

UAG – Provide remote desktop access without Remote Desktop Gateway

As you may already know, Windows Server 2008 is providing new remote desktop functionality, called Remote Access Gateway, which allow RDP access to internal network without VPN.

However, this doesn't provide detailed security management, especially if you publish RPD gateway through ISA or TMG.

To simplify this, you should publish Remote Desktop Access through UAG. With UAG, you don't need RDP gateway and have deeper security management, such as block access if computer doesn't meet security requirements.

To do this, open the UAG console and go to your HTTPS trunk and add new application.

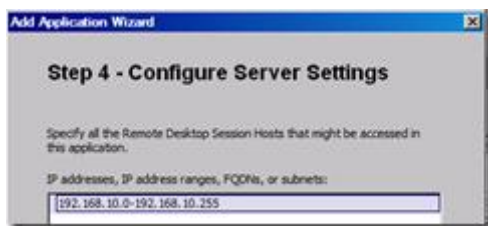
Then choose **Remote Desktop (User defined)**, available at **Terminal Services** section.



Name the application (for example, Remote Desktop) and define the security policy to allow the use and the connection.

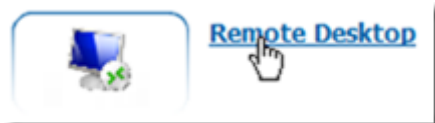


Then define the IP address range allowed for remote access; you define specific IP addresses or a large range of IP; to allow access to all of your LAN, just enter the first IP address and the last one separate with - (for example, 192.168.10.0-192.168.10.255).



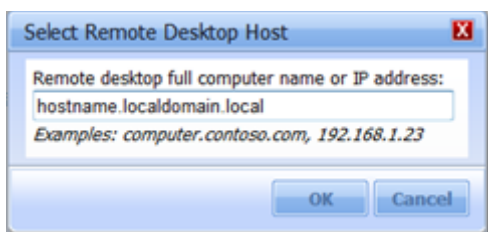
To finalize, define the display settings and if you provide a link on the UAG portal.

Et voilà, you provide Remote Desktop Access to your users.

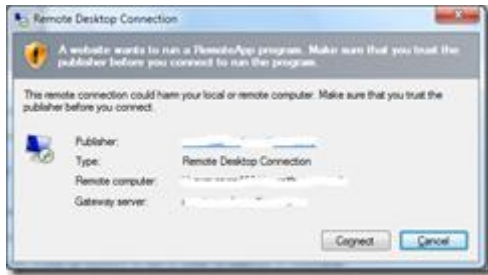


The only thing, is that your users must connect to the portal before accessing your LAN through RDP.

When the choose to connect using RPD, a pop up appears to ask to enter IP address or hostname.



A security window may also appear before connecting to ask users to confirm they trust the publisher.



NOTE: the Gateway Server URL must be the same than the UAG portal URL.