

PROXY Pro Deployment Tool Quick Start Guide: Deploying the Host

The PROXY Pro Deployment Tool is used to generate a transform file (.MST) that will contain and apply a custom string of Host Settings at installation time, such as a license key, permission to connect and any other settings. We encourage using the tool to create the transform file, although we understand you may elect to use your preferred software distribution approach for pushing out the Host software (SCCM, msixexec, group policy or similar). Two additional resources related to this would be our [Deployment Tool Guide](#), or follow along with our [Proxy Deployment Tool Walk Through Video](#) on YouTube.

The first half of this guide covers the process of using the Deployment Tool to create an install package for the Host and deploy it. In the second half, we'll provide recommendations on which Host settings are the most important ones you'll want to set, and we'll bring to light a few optional settings that may be useful too.

Step 1: Importing the Installation Files

After installing the PROXY Pro Deployment Tool, the first step is to load the installer Host-x64.msi (64-bit) into the tool, then we'll create a settings template, and last we'll go through the process of deploying the Host to a machine with your settings.

Right-click **Installation Files**, click **New** and browse to Host-x64.msi – click Open.

Step 2: Creating a Host Settings Template

Within this step, you'll be able to define each of the Host settings, such as the license key, the naming convention, tray icon behavior and any other applicable settings. If you're not entirely sure which settings are appropriate, please refer to the second half of this document, as we'll make some recommendations on which settings are typically the most useful and interesting.

- 1) Expand **Product Configurations**, right-click **Host**, click **New**
- 2) Give the settings template a name, such as HostSettings
- 3) The right pane now lists each available Host Setting – here are a few suggestions.
 - a. Double-click **Licenses** and paste your Host license into the field
 - b. Double-click **Beep on Connect** to turn the connection beep off (default is On)
 - c. Double-click **Show icon while idle** to hide the Host tray icon when there is no connection in progress
 - d. Double-click **Station Name** and use %USERNAME% on %NAME% (Hosts will appear as jsmith on PCNAME)
 - e. For RAS customers, double-click **Gateways**, input the server address (i.e. proxy.yourwebsite.com), with the port and protocol. WSS and 443 should be used externally and TCP and 2303 should be used internally.
 - f. Refer to the second half of this document for information on other common settings to be aware of

Step 3: Creating a Transform File from your Template

When you have finished entering the settings into the template, we'll create a transform file from that template.

Beneath Product Configurations, you'll see Host and under that, you'll see your template. Right-click your settings template -> New -> Transform File, giving the file a name like Host64.mst and now you'll have a transform file that will apply the settings to the Host during install time.

All done. You have successfully created a transform file that will allow your Hosts to be configured with your settings upon installation. The next page covers how to use the Deployment Tool to push the Host out to machines on your network. We'll also have information on the MSIEXEC approach as well.

Step 4: Deploying the PROXY Pro Host

Before we can deploy the Host, first expand (or right-click to refresh) Active Directory Domains, located at the bottom of the tool's left pane. If multiple domains are present, right-click the desired domain, click Refresh. The tool will present the OU structure exactly as its defined within Active Directory. Check the last page for help with any errors.

- 1) To install the Host on a single computer:
 - a. Find a Host, right-click, choose Install Software
 - b. Use the Installation File drop-down to select Host-x64.msi if not already selected
 - c. Use the Transform File Name drop-down to select Host64.mst, your transform file, if not already selected
 - d. Select restart option and hit OK to begin the push
- 2) To install the Host to multiple computers:
 - a. Highlight an OU container in the left pane; the right pane populates with the contents
 - b. Hit Control + A to select all computers in the selected OU
 - c. Follow steps (a) through (d) above

Deployment Tips & Suggestions

If you have OU's containing both 32-and 64-bit machines but cannot tell the difference at a glance, that's OK. You can safely select all computers within the OU, attempt to install the 32-bit Host.msi along with its transform file and the installation should succeed on all 32-bit machines but fail harmlessly on 64-bit machines. Give the container a second pass, this time selecting the 64-bit Host-x64.msi to be pushed, along with the corresponding transform file, and each of the 64-bit machines will receive the Host installation.

If you would like to know which machines are of which architecture, note that when you have selected a group of machines, the first right-click option on the context menu is **Refresh Details**. The Deployment Tool will make contact with each machine and display its OS, OS architecture, whether or not a Host is presently installed and if the machine is reachable for deployment. This could yield helpful information prior to a deployment.

