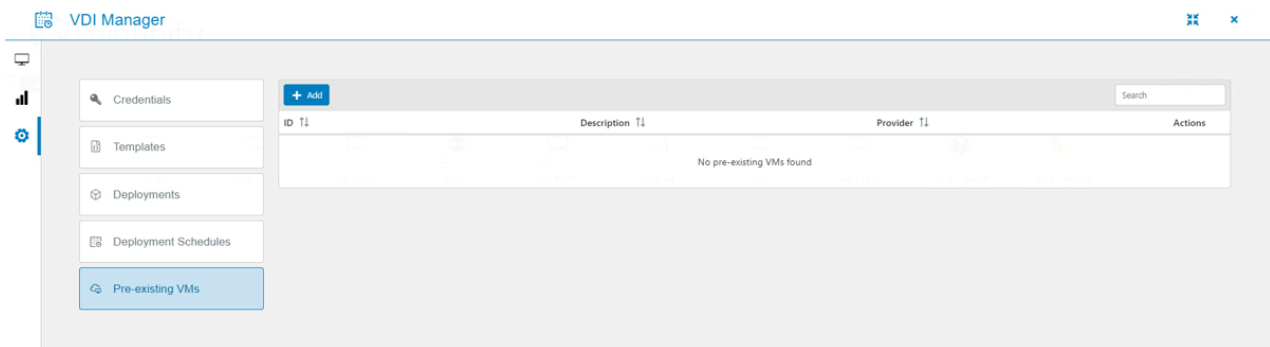
-Access Hours: Define the day and time your application will be available to your users.

-Start/Stop: Define the time the VM will start and stop.

Deployment Schedule: Here you will be able to add the weekly schedules for the VM(s) by day and time.

Exception Dates: Here you can add exceptions, for instance, non-labor days.

Pre-existing VMs



Search: Use this to search for a VM.

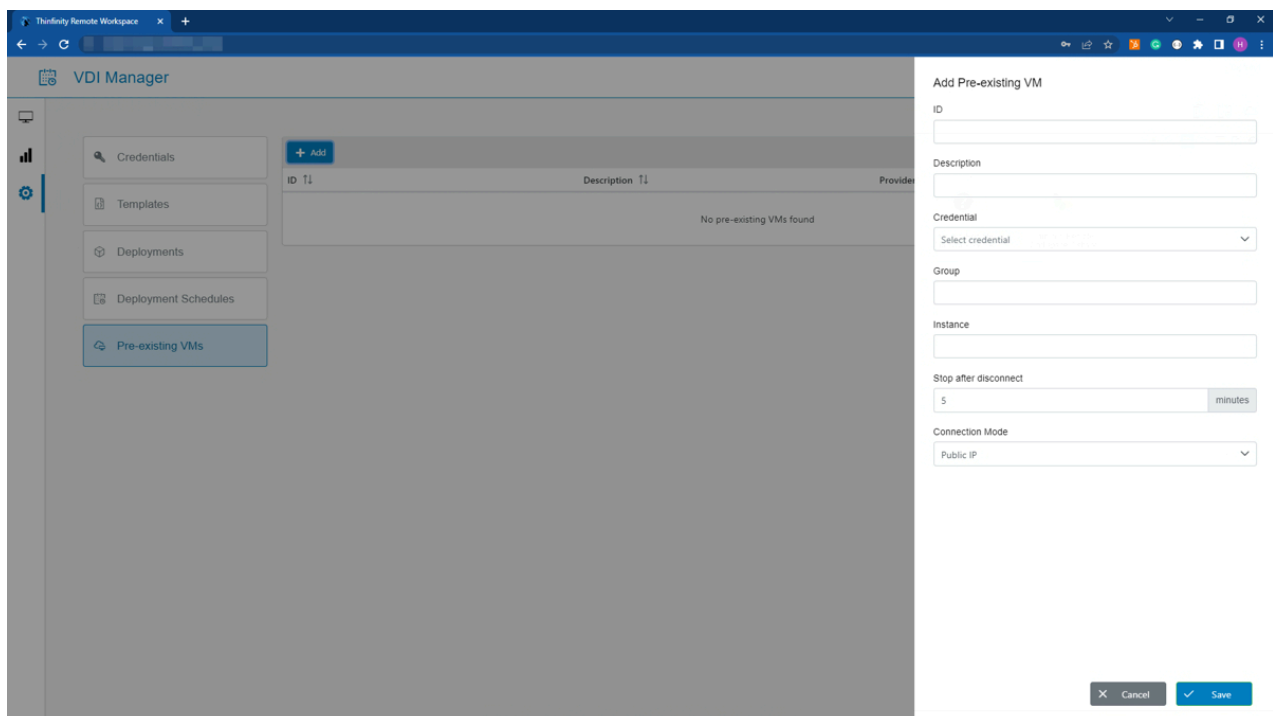
ID: Name/ID of the VM.

Description: Description of the Instance.

Provider: Cloud provider of the VM

Actions: Here you can edit or delete the Pre-Existing VM.

Adding Pre-Existing VMs



ID: Input a name/ID for the instance.

Description: Input a Description for the Instance.

Credential: Select the credentials (App Registration) from the combo box.

Group: Input the Resource Group of the instance.

Instance: Name of the Instance in Azure

Stop After Disconnect: Is the time it will take to deallocate the VM after disconnecting from the session.

Connection Mode:

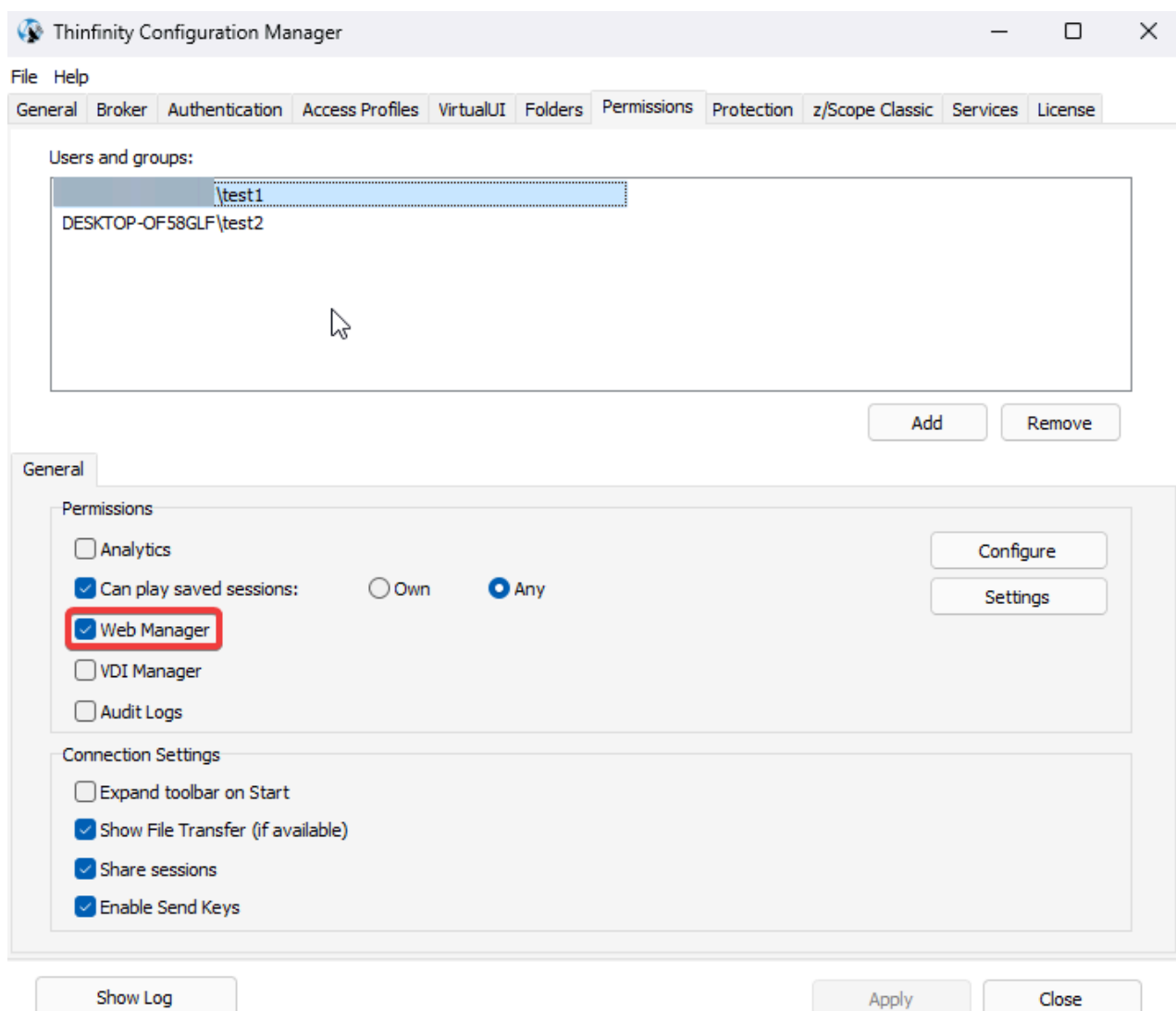
- Public IP: Select this option to connect to a VM through its external IP.
- Private IP: Select this option to connect to a VM through its internal IP.
- Agent Id: Select this option to connect to a VM using the remote ID of the Agent.

