

RDP App Publisher

A remote application publisher and load-balancer
by
buildIT IT-Solutions BV

Table of Contents

Installation.....	3
Configuration of the Terminal Servers.....	3
Enable the Remote Registry Service on each used terminal server.....	3
Installation of the publisher service.....	3
Installation of the client software.....	3
Publish applications.....	4
Add the available servers.....	4
Add users and groups.....	5
Add published applications.....	6
Test your configuration.....	7
Work on the client.....	8

Installation

To use the RDP App Publisher you need at least one Terminal Server (Microsoft Windows Server 2008 or higher with Remote Desktop Services installed, Thinstuff XP/VS Server or any other Microsoft Windows based Terminal Server solution that supports the RDP protocol with Remote Applications) and a machine that can be used as publisher.

The publisher can be installed on (one of) the Terminal Servers, but this is not advised.

All used Terminal Servers and the publisher must be part of the same domain.

Configuration of the Terminal Servers

The used Terminal servers must run the Remote Registry Service. This service is used to get the needed information from this server for the publisher service.

Enable the Remote Registry Service on each used terminal server

1. Open the services on the Terminal Server (services.msc)
2. Find the service "Remote Registry"

Name	Description	Status	Startup Type	Log On As
 Remote Registry	Enables rem...		Manual	Local Service

3. Double click on the name
4. Set the Startup Type to Automatic and start the service

Installation of the publisher service

The .Net Framework 4.5 must be installed on the Publisher server - If it is not installed, you can install this using the Windows Updates.

Next install IIS on the publisher server (add the IIS role with the Server manager)

Then install "RDP PublishedApp Server.exe"

The publisher service is installed as website with the name AppPublisher and is bound to an application pool named AppPublisher (this application pool runs under the domain administrator account you provided). The website is configured to run in SSL mode only on port 2451.

Installation of the client software

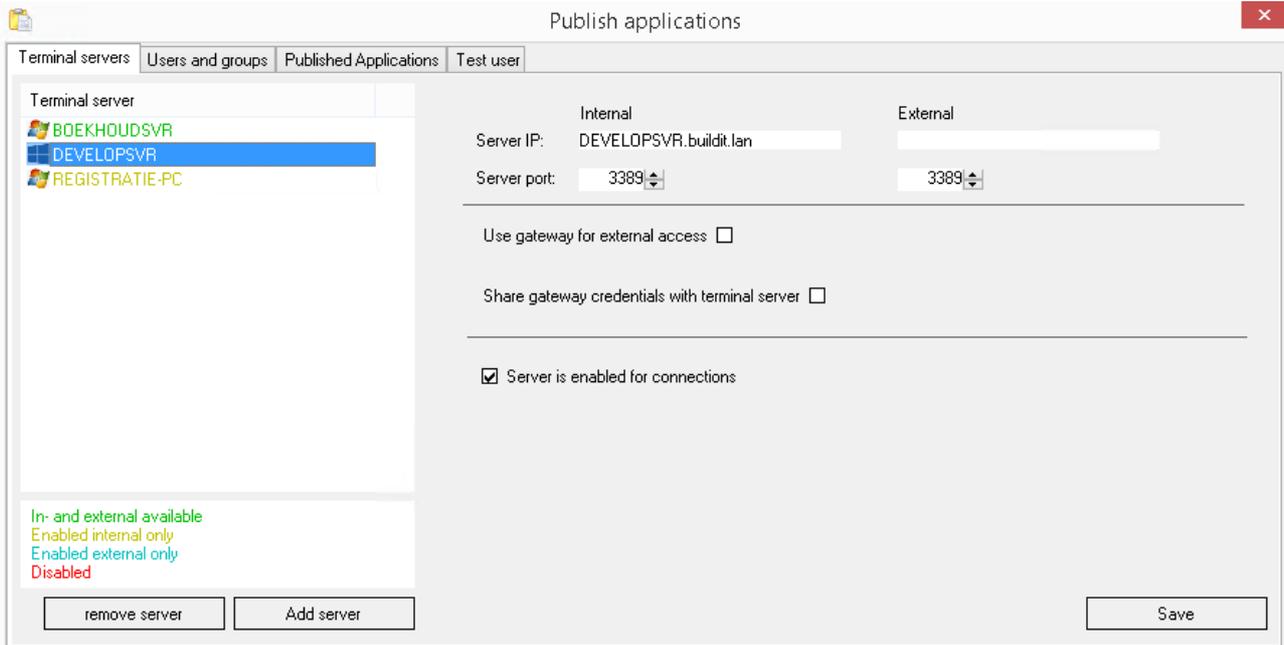
The .Net Framework 4.5 must be installed on the client computers - If it is not installed, you can install this using the Windows Updates.