Deployment via MSIEXEC (SCCM, Group Policy)

The PROXY Pro Host can be installed via msiexec command silently without an InstallShield interface with your desired transform file. Please reference the below baseline command:

```
msiexec /qn /I Host-x64.msi TRANSFORMS="Host64.mst"
```

Using the Deployment Tool's "Updating Host Settings" Capability

The Deployment Tool has an "Update Host Settings" mechanism that can be used to apply a Settings Template out to one or more Hosts within the network. The purpose of this capability is to roll out one or more changes to the existing Host configuration settings, such as changing the Gateway address that the Hosts are configured to report to. Before pushing out a Settings Template, first be sure to have one created – covered in step 2.

- 1) Find the machine or group of machines, right-click, click **Update Host Settings**
- 2) Select the desired template from the **Configuration Name** drop-down
- 3) Click **OK** to apply the Settings Template out to the selected Hosts

Congratulations! The Proxy Deployment Tool has successfully updated the Host settings. It's possible that some attempts may fail - review the next page for help with understanding and resolving common errors.

Understanding and Troubleshooting Common Deployment Errors

The Deployment Tool is dependent on a few underlying Windows technologies and concepts in order to make software deployment possible. There are a few common errors you may encounter and here's how to handle them.

1) RPC Server Unavailable - Error 0x800706ba

- a. The Deployment Tool is unable to communicate with the target machine on TCP port 135. Try again after running the following two commands in an administrative command prompt:

```
netsh advfirewall firewall set rule group="Windows Management Instrumentation (wmi)" new enable=yes
```

```
netsh advfirewall firewall set rule group="Windows Remote Management" new enable=yes
```

2) Fatal error during installation attempt – Error 0x80070035

- a. Try deploying the opposite architecture Host. If the 64-bit Host (Host-x64.msi) is attempted on a 32-bit system (or vice versa) this error could occur.
- b. If the error text is "Network path not found", ensure File and Print Sharing is enabled on the target machine. The Deployment Tool requires that this be enabled on machines.

3) Access Denied – Error 0x80070005

- a. This is the generic error code that Microsoft Windows provides for "permission denied". Try authenticating to the target machine with another set of credentials. The target machine will allow authentication if the account used is a member of its local administrators group.

4) Failed to contact target machine - Error 0xc004c001

- a. The target machine cannot currently be reached. Verify that it's powered on and that it has a network connection.

5) Error Applying Transforms - Error 0x80070643

- a. Please ensure you're using the correct transform file. For example, attempting to push the 32-bit Host.msi with a transform file generated from the Host-x64.msi will result in this error.
- b. Consider re-generating your transform file. Right-click your settings template, pick either Host.msi or Host-x64.msi from the drop-down and label the resulting file appropriately, including a "32" or "64" within the file name to eliminate confusion.
- c. Double-check the license key from within the Settings Template to ensure it goes with the version Host you are pushing out. For example, if the first four keys are 4331, it's for a v10 Host. If 4230, it's for a v9 Host. If it's 4130, it's for v8.10. Ensure the version Host you're pushing corresponds to the license key being used.

6) Failed to Update Host Settings - Error 0xc004c018

- a. The target Host is currently configured to disallow this connection. The setting to disable would be the checkbox on the Proxy Host Control Panel's "Gateways" tab for "Host administration and remote management".

PROXY Pro Host Settings Pre-Deployment Checklist

The PROXY Pro Host is the remote desktop client that gets installed on each computer to be remotely accessed. The Host client can be configured with a wide range of settings combinations to suit a company's needs, use cases and requirements. The purpose of this document is to highlight each major area of the settings to be considered prior to a roll out. Additional assistance from Proxy Networks Support is available to help achieve your ideal configuration.

