



VDI

Remote Application & Remote Desktop Configuration Guide

Version 5.4.0



Change Log

Date	Change Description
August 6, 2019	Remote Application & Remote Desktop Configuration Guide.

CONTENT

Chapter 1	1
1 Introduction.....	1
1.1 Document Description	1
1.2 Objective	1
1.3 Abbreviations and conventions	1
1.4 Using feedback	1
2 Application Scenario	1
3 Condition Description	1
4 Configuration.....	2
5 Configuration method	2
5.1 Configuring Terminal Server	2
5.2 Publishing remote application	4
5.3 Publishing remote desktop.....	6
5.4 Creating new user	7
5.5 Associated roles	8
5.6 Editing group policy	9
5.7 Test Login.....	11
6 Precautions.....	12

Chapter 1

1 Introduction

1.1 Document Description

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR, SINFOR and logo are the trademarks of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Inc.

1.2 Objective

This configuration guide document is mainly applicable to the following engineers.

- Network or application manager.
- On-site technical support and maintenance personnel.
- Network administrator that responsible for network configuration and maintenance.

1.3 Abbreviations and conventions

In this article, the terminal server refers to the Windows Server server that publishes the application.

The VDCs in this document refer to SANGFOR VDC (Virtual Desktop Controller).

1.4 Using feedback

If you find any problems with this information during use, you can give us feedback through the community portal: bbs.sangfor.com.cn

Thank you for your support and feedback, we will do better!

2 Application Scenario

1. For the C/S mode application system, the user terminal does not need to install the client application, and after accessing the VDI, the service can be served. The application system on the device side is used. Reduce the limitations of C/S application usage and improve ease of use.
2. Some B/S architecture applications need to be installed in the client browser to access the plugin, but the plugin is not compatible with the phone or tablet, does not support installation, etc., and can be used by remote application publishing.

3 Condition Description

1. VMP and VDC has been set up.
2. Windows Server for installing and publishing applications. This test guide uses win2016 as an example.
3. Publish Remote Desktop. Skip step 5.1 to configure the terminal server and go directly to step 5.3 to publish the remote desktop.

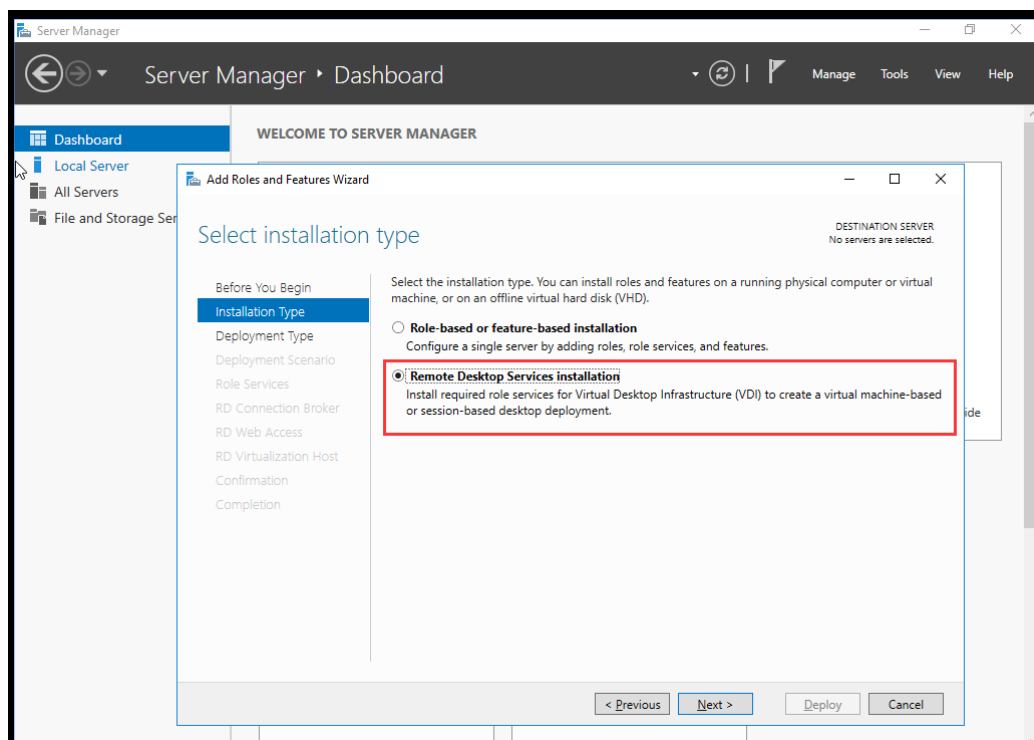
4 Configuration

1. Configure the terminal server.
2. Release remote application.
3. Release remote desktop.
4. New users.
5. Role authorization.
6. Edit group strategy.
7. Terminal access use.