Resource Reservation

Enable Resource Reservation

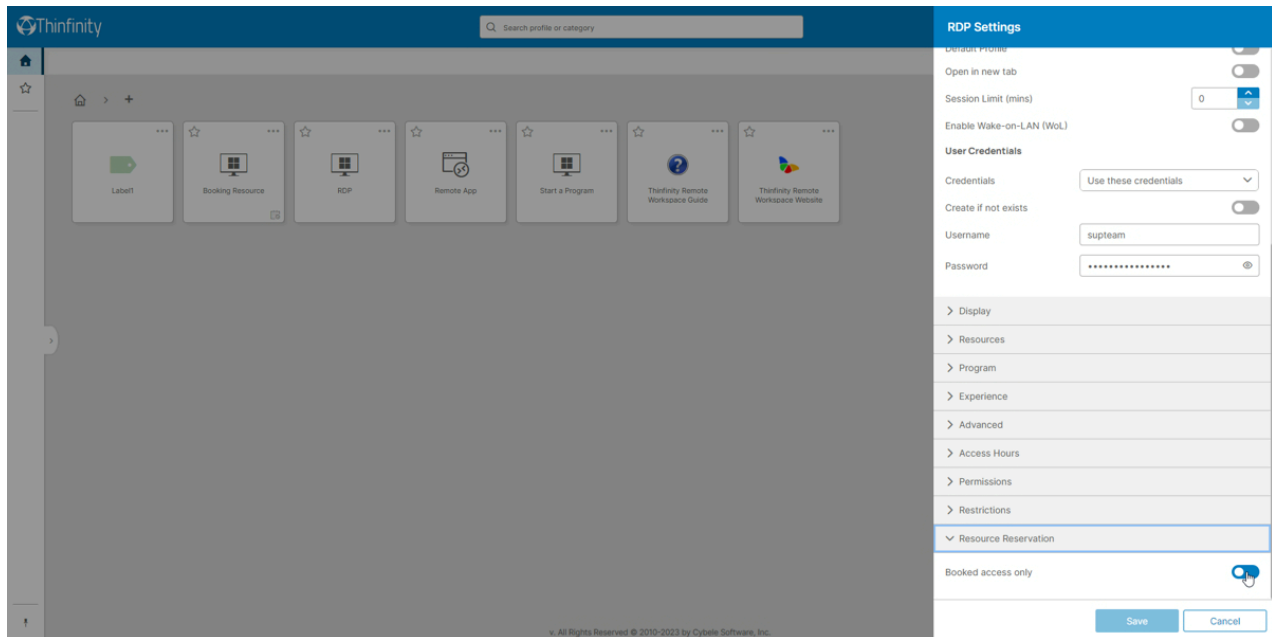
To enable the booking features, first we need to go to the permissions tab of the configuration manager, and then add a user of the local domain to "users and groups"

After that is done we will need to give them web manager permissions, like seen below



After we did that, we need to edit the access profiles we want to enable the Resource Reservation feature. In order to enable it, to do that, we need to open the edit options, and then go to permissions, to check the "booked access only" option,

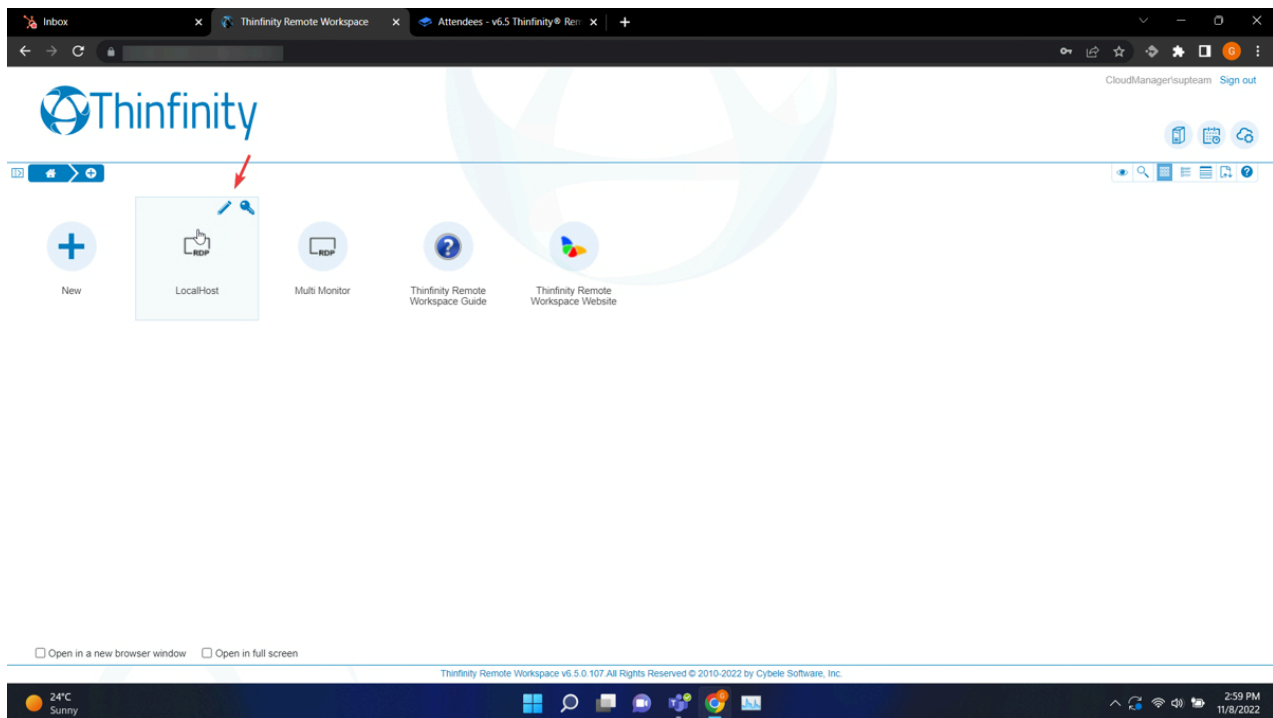
as seen below



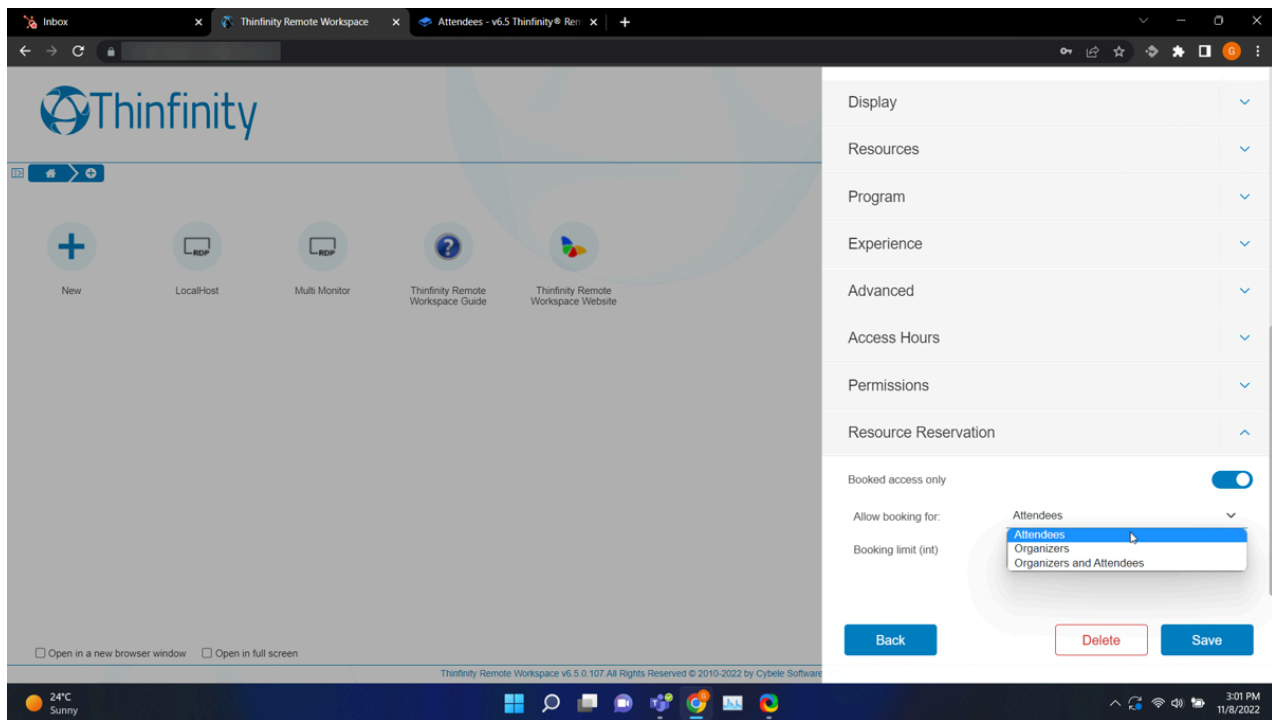
It is necessary to do this only the first time you enable the Booking access, from now on, the user we enabled as a Web Manager will have permission to create new connections from the landing page, and manage the Booking features from there, without the necessity of using the configuration manager

Attendees

To enable the Booking feature "to attendees only" we need to go first to the profile we want to use, and click on the "edit" button



Then, on the menu that opens up, we scroll down the options and on "Booking" we set the "Allow booking for:" to "attendees" as seen below