1. Permission to Connect options

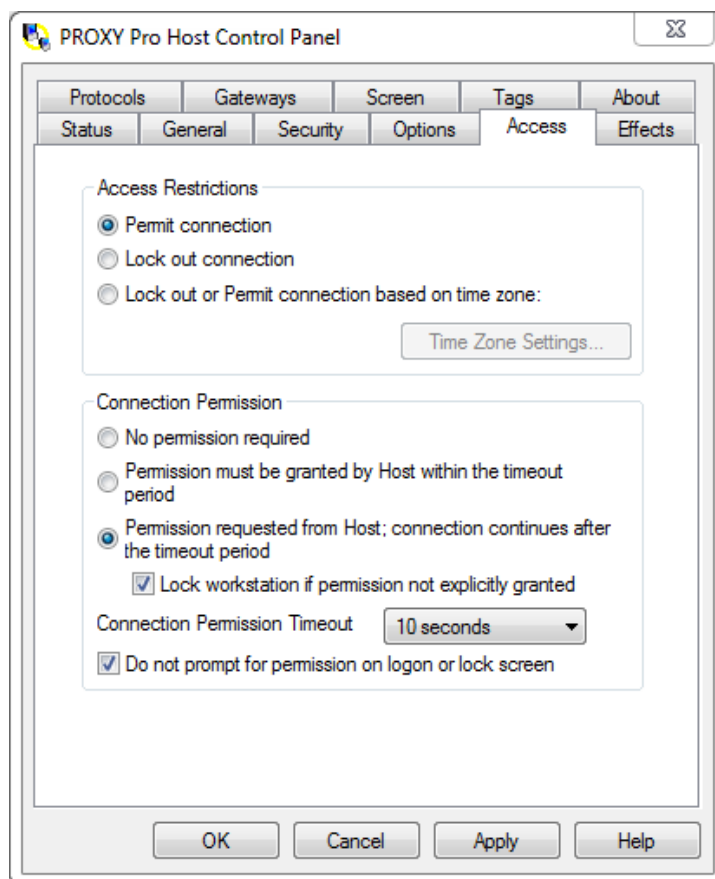
The Proxy Host Control Panel's **Access** tab includes three distinct **Connection Permission** options.

No permission required is the default, meaning that a technician using the PROXY Pro Master or the Proxy Web Console can connect to the Host for remote control without user permission.

Permission must be granted by Host user within the timeout period only allows the connection to succeed if the Host user accepts the connection within the timeout timeframe.

Permission requested from Host; connection continues after the timeout period allows the connection to occur if the Host is unattended and the timeout expires, after having given the user the opportunity to accept or reject the connection. Think of it like knocking before entering.

With both, the Host can additionally lock the workstation if no response is given. The permission prompt can also be ignored if the Host machine is presently at the Windows logon or locked screen.



Connection Permission Setting	Behavior	Preference
No Permission Required	Click & Connect	
Grant	Connect only with end-user approval	
Request	Connect with end-user approval then connect after "X" number of seconds if no response	

Notes

2. Naming Convention, Tray Icon appearance, Connection Beeps and more

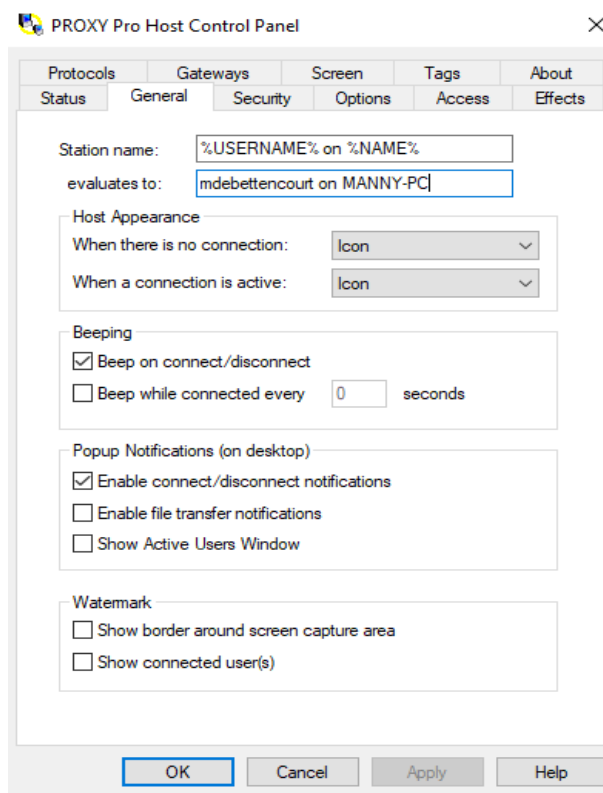
The Proxy Host Control Panel's **General** tab contains settings that primarily control how the Host behaves when connections are made and closed to it.

The **Station Name** field controls how the Host shows up in your console. The %USERNAME% on %NAME% string pulls the logged-in username along with the computer name and presents them in the fashion of "jsmith on PCNAME".

Host Appearance drop-downs control tray icon behavior. Set both values to **Icon** to keep it visible at all times, or only when connections are active. Set both values to **Hidden** to keep it invisible at all times. The tray icon color changes from yellow to green when a connection is in progress and can be a helpful cue to the end user that their machine is being remotely controlled.