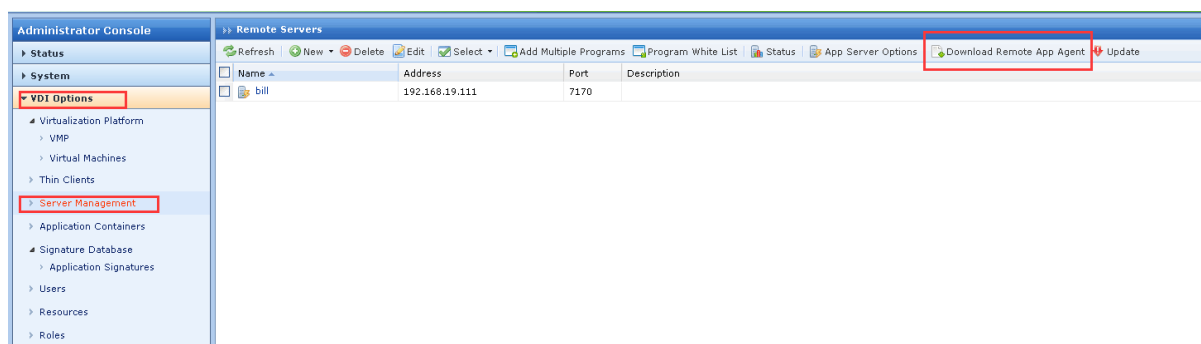
5 Configuration method

5.1 Configuring Terminal Server

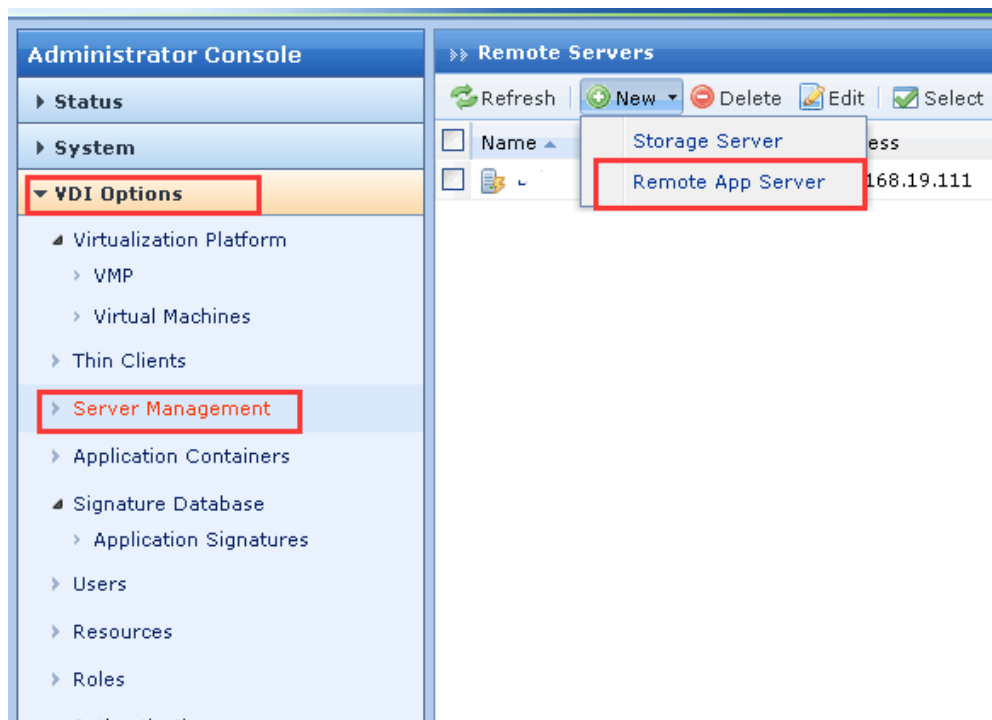
1. Install terminal service and authorization in win2016, follow the prompts to complete the installation.