Then install "RDP PublishedApp Client.exe"

Publish applications

Add the available servers

On the "Terminal Servers" tab you can add and configure your Terminal Servers.



Press "Add server" to add a server.

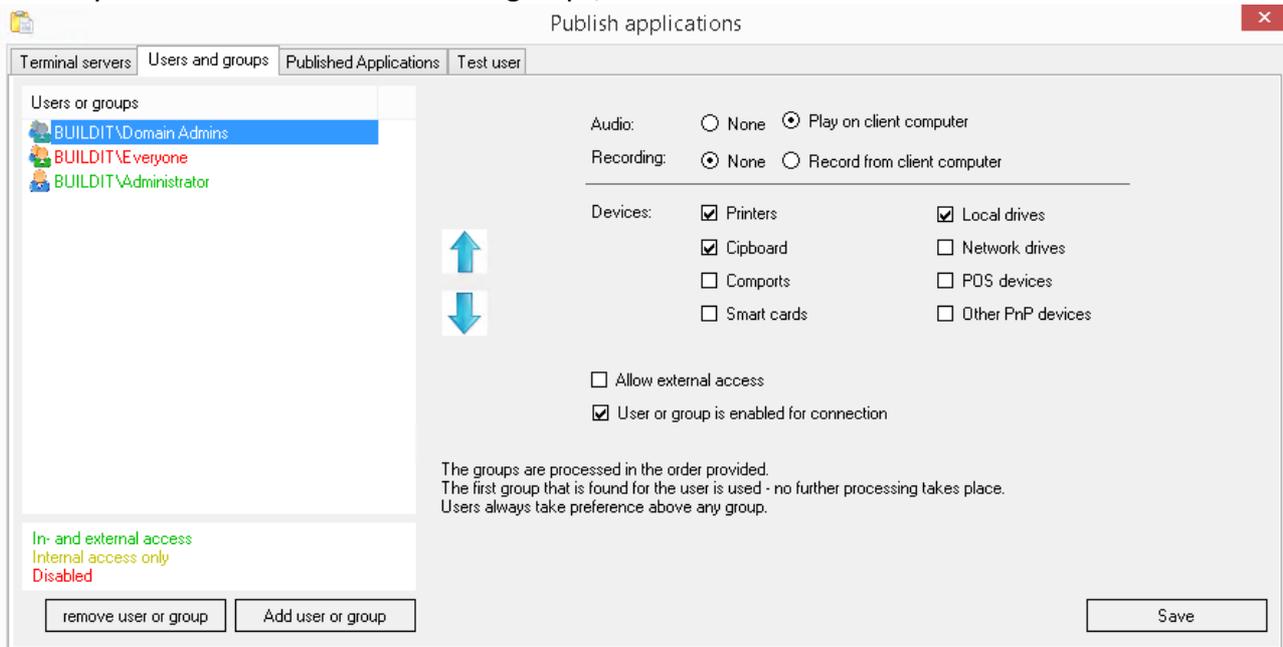
The internal IP is automatically filled with the FQDN of the server.

If you want to make the server available from the internet you have to add the IP or DNS name (and port) at "External", and if you use a gateway server, check the "Use gateway" check box and provide the details for the gateway.

A server can be made unavailable (by example because of maintenance) by clearing the check box "Server is enabled for connections". Existing connection will be preserved, but no new connections will be made to this server when this check box is cleared.

Add users and groups

Security is based on domain users and groups, as are the available client devices.