Beep on Connect sends an audible chime to the Host computer when connections are opened or closed.

Popup Notifications when enabled will cause a message to appear in the bottom-right corner of the screen to indicate when users connect and disconnect from the machine.



Connection Behavior Setting	Available Values	Preference
Tray Icon (Idle)	Hidden or Visible	
Tray Icon (Active)	Hidden or Visible	
Connection Notifications	Enabled or Disabled	
Beeps on Connect/Disconnect	Enabled or Disabled	
Show active users list on connect	Enabled or Disabled	
Show watermark border upon connection	Enabled or Disabled	
Show watermark text box of active users on connect	Enabled or Disabled	
Connection Behavior Setting	How the Host is displayed	Preference
Show Proxy Hosts by PC name	DELL-XPS-123 (default)	
Show logged-in user and PC name	Jsmith is logged into DELL-XPS-123	
Show logged-in user with domain and PC name	DOMAIN/jsmith is logged into DELL-XPS-123	
Show first name followed by last name	John Smith	
Show first name followed by last name and the computer name	John Smith is logged into DELL-XPS-123	

3. Effects and Performance Optimization Options

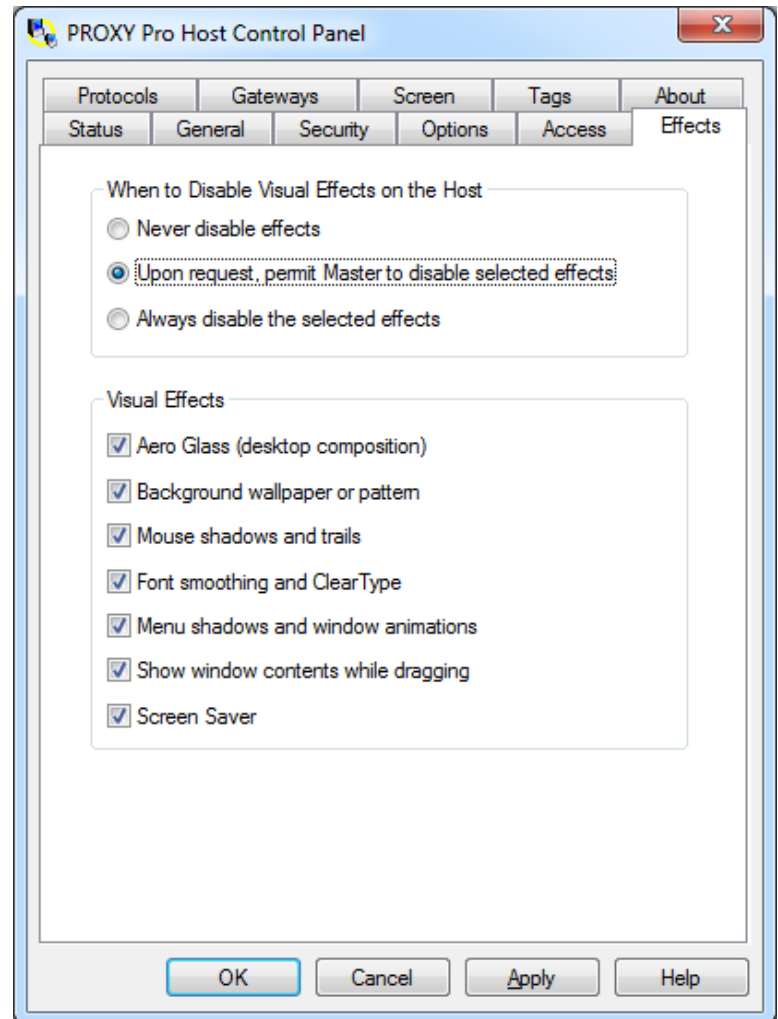
The **Effects** tab on the Proxy Host Control Panel is used primarily to disable extra unnecessary Windows “effects” that can improve the overall performance and responsiveness as a result during the remote control experience. Not all effects may be needed but by ignoring these, we’ll get the fastest possible responsiveness.

The **When to Disable Visual Effects on the Host** setting defaults to **Upon request, permit Master to disable selected effects**. This means the Master user can decide on a connection-by-connection basis if they want the effects enabled or disabled during the connection.

Using **Never Disable Effects** leaves all effects un-touched.

The **Always disable the selected effects** disables each selected effect for each connection made to that Host.

The individual **Visual Effects** list can be preconfigured to ignore some effects but not others. Use this checklist to determine which effects are to be disabled.



Effects and Connection Optimization	Description	Preference
Never disable effects	If enabled, no changes are made (Stealth mode)	
Upon request, Master user may choose effects	Master user can toggle effects on/off (default)	
Always disable selected effects	Selected items will always be ignored	

Notes

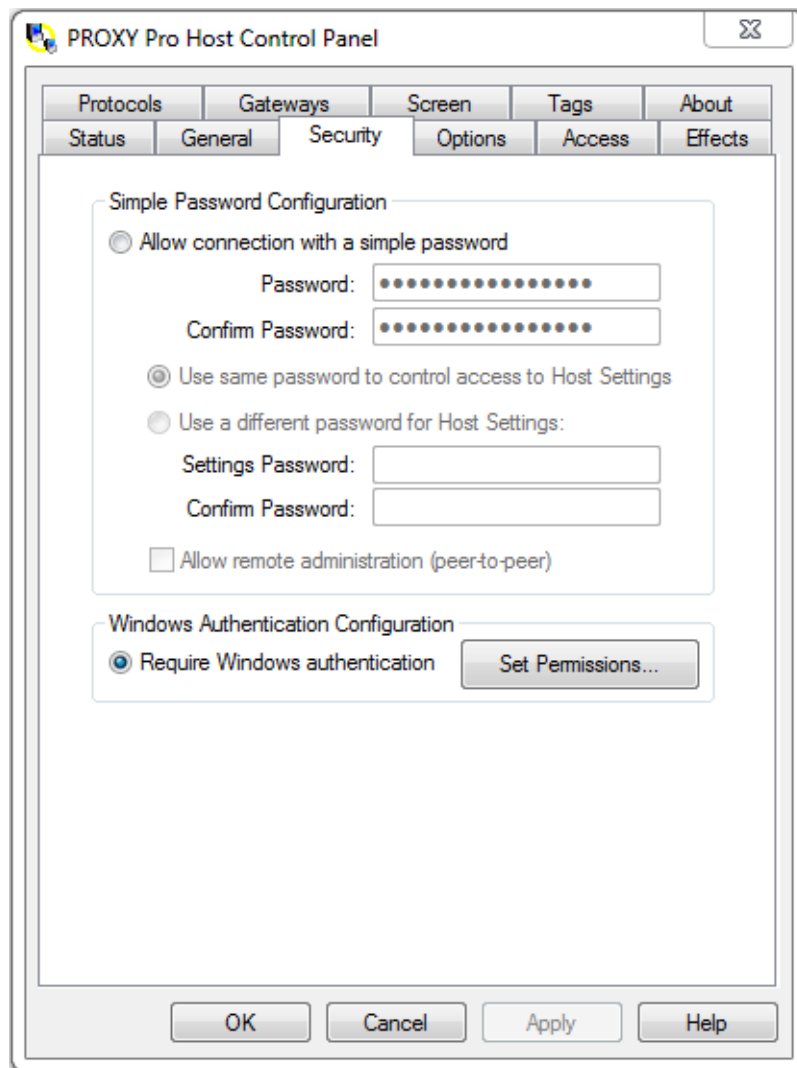
4. Locking down the PROXY Pro Host - Security Settings

The **Security** tab on the Proxy Host Control Panel is used for controlling access to the Host computer and Host Settings.

The **Simple Password Configuration** is for non-domain environments where you would otherwise be using the Windows Security Model. A simple password string can be set requiring PROXY Pro Master users to supply this password when accessing the Host from the P2P Hosts tab. This password does not apply for Gateway-based connections. Optionally a Settings Password can be used that would then need to be specified in order to open the Proxy Host Control Panel.

Additionally, allow or disallow the Host to be contacted by the Deployment Tool when using its “Update Host Settings” capability later.

Windows Authentication Configuration is recommended for domain environments. By default, members of the machine’s local administrators group will have Full Control/Administration over the Proxy Host Control Panel. If your end users are not local administrators, no special instructions here apply. If they are, you can supply an alternate group such as domain administrators.



The screenshot shows the PROXY Pro Host Control Panel window with the Security tab selected. The window has a title bar with the PROXY logo and a close button. Below the title bar is a tabbed interface with tabs for Protocols, Gateways, Screen, Tags, About, Status, General, Security (selected), Options, Access, and Effects. The Security tab contains two main sections: Simple Password Configuration and Windows Authentication Configuration. The Simple Password Configuration section has three radio buttons: 'Allow connection with a simple password' (selected), 'Use same password to control access to Host Settings', and 'Use a different password for Host Settings:'. Below the first radio button are two password fields labeled 'Password:' and 'Confirm Password:'. Below the second radio button are two password fields labeled 'Settings Password:' and 'Confirm Password:'. There is also a checkbox for 'Allow remote administration (peer-to-peer)'. The Windows Authentication Configuration section has a radio button for 'Require Windows authentication' (selected) and a 'Set Permissions...' button. At the bottom of the window are four buttons: OK, Cancel, Apply, and Help.