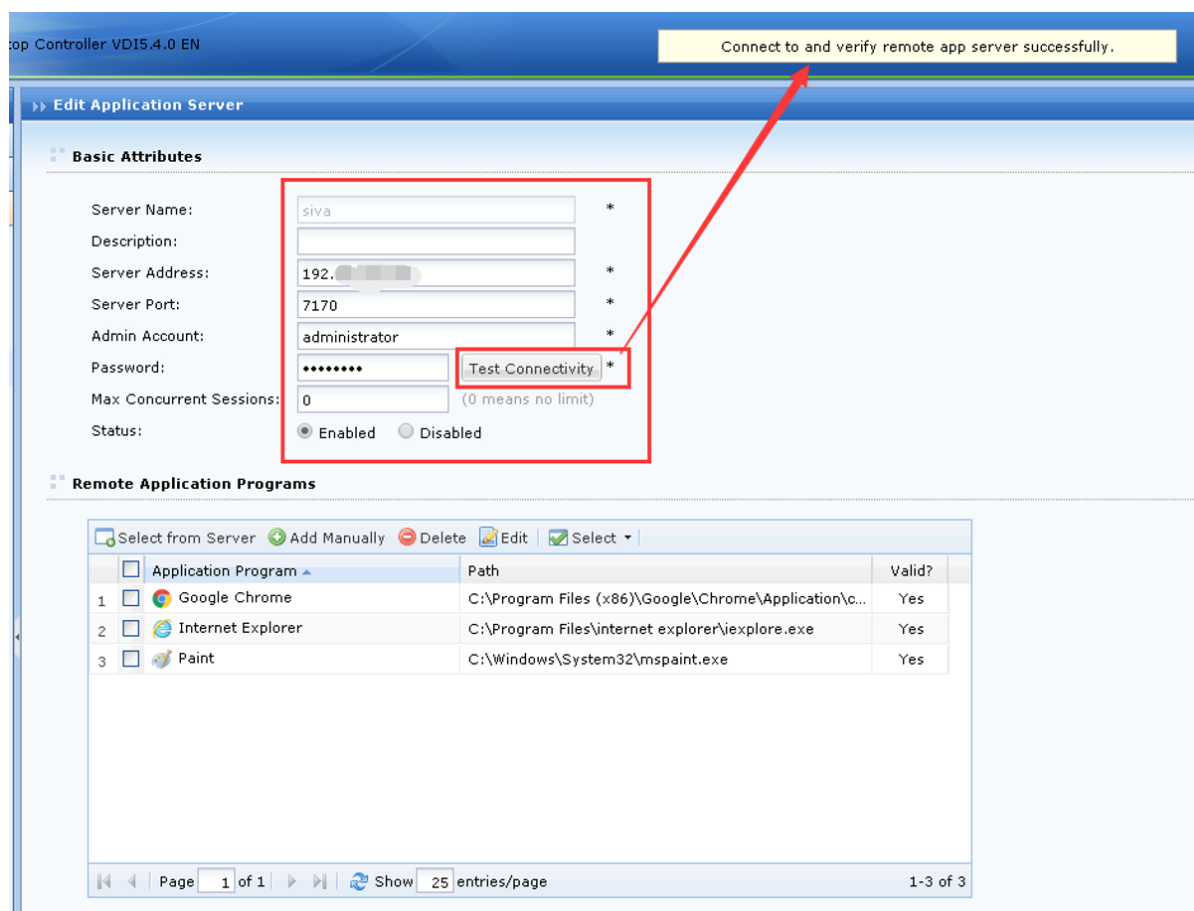
2. Log in to VDC, and download the terminal server program SFRemoteAppServerInstall.exe into win2016.



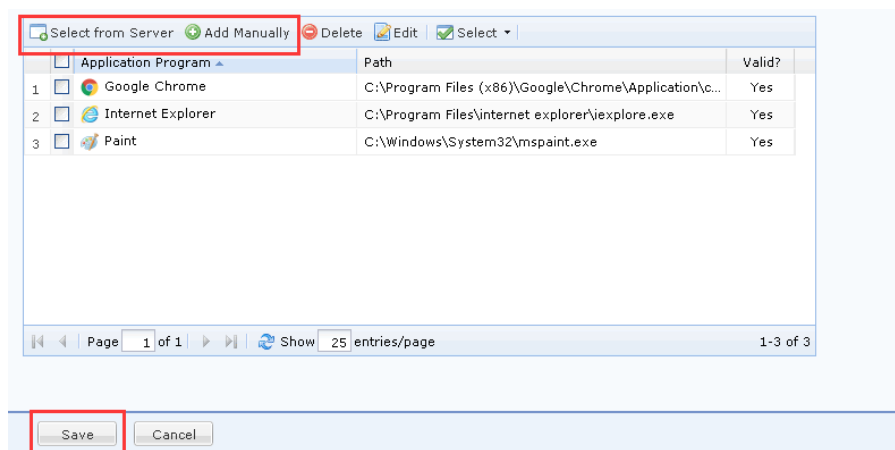
- Go to Server Management and Remote App Server.



Fill in the Remote App Server name, Windows Server IP address, username and password, and click "Test Connection" to test the connection with the terminal server.

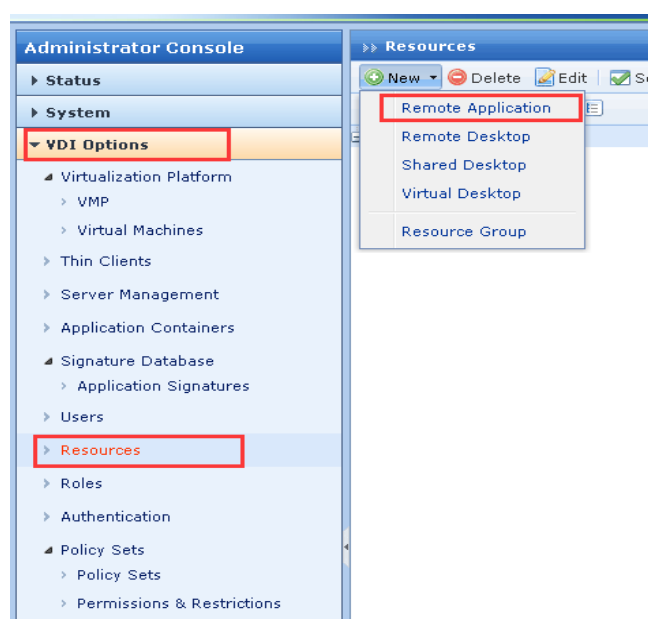


Choose preset application from [Select from Server] if the application is not in the list, select [Add Manually] and provide the path. Lastly click [Save].



5.2 Publishing remote application

New remote application.



Take the publish of Chrome browser as an example. The program selected must be a preset or program added when the resource server is created. The Command Line Argument refers to what is opened by default after opening this program, such as www.sangfor.com filled in here, after opening Chrome in remote application mode it will automatically opens www.sangfor.com. Check the resource server that publishes the current resource.


Basic Attributes

Name: Chrome *

Description:

Area: All/Default area/ >> ⓘ

Added To: Default group >>

Icon: 

☒ Enable resource

Program: Google Chrome Select

Working Directory:



Command Line Argument: <https://www.sangfor.com/>

☒ Maximize window after program is launched

☐ Single instance is allowed (for an application running on remote server, not allow user to run a :

App Server SSO License

Select a remote application server to deliver this resource.

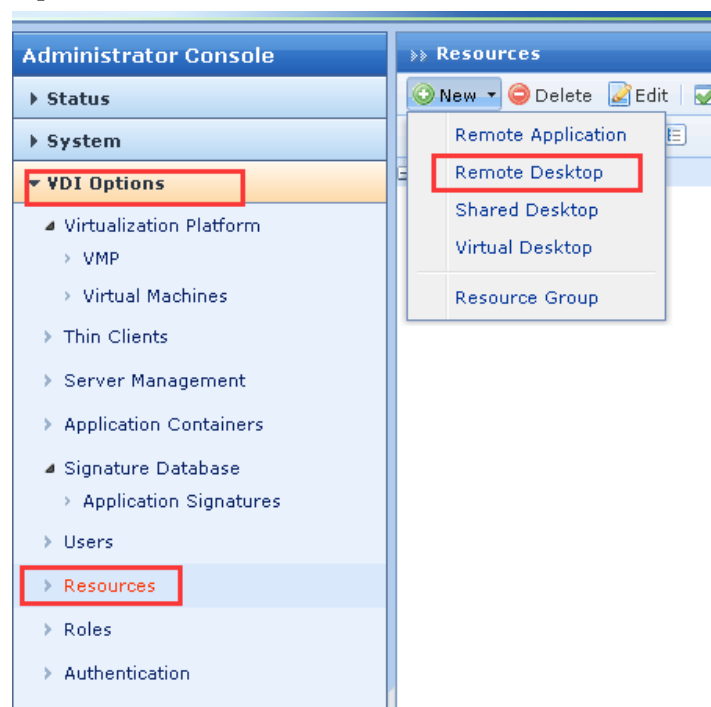
<input type="checkbox"/>	Server Name	Occupied	IP Address	Status
<input type="checkbox"/>			192.168.1.111	Online
<input checked="" type="checkbox"/>			192.168.1.208	Online

Page 1 of 1 Show 25 entries/page 1-2 of 2

Save and Add Save Cancel

5.3 Publishing remote desktop

Add new remote desktop.

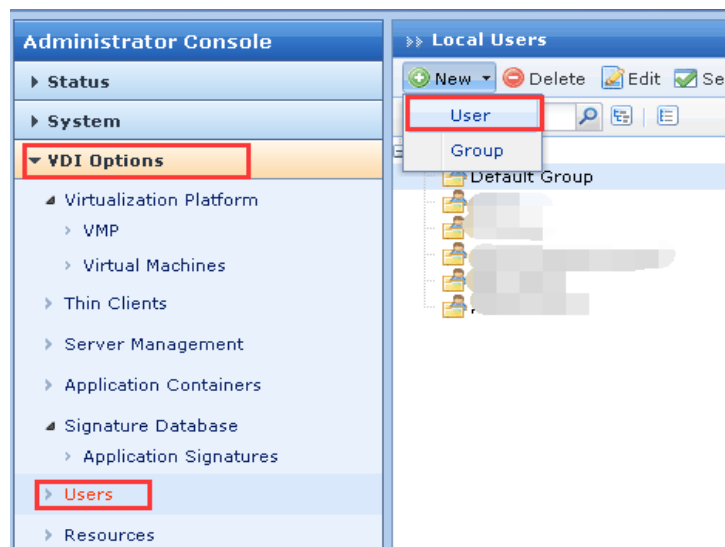


Configure resource name, address, and port.

The screenshot shows the 'Basic Attributes' configuration window. The 'Name' field is set to 'RDesktop', 'Description' is empty, 'Added To' is 'Default group', 'Area' is 'All/Default area/', 'Address' is '192.168.1.208', and 'Port' is '3389'. These fields are grouped together and highlighted with a red box. Below these fields is an 'Icon' section with a computer icon and a checked 'Enable resource' checkbox. At the bottom, the 'Save and Add' button is highlighted with a red box, along with 'Save' and 'Cancel' buttons.

5.4 Creating new user

The VDC performs access control by user authentication. If an end user needs to access the access resource, he/she needs to add the user first and specify the authentication mode.

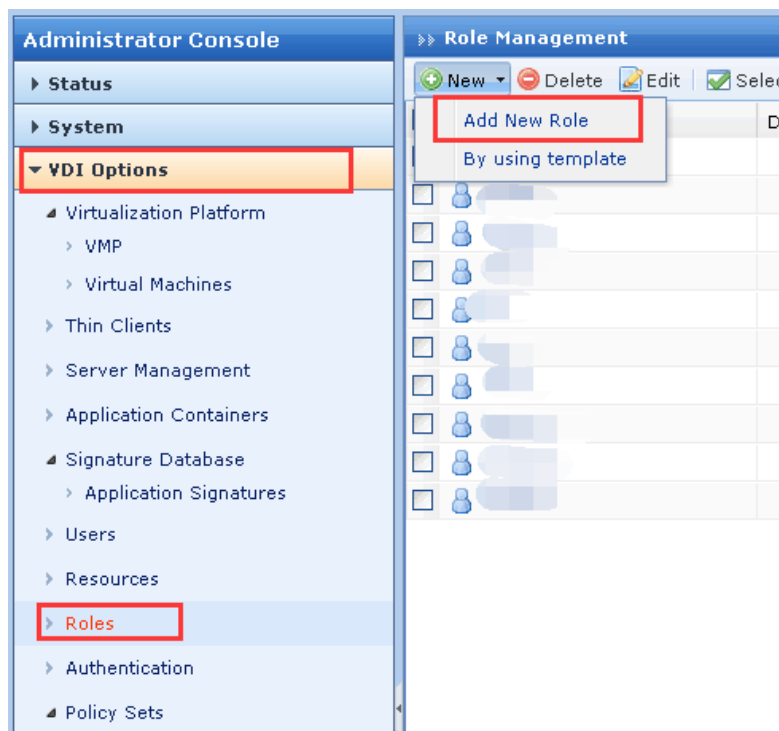


Enter the user Name, Password and be sure to Save it.

The image displays the 'Basic Attributes' form for user creation. It includes input fields for 'Name', 'Description', 'Password', 'Retype Password', 'Mobile Number', and 'Added To'. There are also checkboxes for 'Inherit parent group's attributes', 'Inherit authentication settings', and 'Inherit policy set'. The 'Authentication Settings' section has options for 'Primary Authentication' (Local password, Certificate/USB key, External LDAP/RADIUS) and 'Secondary Authentication' (Hardware ID, SMS password, Dynamic token). The 'Policy Set' section has a dropdown for 'Policy Set'. The 'Assigned Roles' section has a dropdown for 'Roles' and a 'Create and Associate' button. At the bottom, there are 'Save' and 'Cancel' buttons, with the 'Save' button highlighted by a red box.

5.5 Associated roles

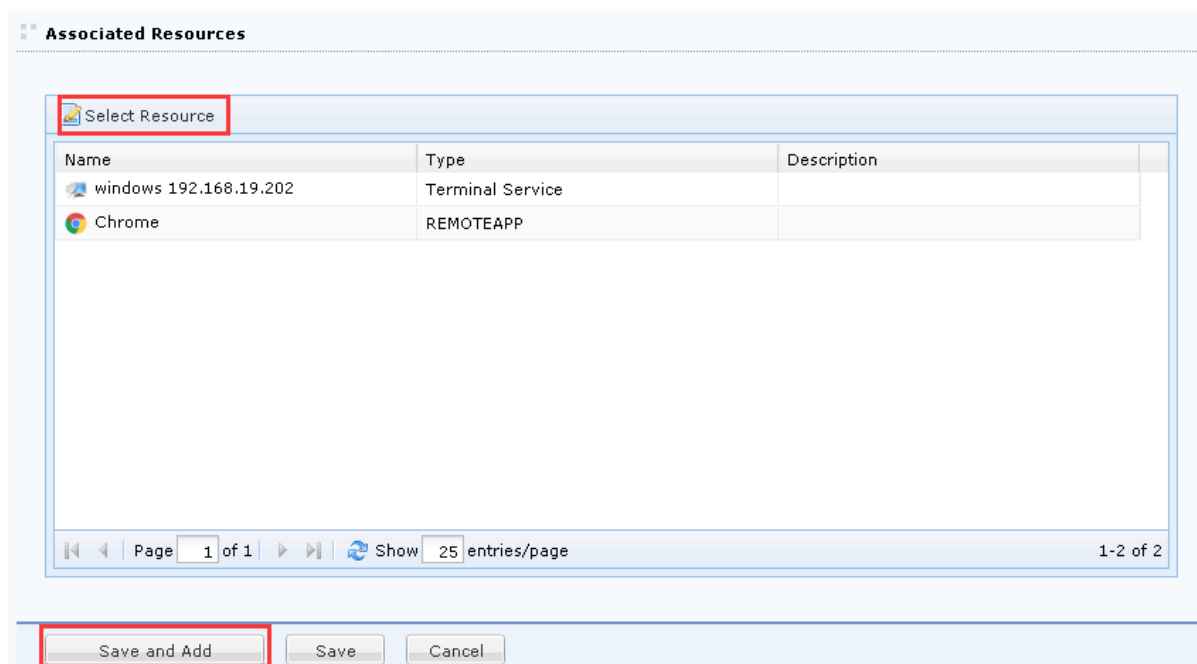
The VDC restricts the desktop resources that users can access through role authorization. A user can associate multiple roles. A resource can also belong to multiple roles at the same time.



A resource that a user can access is a collection of resources included in the associated role.

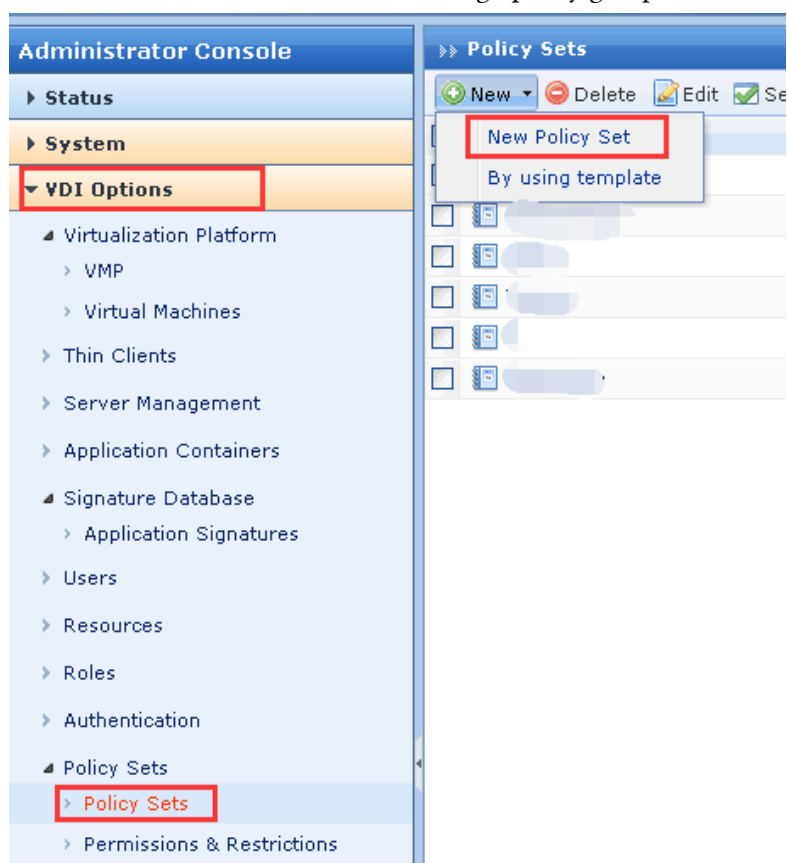
The screenshot shows the 'Basic Attributes' form for configuring a role. The form includes the following fields and controls:

- Name:** A text input field with a red box around it and an asterisk (*) indicating it is required.
- Description:** A text input field.
- Area:** A dropdown menu showing 'All/Default area/' with a red box around it and an information icon (i).
- Assigned To:** A text input field with a red box around it and a 'Select User' button to its right.
- Security Policy:** A text input field with a 'Select Role-level Policy' button to its right.
- Enable Role:** A checkbox that is checked.



5.6 Editing group policy

The VDC manages user access control over resources through policy groups.



Basic Attributes

Name: *

Description:

Area: All/Default area/

Policy Options

Account Options Virtual Desktop Options Remote App & Shared Desktop

Logon to Remote Server

User Account:

Type: ☒ User privilege ☐ Admin privilege

Deletion: ☐ On removing user from local device, remove account and related data from remot

Allow Use of Local Devices/Resources in Remote Session

Each user associates the default policy group by default, or you can associate a new policy group with the user for flexible management.

Edit User

Basic Attributes

Name: *

Description:

Password:

Retype Password:

Mobile Number:

Added To:

Area: All/Default area/

☐ Inherit parent group's attributes

☒ Inherit authentication settings

☐ Inherit policy set

Authentication Settings

Primary Authentication

☒ Local password

☐ Certificate/USB key

☐ External LDAP/RADIUS

Require: ☒ Both ☐ Either

Secondary Authentication

☐ Hardware

☐ SMS pas

☐ Dynamic

Policy Set

Policy Set:

Assigned Roles

Roles:

Policy Sets

Edit

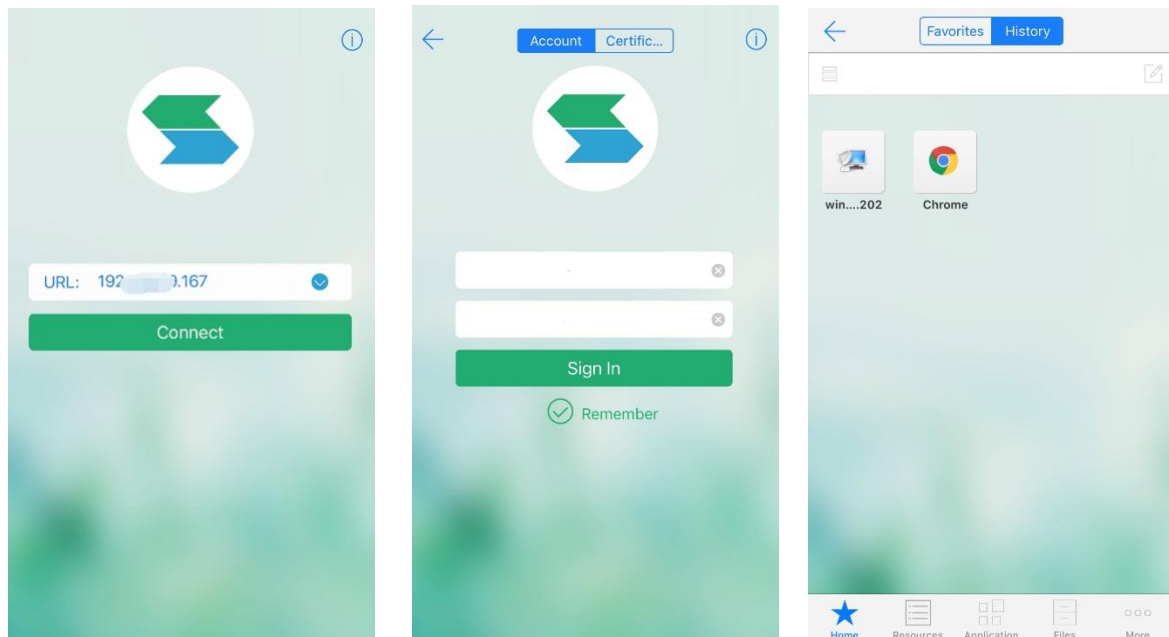
Name
<input checked="" type="checkbox"/> Default policy set
<input type="checkbox"/> <input type="text"/>
<input type="checkbox"/> <input type="text"/>
<input type="checkbox"/> <input type="text"/>
<input type="checkbox"/> <input type="text"/>
<input type="checkbox"/> <input type="text"/>