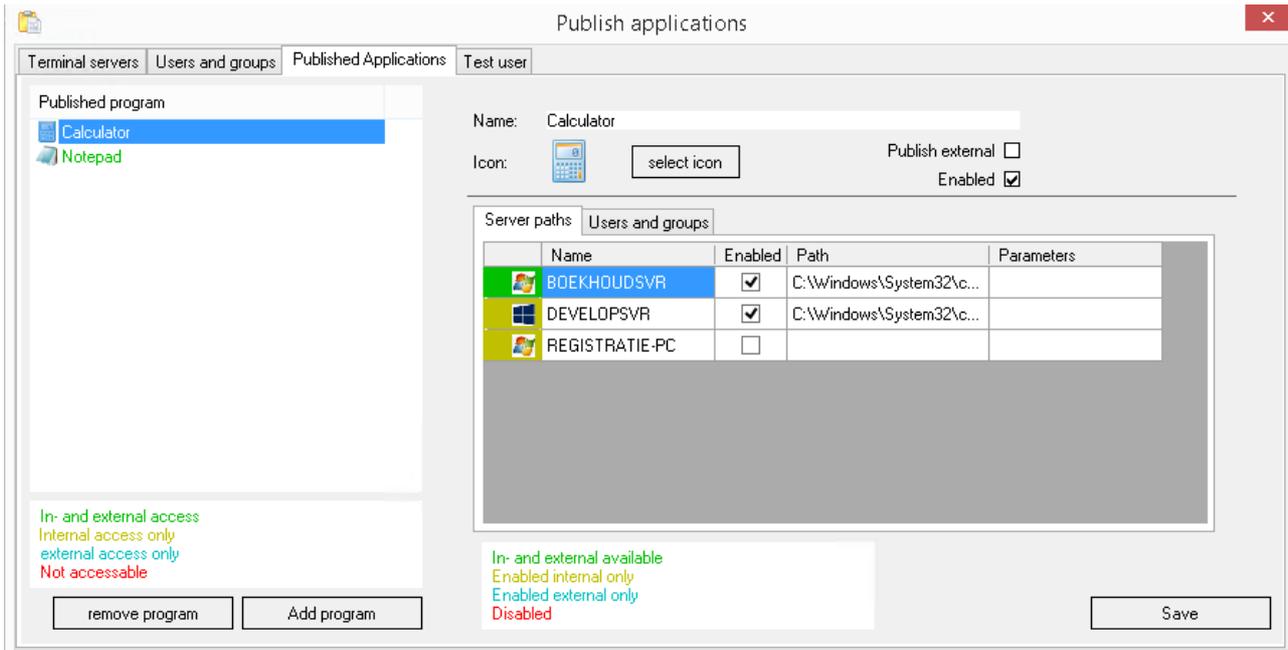


Press "Add user or group" to add a user or a group.

If a user is defined, he will always get the settings that are provided on the specific user - never on a group. If a user is not defined, the groups will be processed from top to bottom - the first group that applies to the user will be used to grant the rights.

Add published applications

You can publish the applications on the "Published Applications" tab.

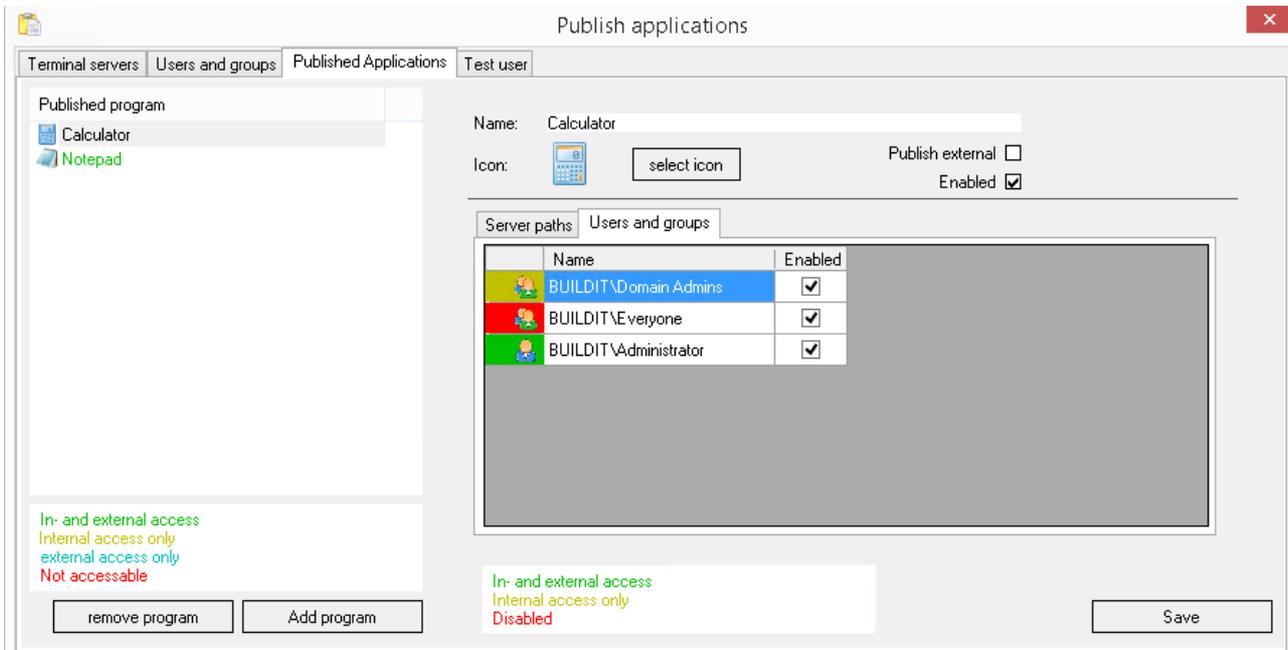


Press "Add program" to add a published application.

Give the application a name in the Name field and add the path per server for the application in the Server path grid. The icon is automatically extracted from the selected file if no icon head been selected previously.

To browse the path to the application you can press F4 when the server grid has the focus. Press F3 to automatically fill and enable all servers that have the application in the same path.

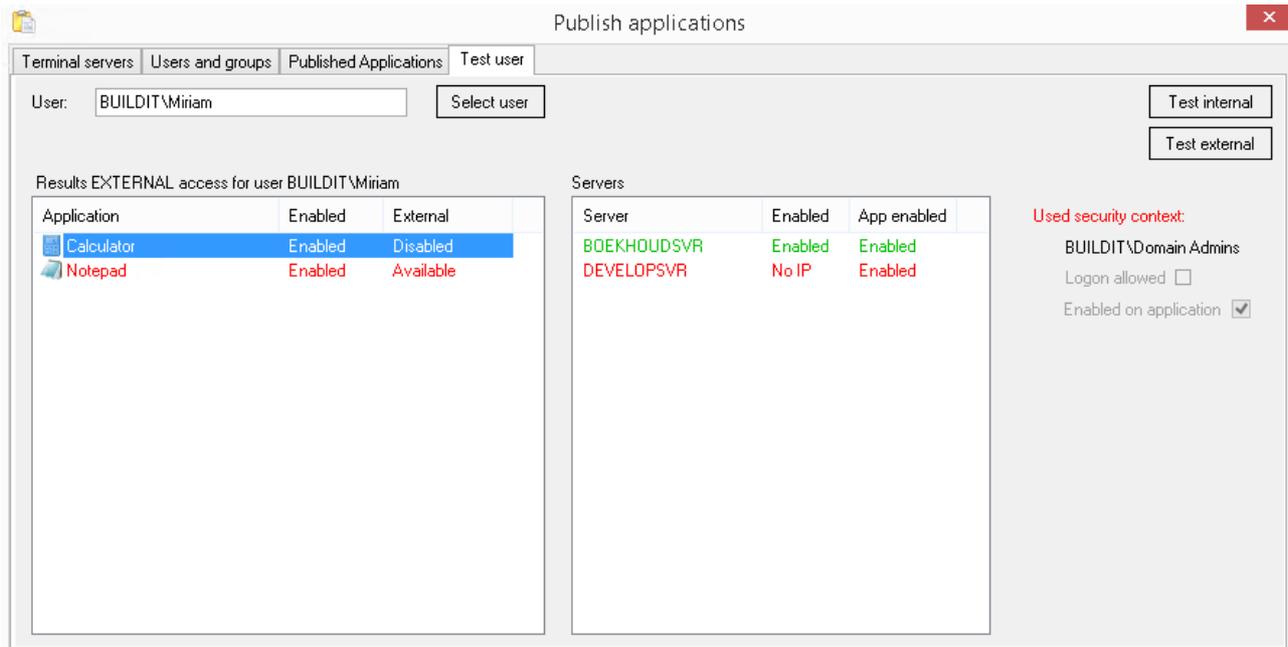
After you configured the servers, you can configure the user rights on the "Users and groups" tab.



