

## How to Configure SSL VPN Applications for RDP

<https://campus.barracuda.com/doc/50266314/>

When accessing an application resource via CudaLaunch, an SSL tunnel is created that connects your client with the SSL VPN. Then, the native RDP client automatically launches and connects. The native RDP app creates an SSL tunnel from a random port on 127.0.0.1 to the port 3389 on the destination Windows server or PC behind the firewall. The native RDP client is automatically launched and supplied with the connection information. It is not possible to configure single sign-on for native RDP apps. To use application resources you must have a Remote Access Premium subscription.

### Before you begin

Enable the SSL VPN service and CudaLaunch. For more information, see [How to Enable SSL VPN and CudaLaunch](#).

### Create an application resource

Create an application resource to give your end users direct access to an internal application. Application tunneling allows tunneling of application data to the user's localhost IP address.

1. Go to the **VPN > SSL VPN** page and click the **Resources** tab.
2. In the **Applications** section, click **Add Application**.
3. In the **Add Application** window, set **Enable** to **Yes**.
4. (optional) Click **Browse** to upload a PNG file for the web portal, less than 30 kB and not larger than 80x80 pixels.
5. Enter the visible **Name**. This is the name used in the web portal for this application.
6. In the **Target Server** field, enter the IP address of the server hosting the application.
7. From the **Application** drop-down list, select the protocol that the target server is providing.
8. (optional) To override the application's standard port, enable **Port Override** and specify the **Port** to be used instead of the application's standard port.

## Add Application ?

Enable: ☐ Yes ☒ No

Icon:     
PNG File, less than 30kB and not bigger than 80x80 pixel.

Name:   
Name displayed in the SSL-VPN portal page

Target Server:

Application:

Port Override: ☐ Yes ☒ No

Port:

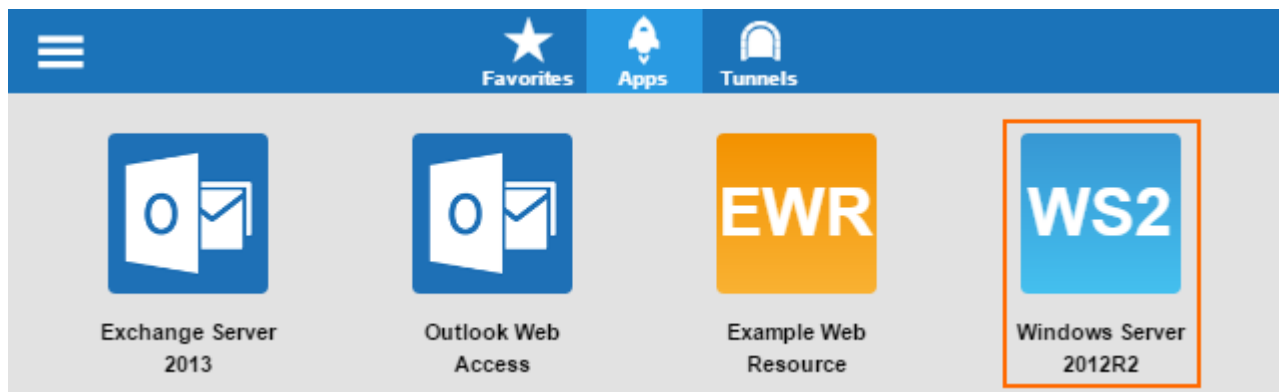
Client Loopback TCP Port:   
Use zero as local loopback port to use a randomly chosen port.

Allowed Groups:     
Use \* as a wildcard

- To enable tunneling of application data to the user's localhost IP address 127.0.0.1:7000, enter the **Client Loopback TCP Port** number for the application tunnel. To use a random port, enter 0 (default).
- (optional) To restrict access to the application by user group, remove the \* entry in the **Allowed User Groups** list. Enter the user groups that can access the application, and click + after each entry. If no groups are added, the application will not be accessible by any users. You can use question marks (?) and asterisks (\*) as wildcard characters.
- Click **Save**.

## Launching an RDP application

- Start CudaLaunch.
- In the **Apps** tab, click on the configured app.



The native RDP client starts automatically and connects to the remote Windows server.

## Figures

1. ssl\_res\_03.png
2. sslvpn\_native\_rdp\_03.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.