Page 1 of 1

5.7 Test Login

In order to better see the effect, this test takes the mobile terminal as an example. On the mobile terminal of Android or iOS, the mobile access resource can be access by installing the EasyConnect application.

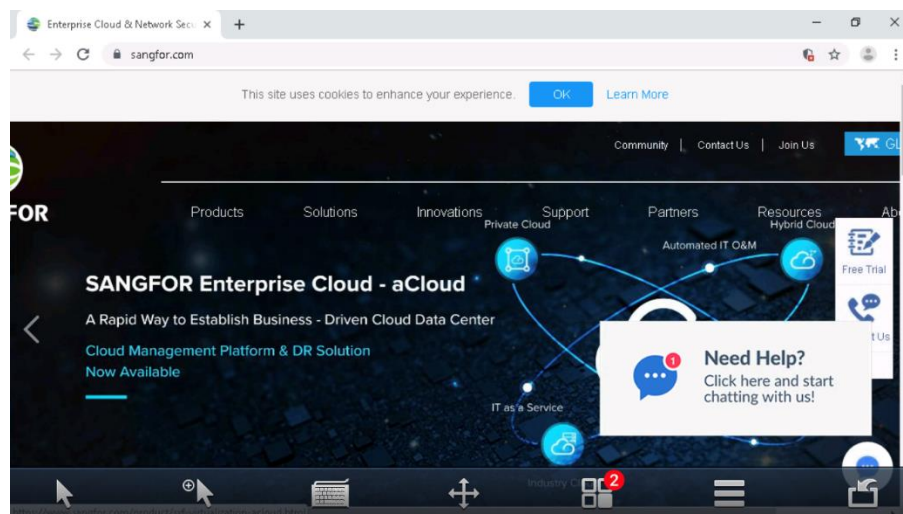
First Enter the URL for login, then enter username and password, and you will see the resource created.



To enter the Remote Desktop, click on its icon, then enter Windows username and password to continue.

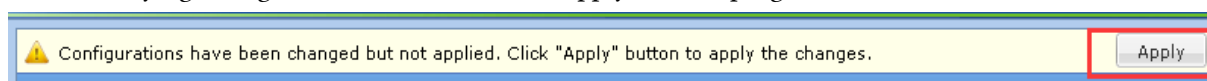


After testing, select "Chrome browser". The Chrome browser should automatically opens www.sangfor.com as configured in the parameter earlier.



6 Precautions

1. After modifying configurations, be sure to click Apply at the top right of the screen.



2. Windows Server system needs to be activated, otherwise the remote application resources may not work properly.
3. VDC and Windows Server use TCP 7170, TCP 7171, TCP 7172 port for communication, The device that passes through the Windows firewall and the intermediate network must allow the port to communicate.
4. If the Windows Server terminal server is added to the AD domain, the terminal server user name needs to fill in the domain suffix. Eg: administrator@sangfor.com
5. Print Spooler and Secondary Logon services need to start on Windows Server, otherwise the terminal server program SFRemoteAppServerInstall.exe installation will fail.
6. It is recommended to ensure that the network between the VPN device and the terminal server has no NAT environment during deployment. Otherwise, the remote application will be abnormal.



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc