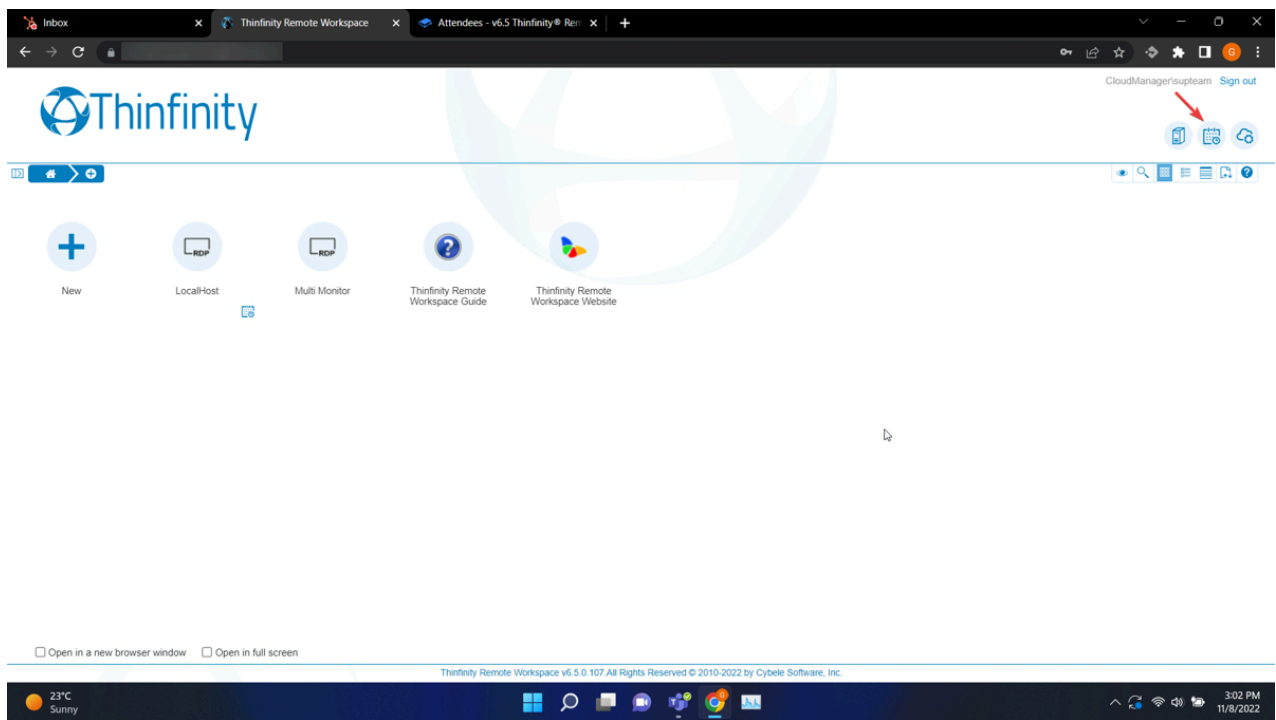
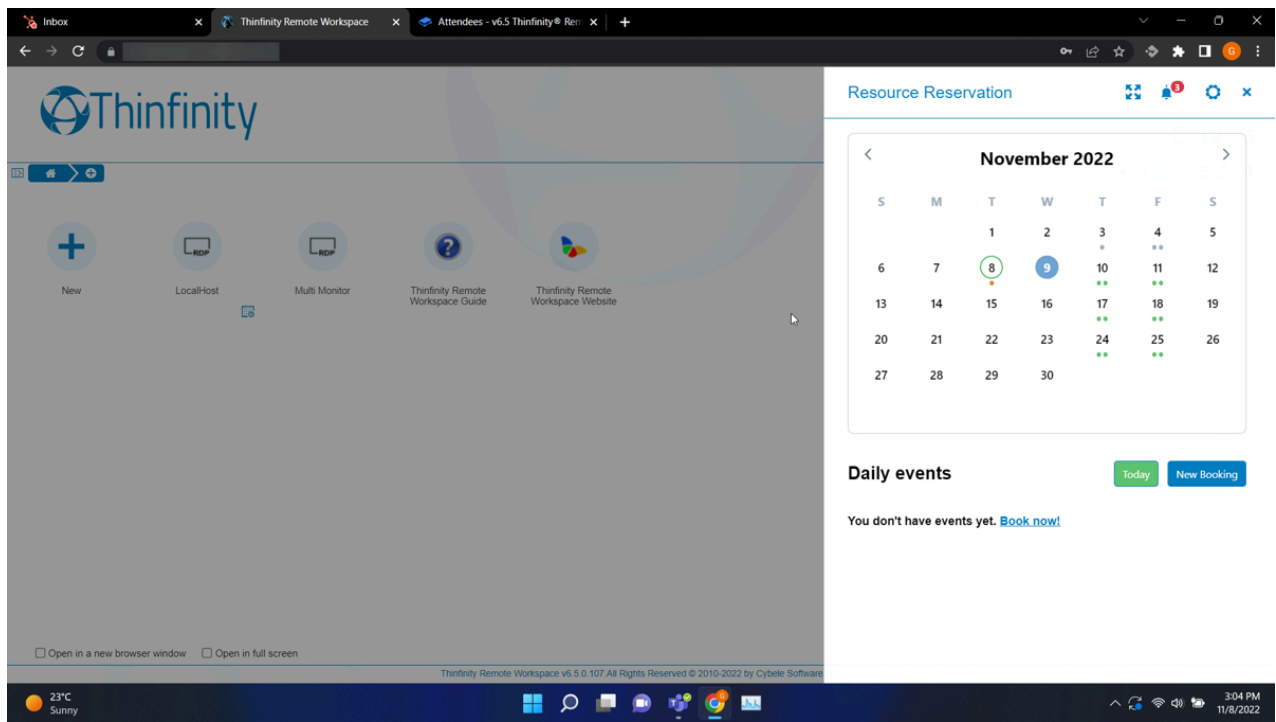


After we did our changes, we have to click on "commit" to save them, and now the connection is ready to allow bookings from attendees only

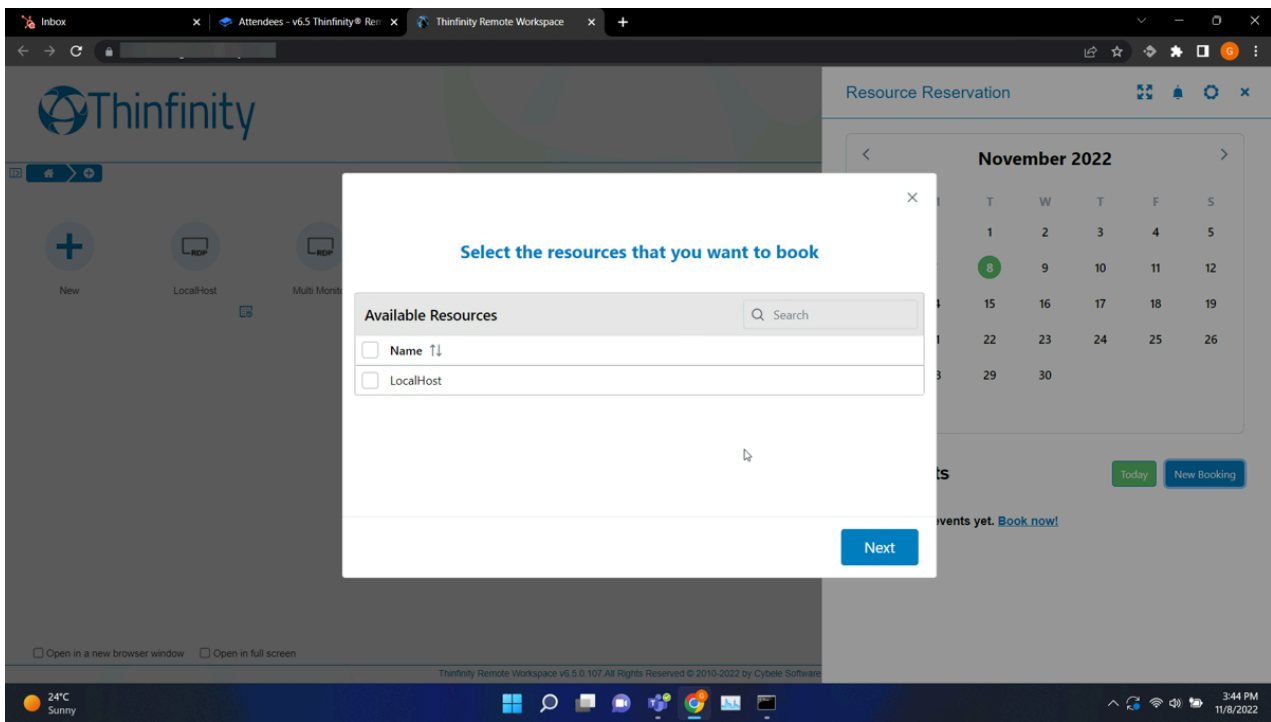
How to schedule bookings as an attendee

To make a new booking as an attendee first we need to click on the icon of the calendar, in the top right corner of the screen

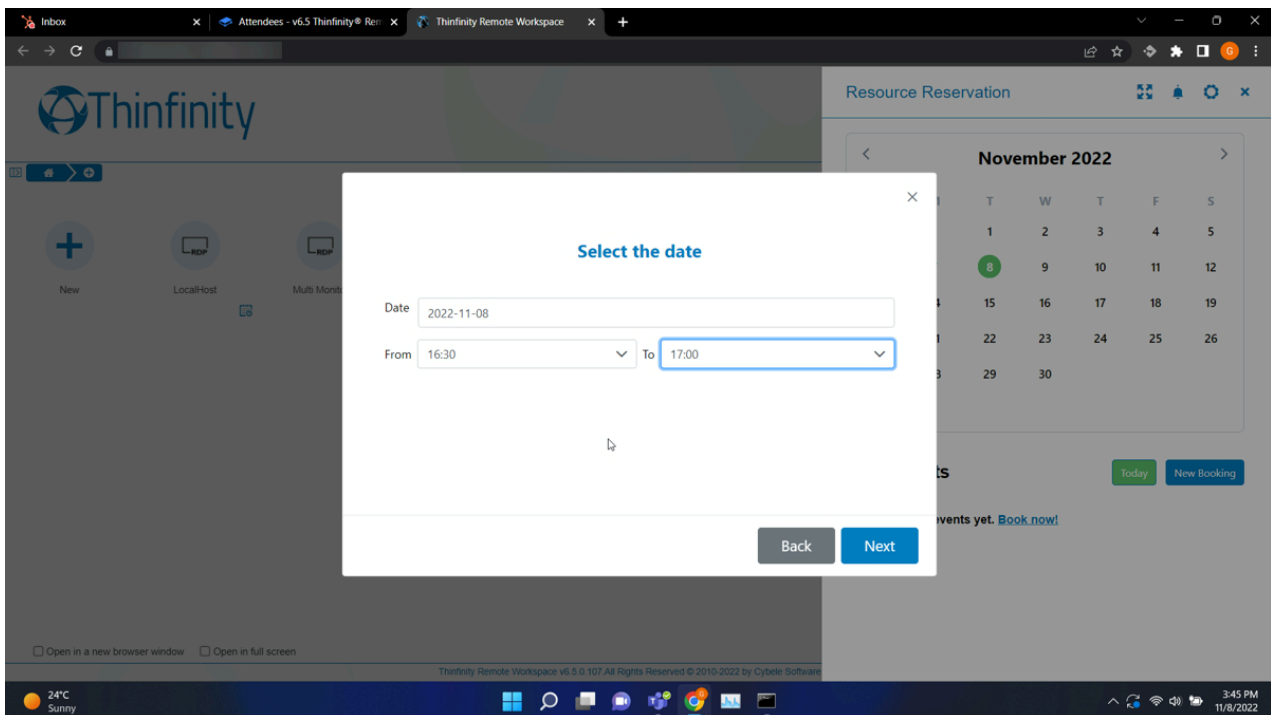
Then we will get the calendar to select the date:



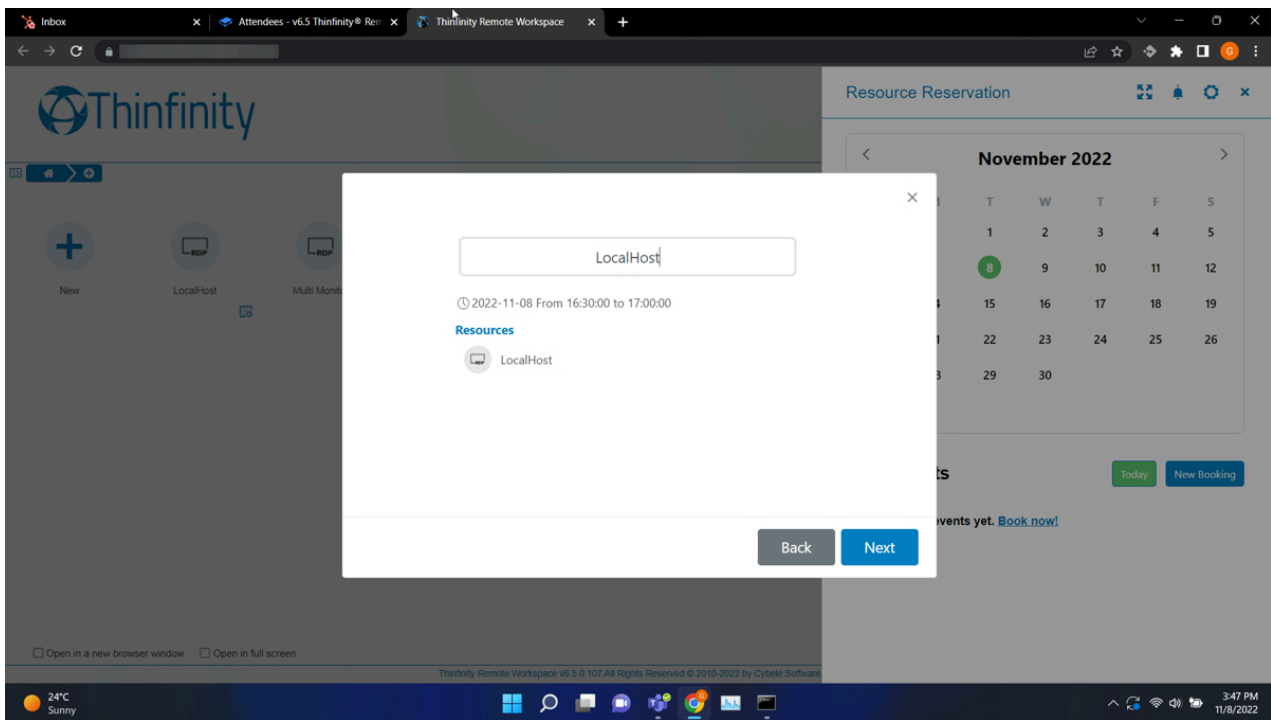
Select the resource you wish to book:



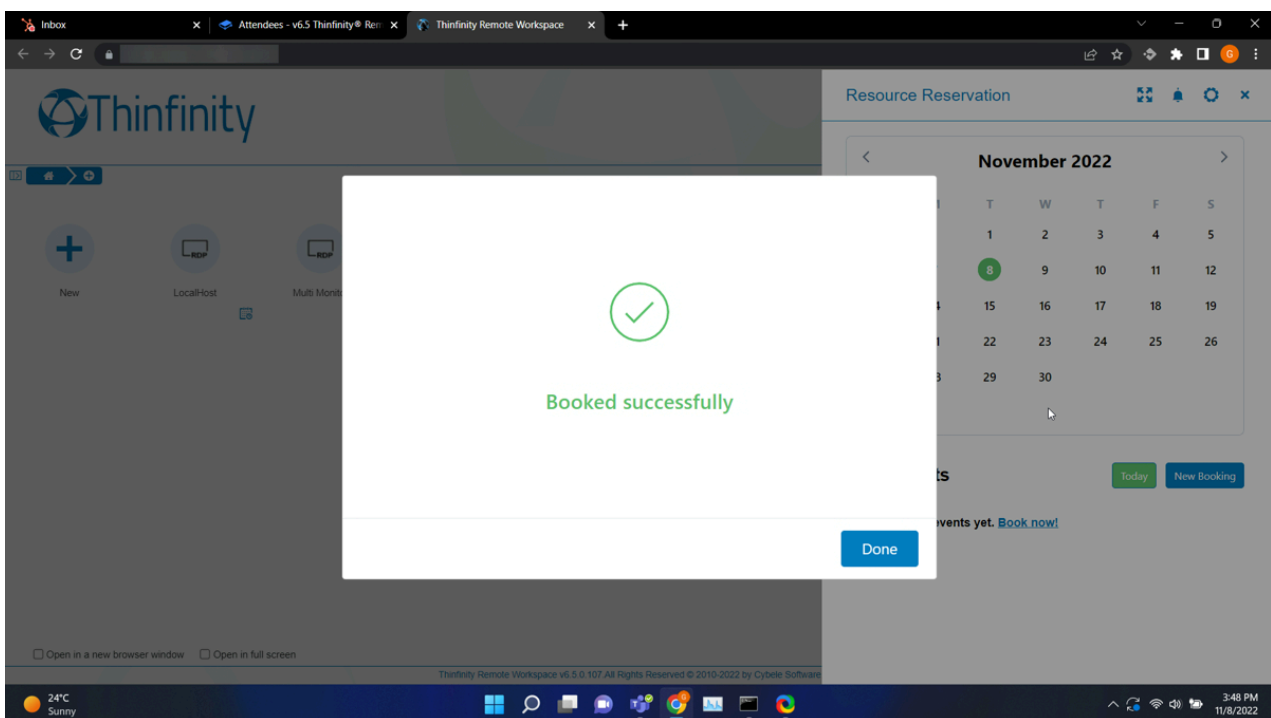
Select the time frame:



Fill the name for the booking:



After applying the changes you will get a confirmation message:



Below you will see how the page looks, once the booking is saved:

Inbox

Attendees - v6.5 Thinfinity® Re

Thinfinity Remote Workspace

+

←

→

↺

🔒

Thinfinity

12

🏠

➡

⚙

+

New

🖥

Local-Host

📄

🖥

Multi Monitor

?

Thinfinity Remote
Workspace Guide

🌐

Thinfinity Remote
Workspace Website

Resource Reservation

🔍

🔔

⚙

✕

<

November 2022

>

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Daily events

Today

New Booking

🕒

8

Nov

LocalHost

🕒 From 16:30:00 to 17:00:00

Organized by me

☐ Open in a new browser window

☐ Open in full screen

Thinfinity Remote Workspace v6.5.0.107 All Rights Reserved © 2010-2022 by Cybele Software

🌞 24°C Sunny

🪟

🔍

📁

🗂

📧

📅

📺

🎮

🌐

🔌

📶

📶

🔊

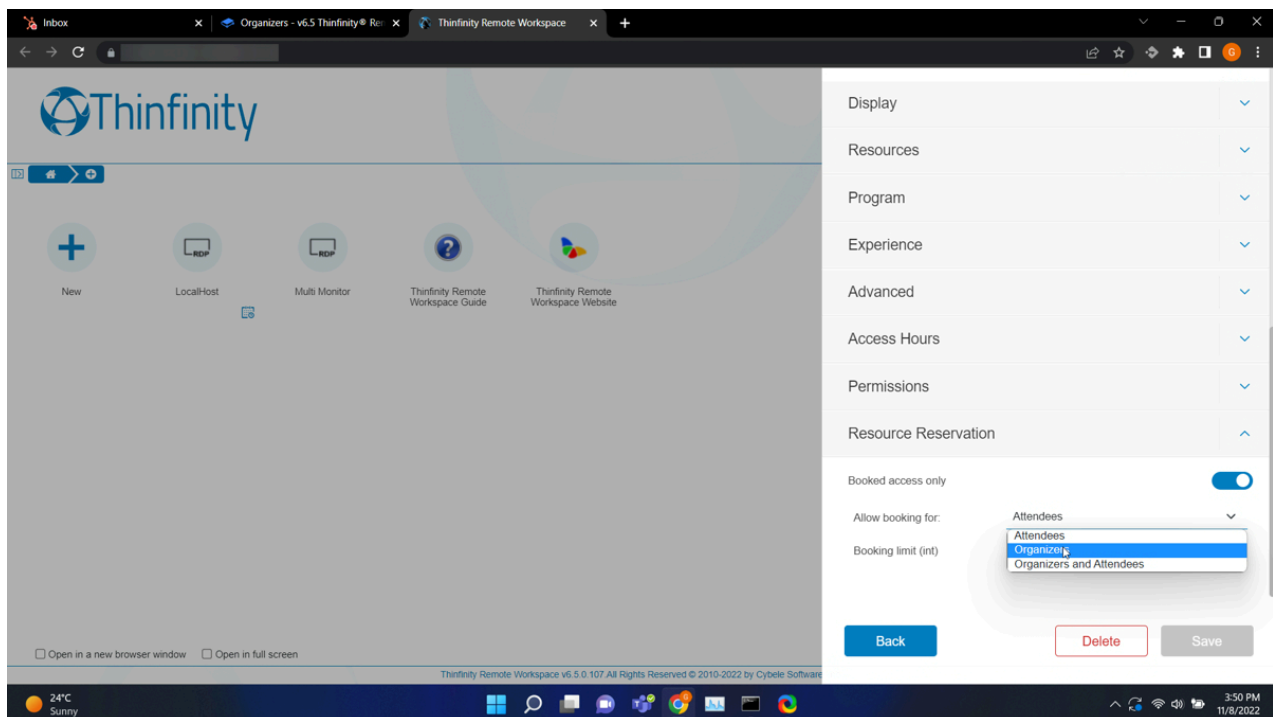
🔌

3:49 PM
11/8/2022

Organizers

To enable the Booking feature "to organizers only" we need to go first to the profile we want to use, and click on the "edit" button

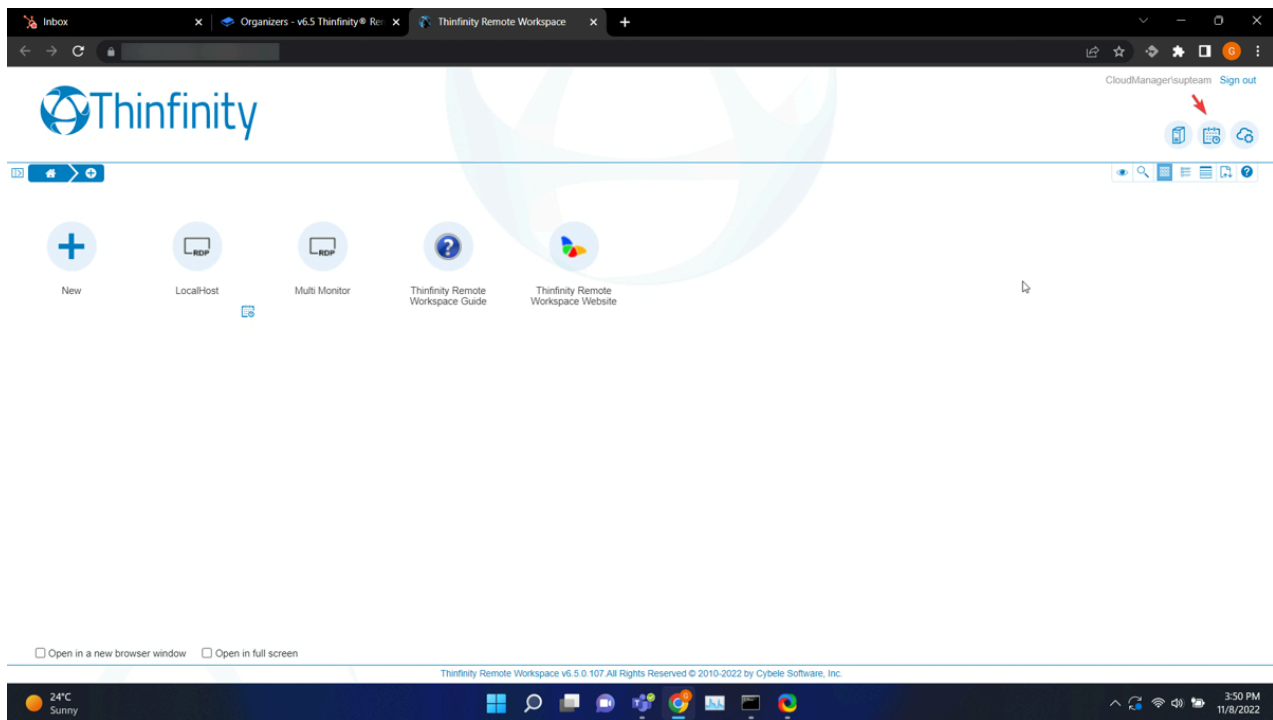
And in similar fashion to the "attendees only" option, got to the bottom of the options given, and in Bookings, select "Organizers"



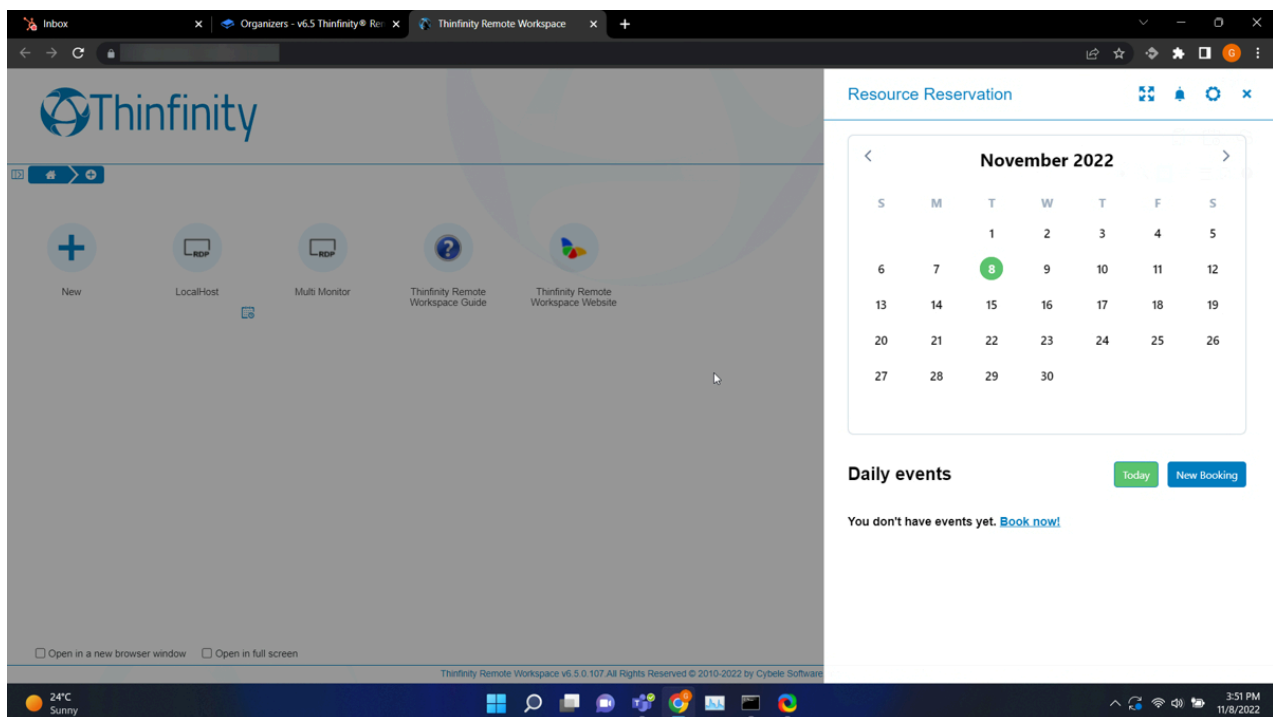
Bear in mind that is necessary to add a user as an organizer by clicking on "+ Add" before we can continue as organizers

How to schedule bookings as an organizer

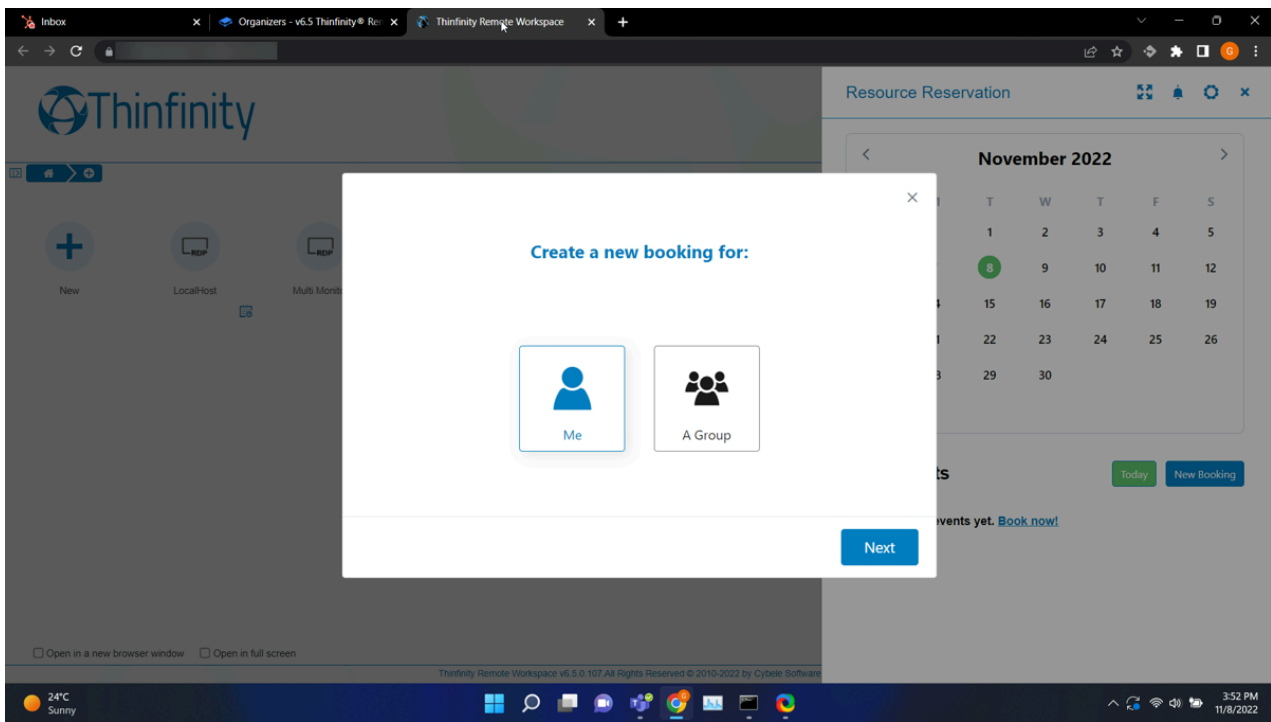
To make a new booking as an organizer first we need to click on the icon of the calendar, in the top right corner of the screen



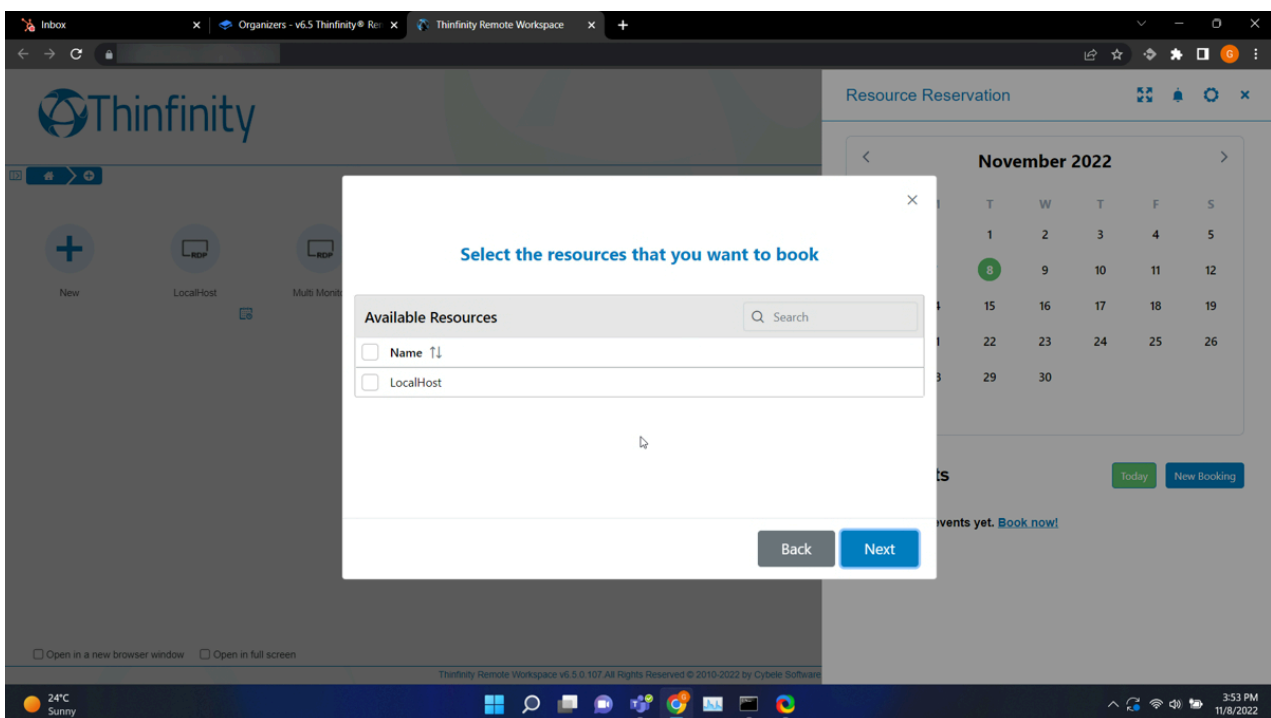
Then we will get the calendar to select the date:



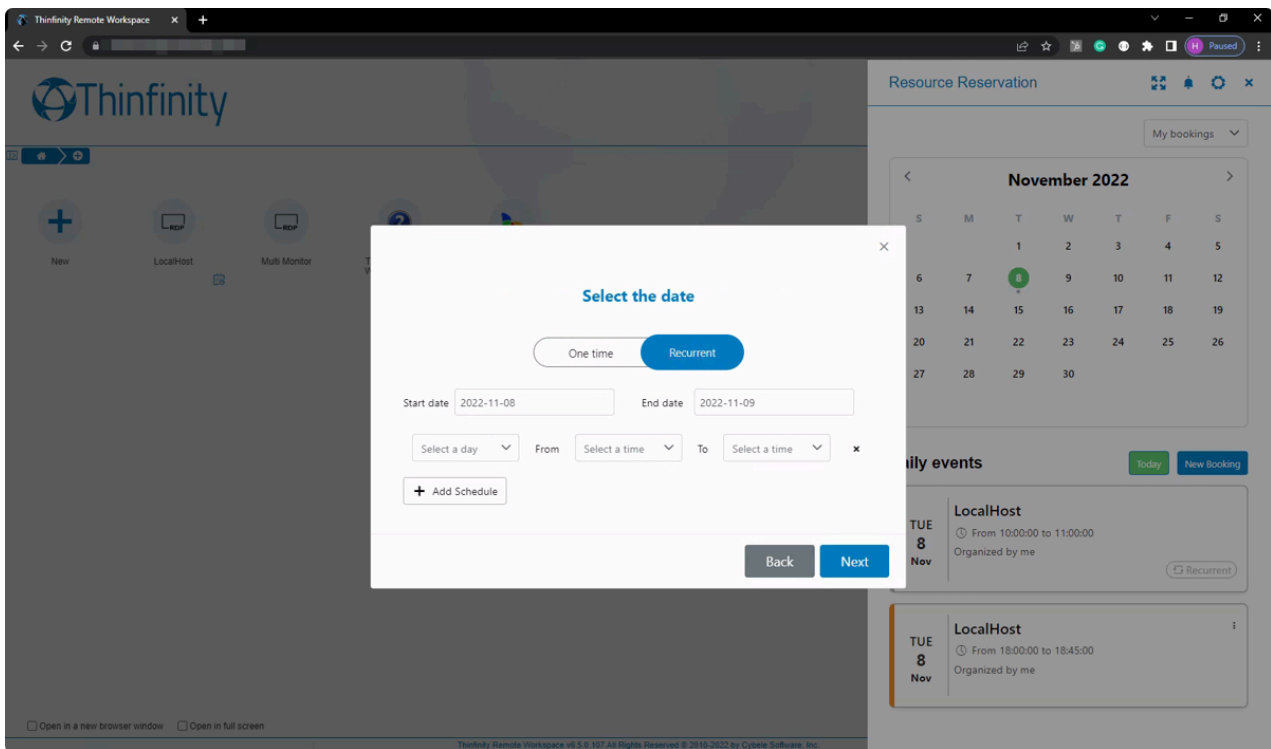
Select if it will be a booking for yourself or a group. In this example will show how to create a booking for a group:



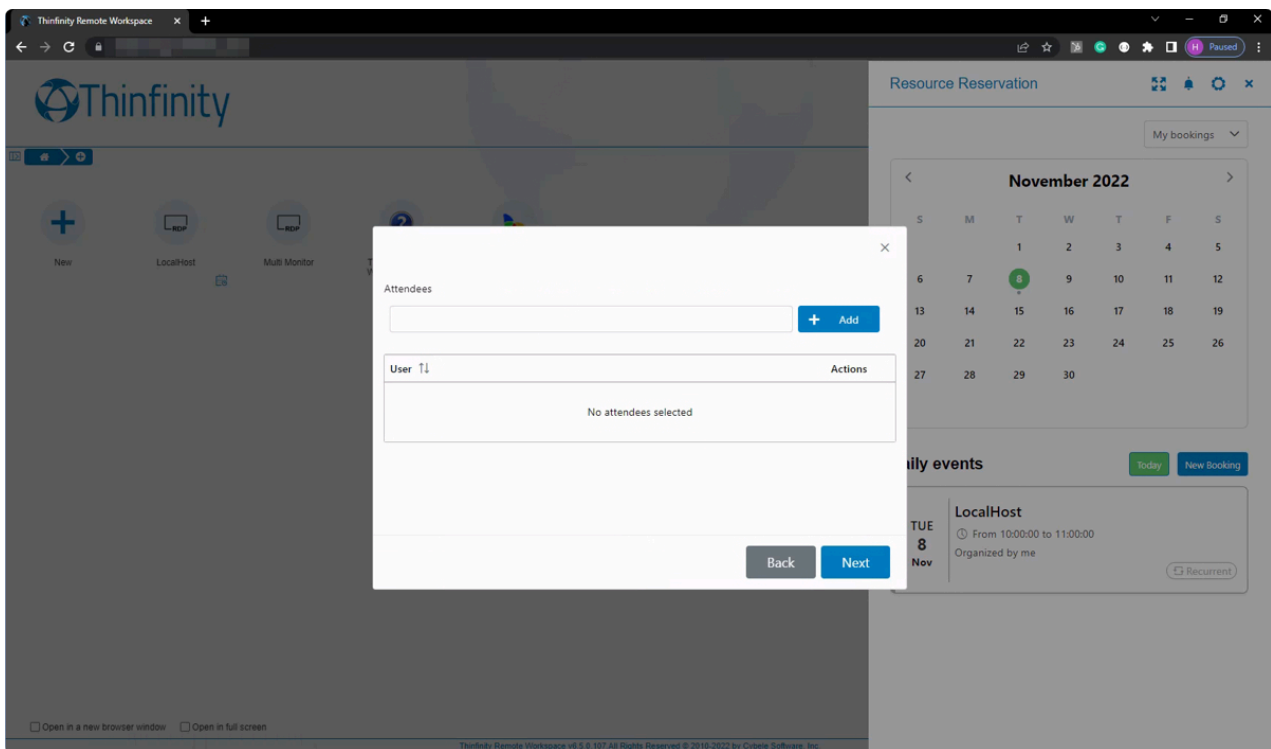
Select the resource you wish to book:



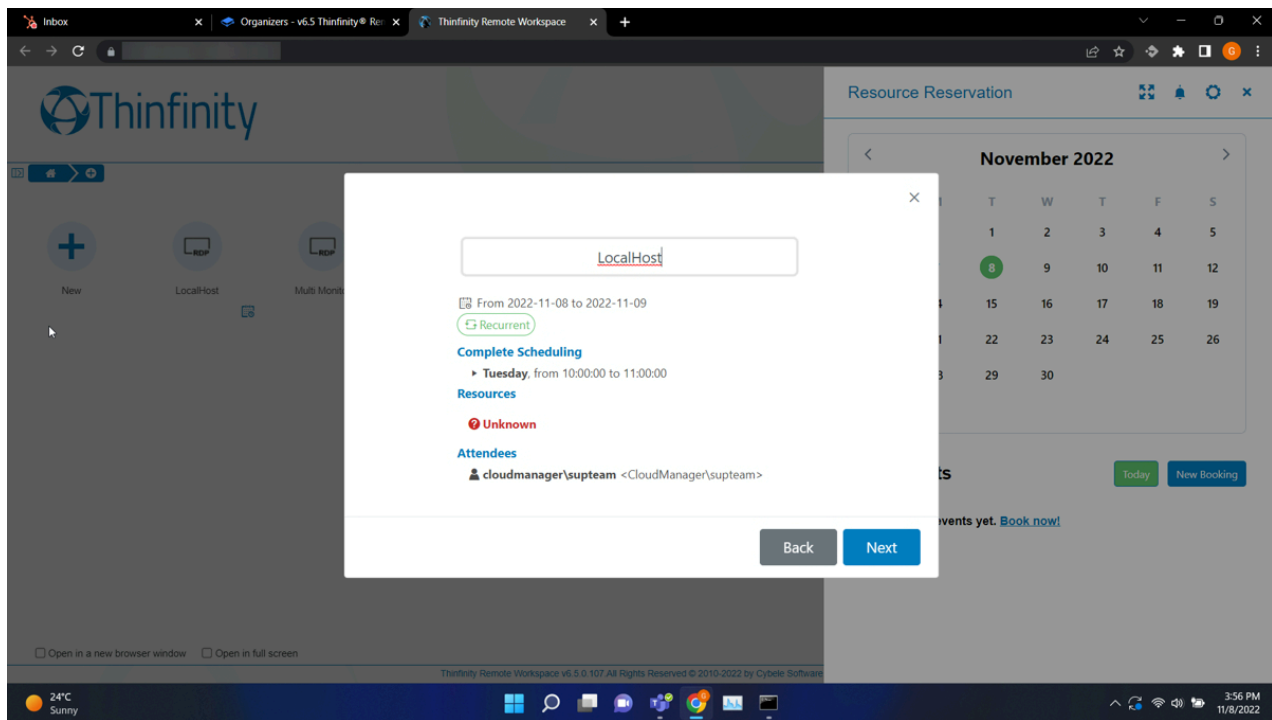
Select the date/schedule, for this example, will use the 'Recurrent' option:



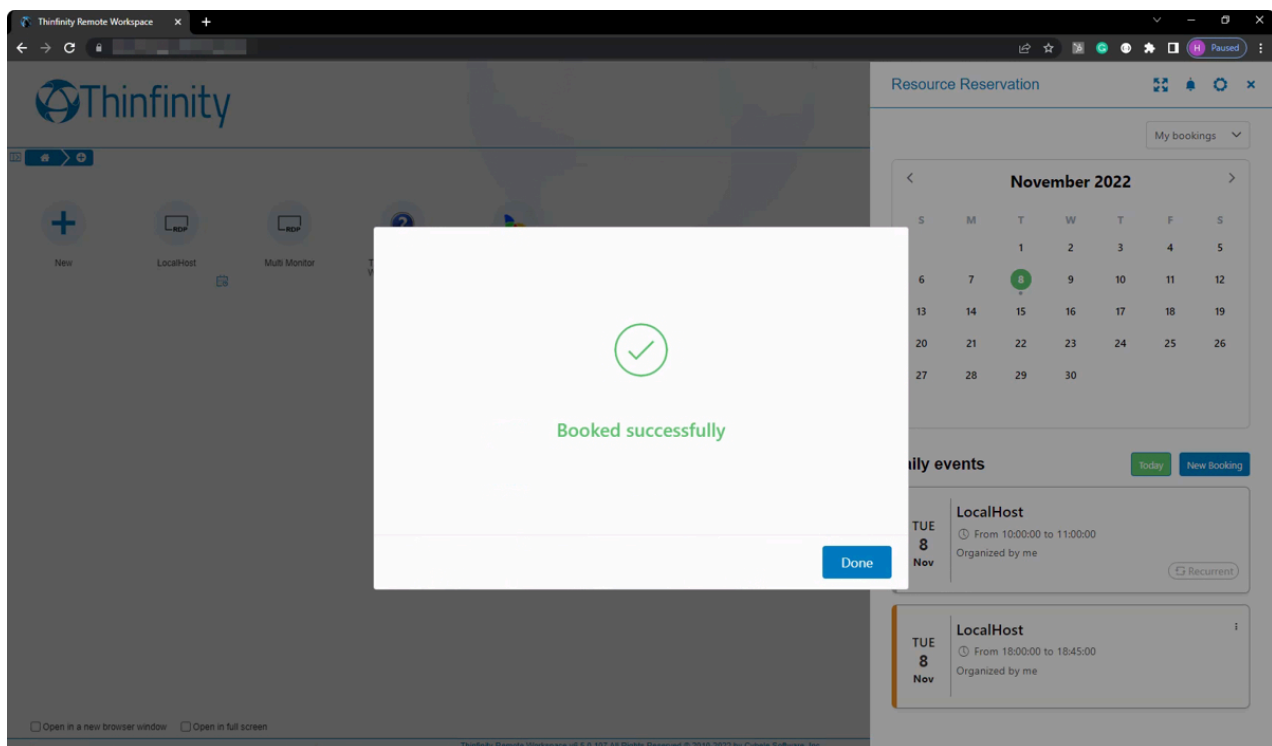
Add the attendees:



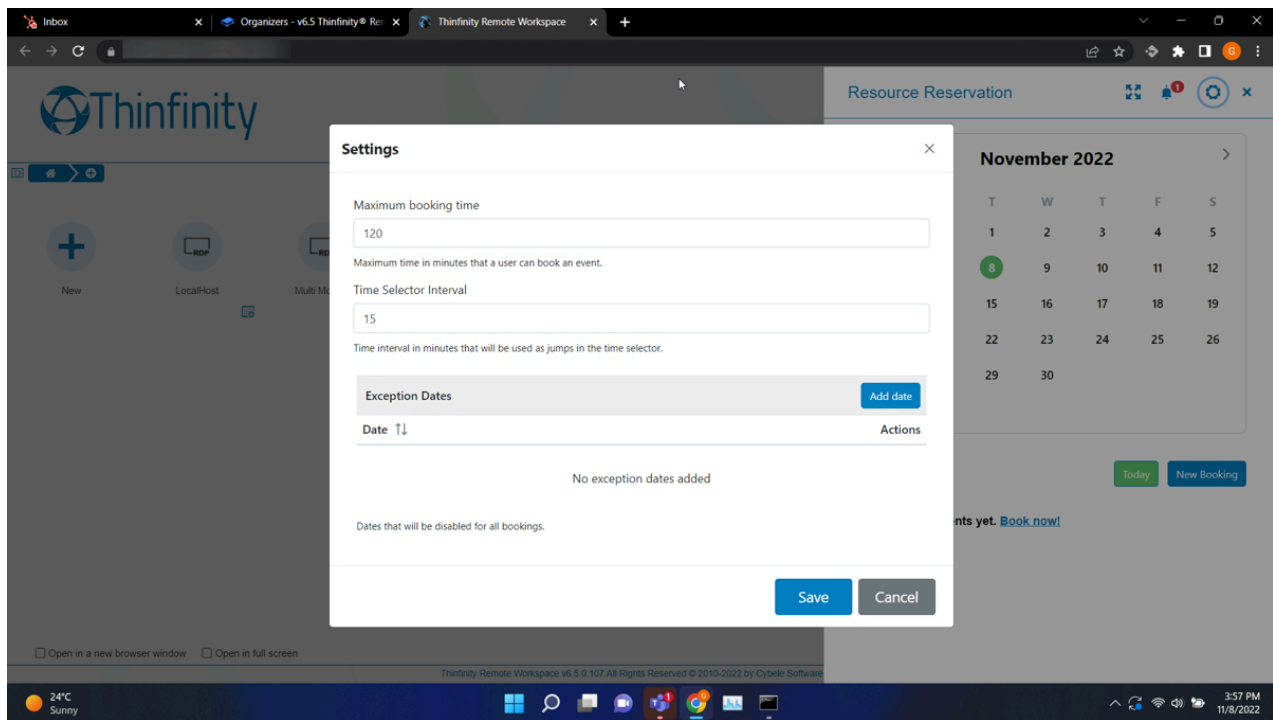
Fill the name for the booking:



After applying the changes you will get a confirmation message:



These are the settings you can change for each booking from the options in the 'Resource Reservation' panel:



User guide Section

User Guide

This section is a quick User Guide, focused on the everyday use of Thinfinity® Remote Workspace.

[Logging in](#)

[Accessing from Mobile Devices](#)

[Toolbar](#)

[Features](#)

[Disconnecting](#)

Features

These are some of the most important Thinfinity® Remote Workspace features:

[.File Transfer](#)

[.Remote Printer](#)

[.Remote Sound](#)

[.Share Session](#)

[.Mapped Drives](#)

[.Analytics](#)

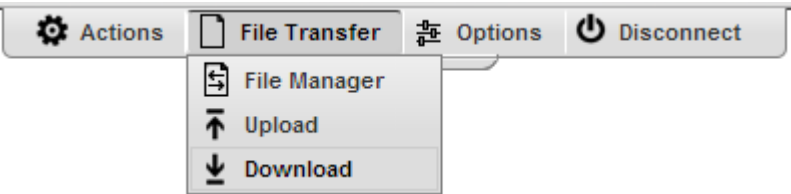
File Transfer

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.

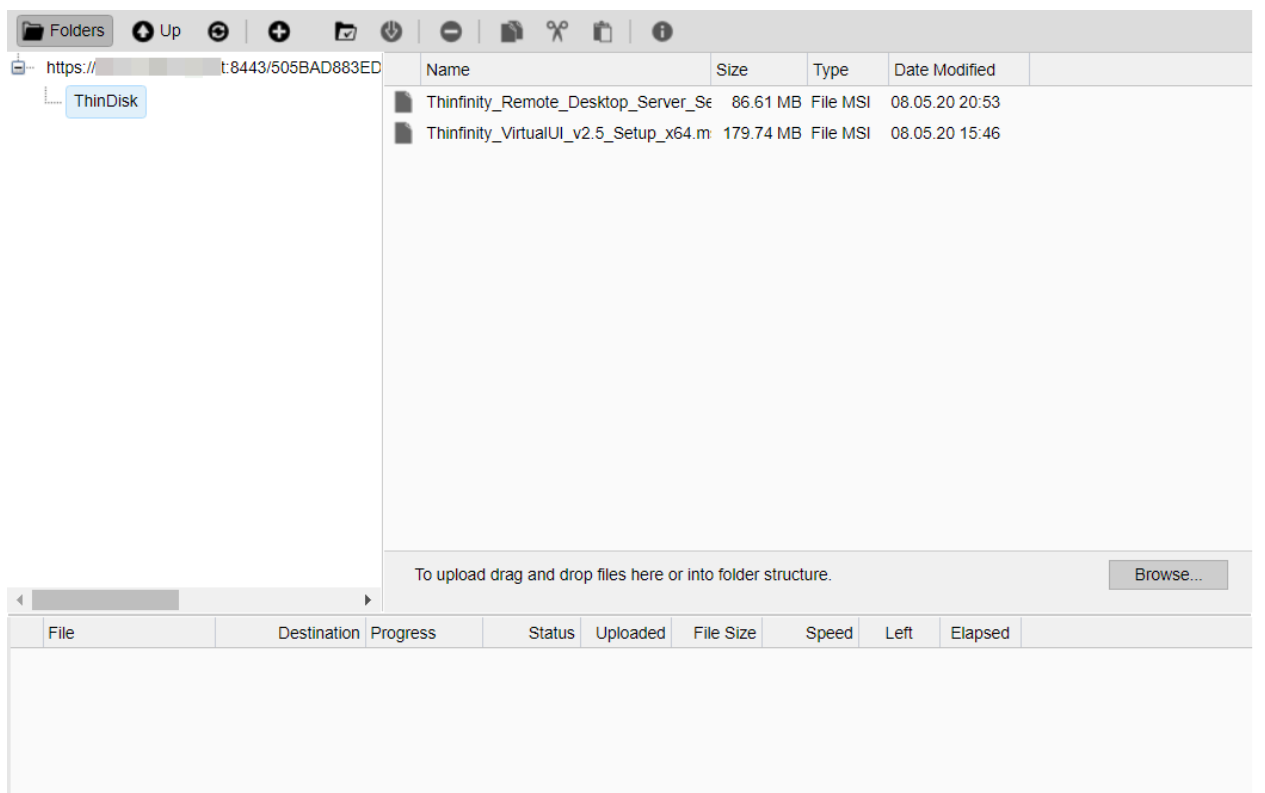


2. Click on the "File Manager" option, located inside the File Transfer toolbar option. If the button is not available ask the system administrator to set you the [permissions](#) for it.