Here you check then Enabled field for each user or group that will have access to this application.

Test your configuration

You can test the configuration on the "Test user" tab.



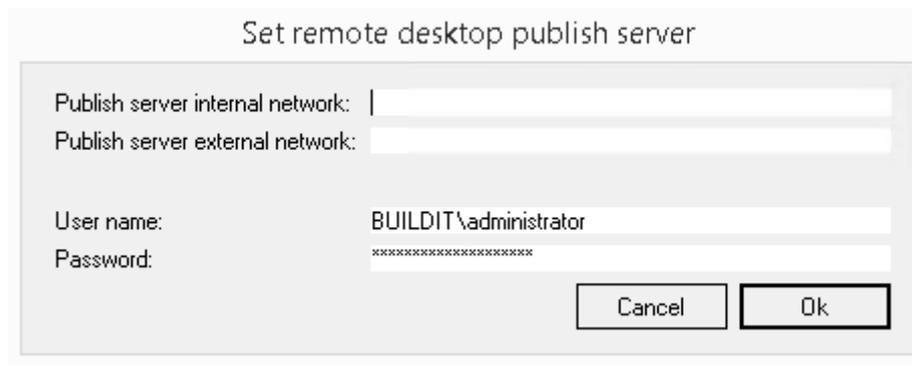
To test, select a domain user and press "Test internal" or "Test external" to see the result for internal or external access.

In the above example, the user Miriam has no external access to any application.

The calculator application is not activated for external access, the Notepad application is and has a server that serves this application externally, but the user Miriam is using the security context Domain Admins, which as no external logon access in the configuration.

Work on the client

When the client starts the first time, the configuration is displayed:



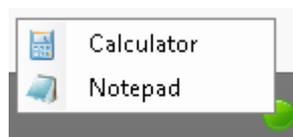
Fill in the DNS name of the publisher including the port number for the internal and or external publisher server (example: publisher.yourdomain.lan:2451), the domain username to connect with and the password for this user. Press Ok to save the information.

The password is stored in an encrypted form and the connection to the publisher is made over an SSL encrypted connection.

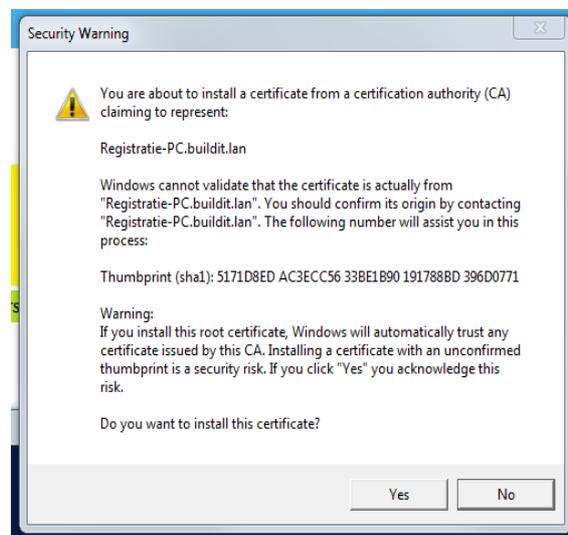
In the notification area at the left bottom of your screen, the client icon is displayed; a red circle is displayed when there is no connection to the publisher server, an orange circle is displayed when the client is initializing and a green circle is displayed when the connection to the publisher is available.

Double click on the notification icon to get the configuration window.

Right click on the icon in the notification area to get the publish applications menu:



Click on an item to start the remote application. All connections to the remote applications are encrypted with use of an X509 certificate. Because of this, you get the following message the first time you connect to a server (or when a server certificate has been replaced):



Press Yes to save the server certificate in the Root store - this is needed to use the server with saved credentials and logon security on the highest level (Kerberos or X509 SSL authentication). If you press No, the application won't start.