Locking down the Proxy Host	Recommendation	Preference
Windows Authentication	Recommended for domain environments	
Simple Password	Recommended for non-domain environments	

Notes

5. Configuring the Host to report to a PROXY Pro Gateway server

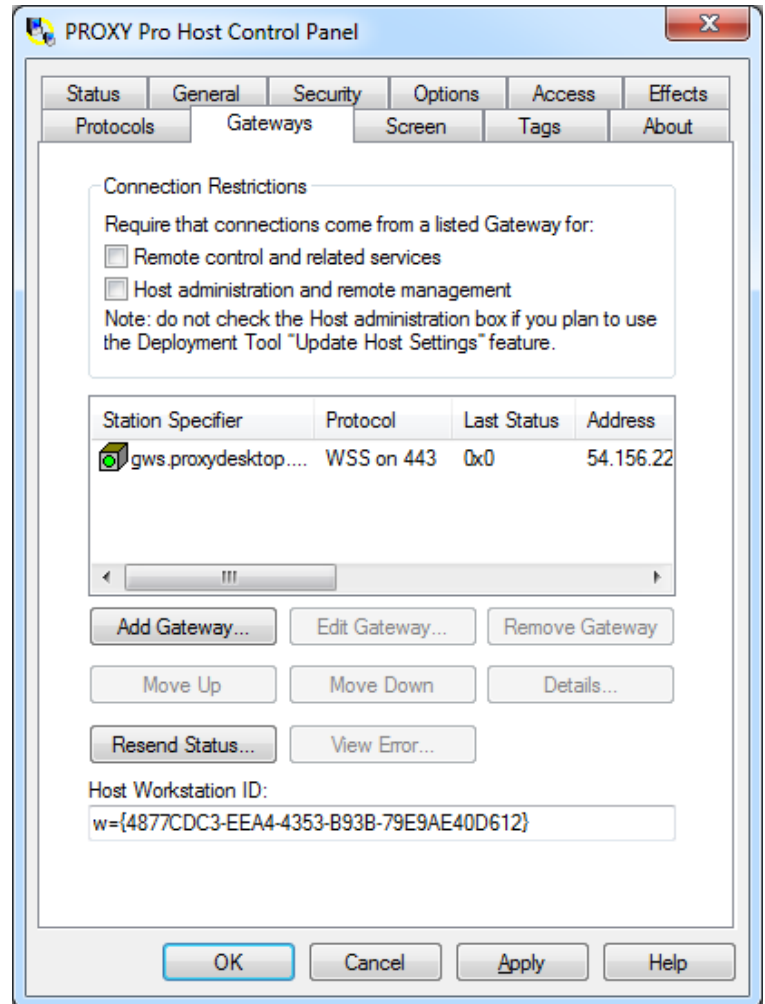
The **Gateway** tab on the Proxy Host Control Panel is used for defining which RAS server the Host will make itself accessible for connectivity through. Note that this applies only to RAS Edition customers.

You can fill in your server address after clicking the **Add Gateway** button. Expected values for the address would be:

- support.mywebsite.com (external address)
 - Protocol: WSS
 - Port: 443 (default for WSS)
- servername.mywebsite.com (internal address)
 - Protocol: UDP or TCP
 - Port: 2303 (default for both)

It's recommended to supply both the internal and the external address if the Hosts will be, for example, laptops that may come and go from your company network. If the Host will be installed onto desktop computers that would never leave the RAS server's network, only the internal address is needed.

Connection Restrictions can be set to require that any incoming connection attempts must be made through the Gateway(s) that the Host is configured to report to (the first checkbox). PROXY Pro Masters will not be able to establish connections from the P2P Hosts tab – only the Gateway Hosts tab or from the Proxy Web Console. The Host can also restrict incoming communication attempts from the PROXY Pro Deployment Tool (the second checkbox).



Notes

Need more help?

The Proxy Networks Support Team is available to ensure the settings you've chosen are right for you, and that your overall deployment of Proxy goes well. If you'd like us to look over your settings template prior to a rollout, we're glad to help out.