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

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



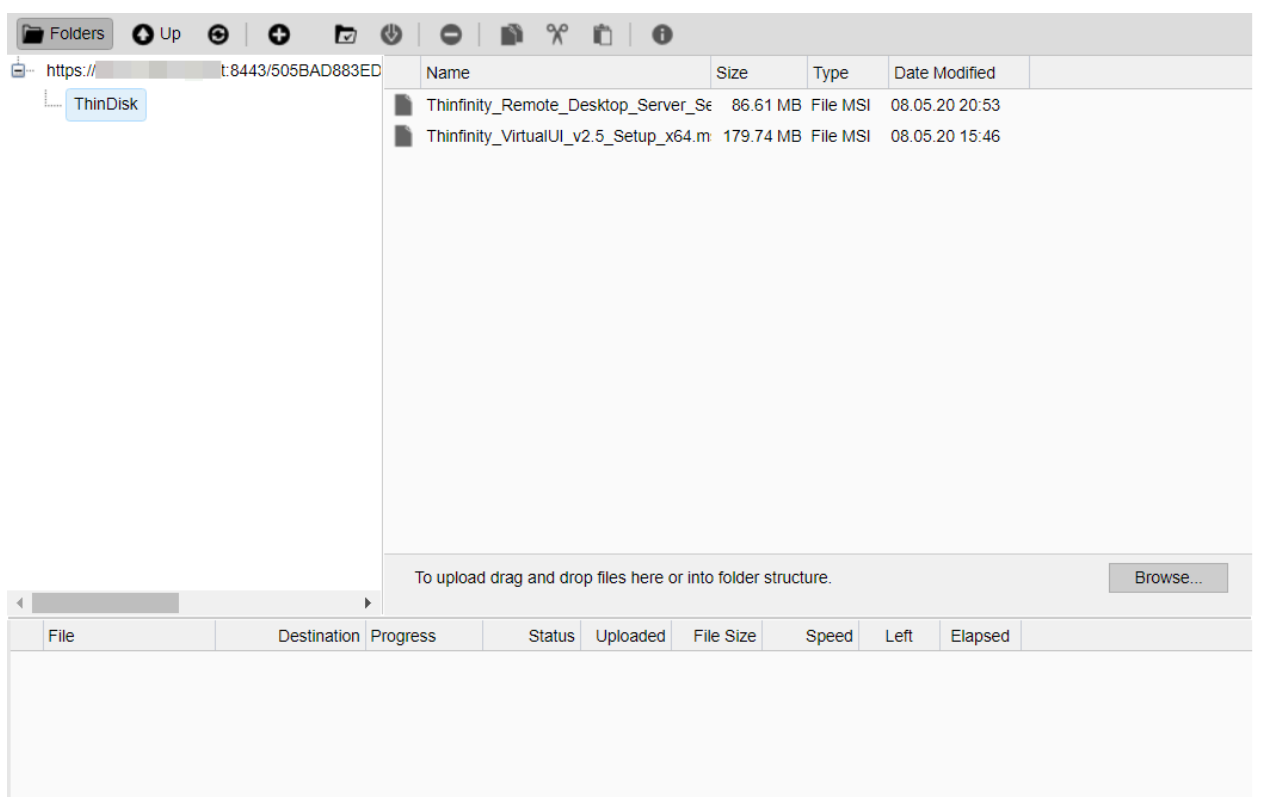
4. Observe that the "[Shared Folders](#)" and the "[Intermediate disk](#)" are the only remote directories available to exchange files with. If you need to [download or upload remote files](#) from the file manager, you should always move them first into these directories (they are going to be mapped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

Navigating

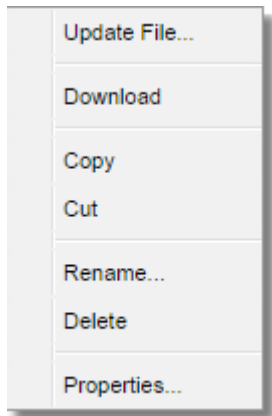
On the upper part of the screen you will see your remote files and folders. Browse to the remote location by double clicking on the folders on the right, or expanding the tree structure on the left.

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.



File Options



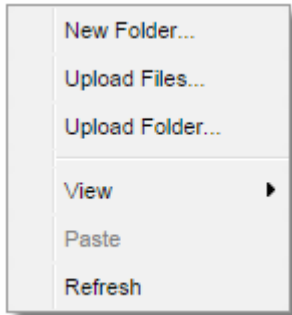
Right click on a remote file to access these options:

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.

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.

Downloading and Uploading files

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.

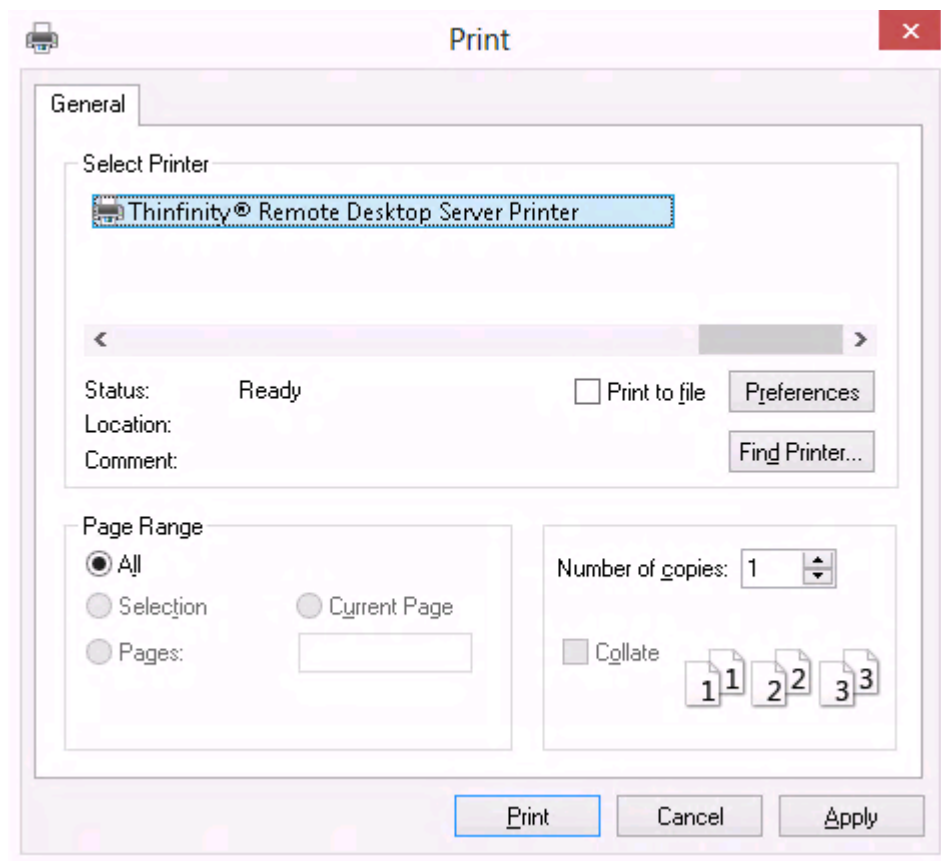
Uploading local files:

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.

Remote Printer

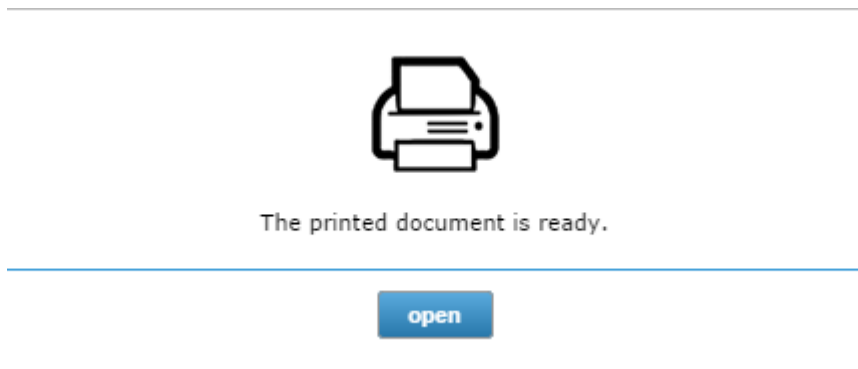
The Thinfinity® Remote Workspace Remote Printer allows you to print any remote document locally. If the Remote Printer is enabled to a connection, every time you print a document, the Thinfinity® Remote Workspace Printer will be shown among the list of available printers.

1. Open a remote document and try to print it.



2. Select Thinfinity® Remote Workspace 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.

Remote Sound

With Thinfinity® Remote Workspace 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.

Share Session

The "Share Session" feature allows users to share an active desktop connection with other users, so that they can see and interact with it in many ways.

The shared session will present the remote user exactly what is being shown on the local connection. It replicates the remote desktop image on the remote user browser and is updated continuously.

Follow the next steps and learn how to share your desktop connection with other users:

1. Open the desktop connection you want to share.
2. On the connection toolbar click on the Actions button and then on the "Share Session". If the button is not available ask the system administrator to set you the [permissions](#) for it.



3. A dialog will present you with the Sharing Address and password that should be used to access this same connection remotely.

Session sharing

Share this session with another user sending the sharing address and password.

Sharing Address:

`https://127.0.0.1:8443/oturl.html?skey=537614C9-3E92-44D2-9A36-1425E82D55DF`

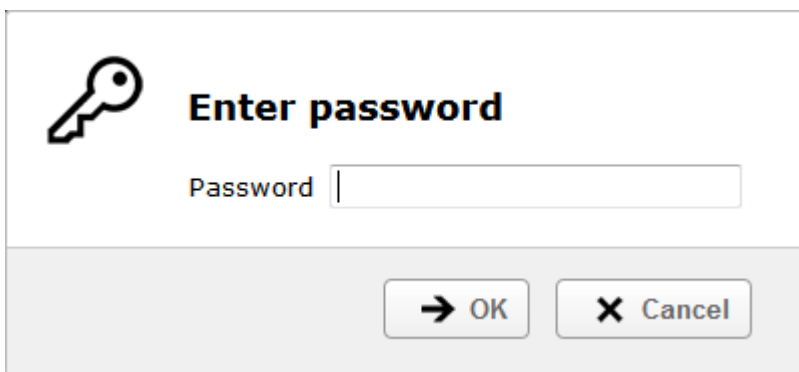
Password:


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



 **Enter password**

Password

→ OK × Cancel

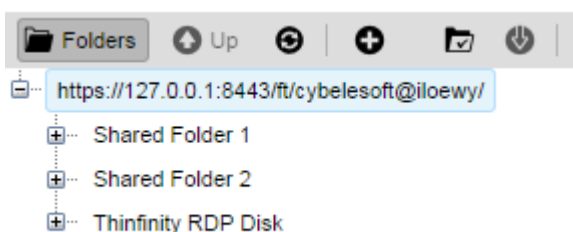
3. You should now be able to see and interact with the previously shared connection.

Mapped Drives

Mapped Drives

In order to exchange files with the remote machine, Thinfinity® Remote Workspace 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.



Thinfinity® Remote Workspace maps two kinds of directories:

Intermediate disks

The intermediate disks are directories created by Thinfinity® Remote Workspace 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 Workspace as an "anonymous user".

Shared Folders

The Shared Folders are network directories accessible by all Thinfinity® Remote Workspace 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.

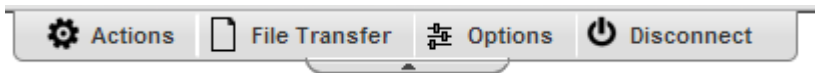
If you need to [download or upload remote files](#) you should always move them first into these directories (they are going to be mapped drives also), and after that transfer to the desired location.

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.