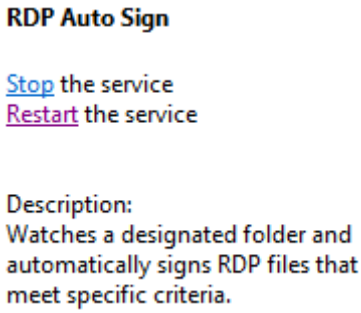
Configure Automatic RDP File Signing

RDPAutoSign is a service that must be installed on the IIS server hosting the RDP file generation webpage.



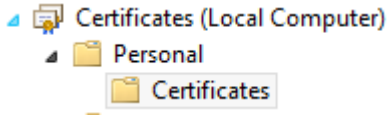
Configure Required Options

Open ‘mmc’ from the run box and choose File -> Add/Remove Snapin

Add ‘certificates’ from the left hand box and select ‘Computer Account’ when prompted.

Click OK

Navigate to Certificates (Local Computer) -> Personal -> Certificates



Double click on the certificate you’d like to use for signing the RDP files.

You must have the private key for this certificate installed, and it must have a subject or subject alternate name of the RD host (or gateway) server you are generating.

Choose the details tab and scroll down to ‘Thumbprint’.

Copy the thumbprint into the clipboard.

Open ‘RDPAutoSign’ in the ‘RLE Stat Package’ folder and find the ‘rdpautosign.exe.config’ file.

Open this file in notepad.

Find the setting ‘signwithcert’ and paste the certificate thumbprint you copied between the <value> and </value> marks:

```
<setting name="signwithcert" serializeAs="String">
    <value>12 72 a2 a6 0d 46 c7 f3 14 aa 75 2f 1d 79 f1 30 f7 b2 64 e8</value>
</setting>
```

If you are using a non-english version of Windows, you may need to change the ‘confirmmessage’ setting. Otherwise, leave as-is.

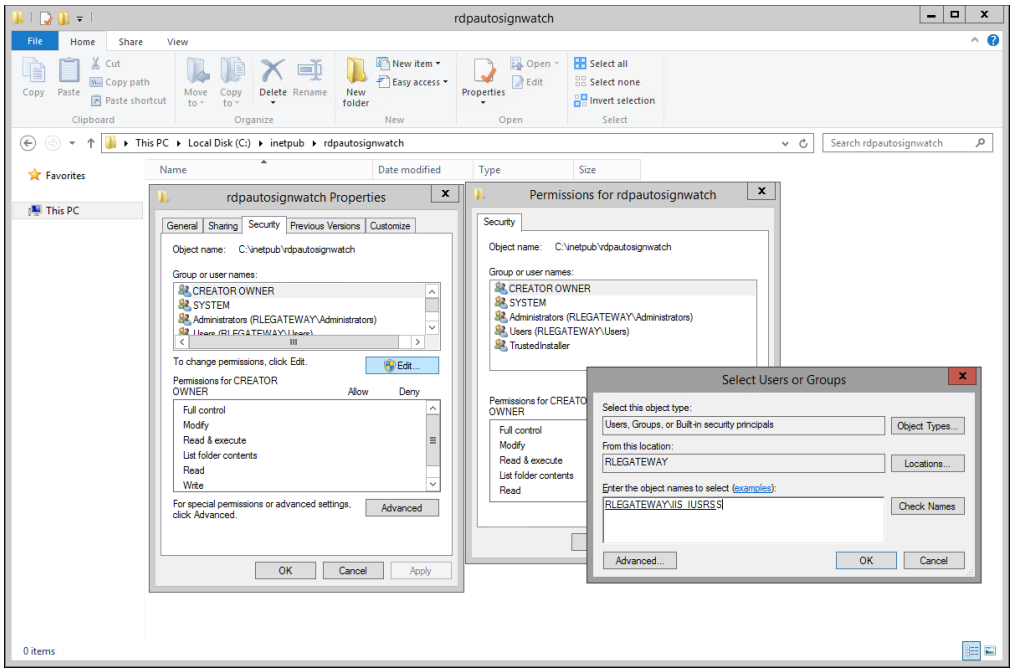
You now need to restrict the destinations that you want RDP Auto Sign to sign automatically. These are written in .net regular expression format. For example:

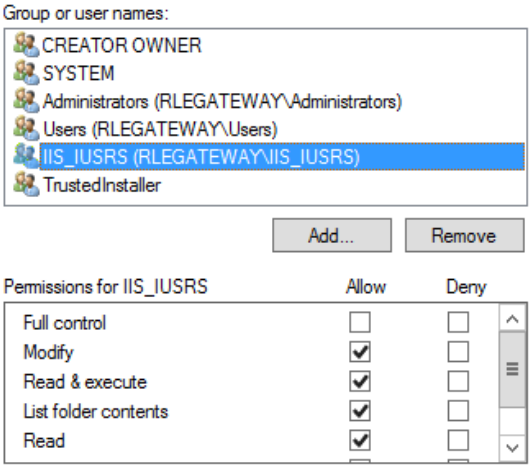
Intended Result	Regular Expression
Allow any destination (not recommended)	.*
Allow destinations ending '.yourdomain.local'	.yourdomain.local$
Allow destinations starting 'myserver'	^myserver

Enter these expressions as <string> </string> values in the 'alloweddestinations' setting:

```
<setting name="alloweddestinations" serializeAs="Xml">
    <value>
        <ArrayOfString xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xmlns:xsd="http://www.w3.org/2001/XMLSchema">
            <string>.mydomain.com$</string>
            <string>.internal.mydomain.com$</string>
        </ArrayOfString>
    </value>
```

Finally, modify the 'watchfolder' to a folder that the IIS server can write to. It is recommended that you create a new folder called 'rdpautosignwatch' in 'c:\inetpub\' and grant the IIS App Pool user 'modify' permissions: (this account is usually IIS_IUSRS)





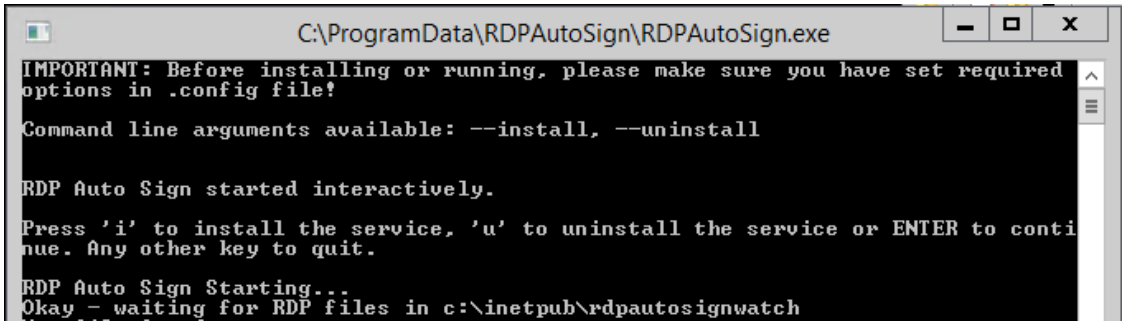

```
<setting name="watchfolder" serializeAs="String">
    <value>c:\inetpub\rdpautosignwatch</value>
</setting>
```

Install RDP Auto Sign on the IIS Server

Copy the RDPAutoSign folder to c:\programdata\

Run RDPAutoSign.exe as administrator and press ENTER

If all has been configured correctly, you should see the following:



Copy an unsigned RDP file to the watch folder to test the destination matching.

You should see something as follows:

If you receive errors about not finding the certificate, make sure that you have installed the certificate into the Computer -> Personal store, that it has the private key installed and the thumbprint is correct.

Close the window and re-run as administrator.

Press 'I' to install the service.

When installed, services.msc should show the following: