

NETOP™

RemoteControl

Secure Remote Management and Support

**Windows Azure Multi-Factor
Authentication**



Netop develops and sells software solutions that enable swift, secure and seamless transfer of video, screens, sounds and data between two or more computers over the Internet. For more information, see www.netop.com.

Contents

1 Introduction 2

2 Retrieve the Windows Azure information 3

3 Configure the Host machine 7

 3.1 Apply the Windows Azure information 7

 3.2 Configure the Host 12

4 Connect to the Host machine 15

5 Troubleshoot 17

 5.1 I do not receive any text message. 17

 5.2 Error connecting to Host. Error = 100 17

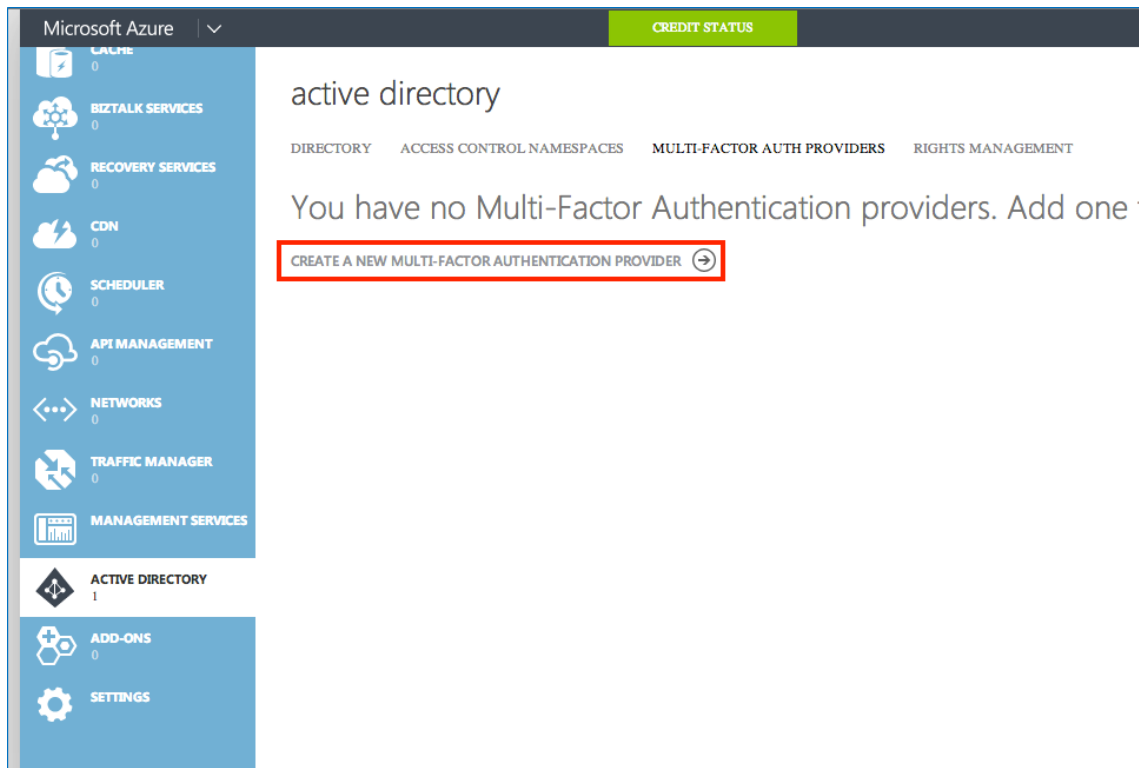
1 Introduction

Netop Remote Control version 11.6 introduces extended security with Windows Azure multi-factor authentication. The host is validated based on two factors: one authentication factor is the Host credentials (something the user knows), the second factor is a passcode received by phone (something the use has).

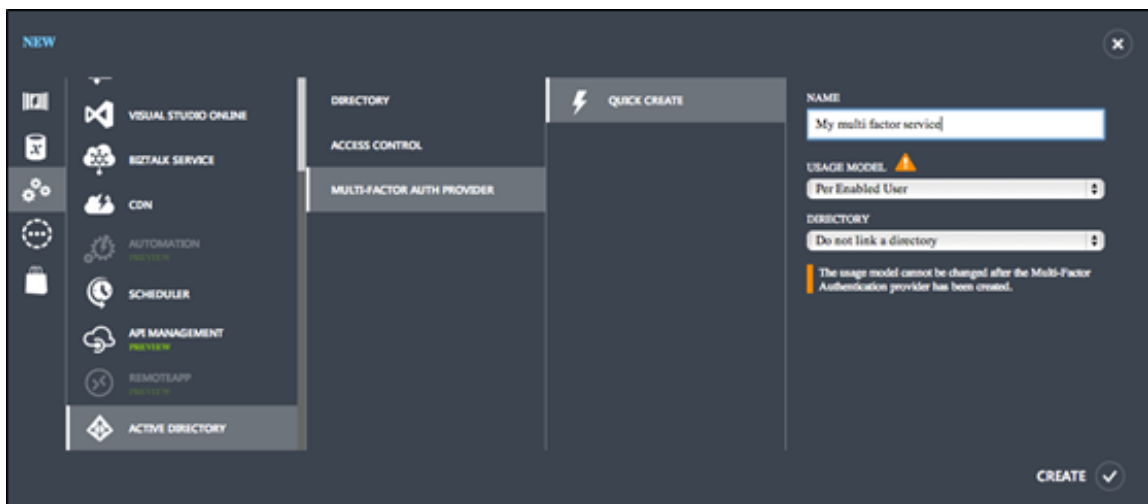
This document explains how to retrieve the Microsoft Azure information, how to configure and connect to the host.

2 Retrieve the Windows Azure information

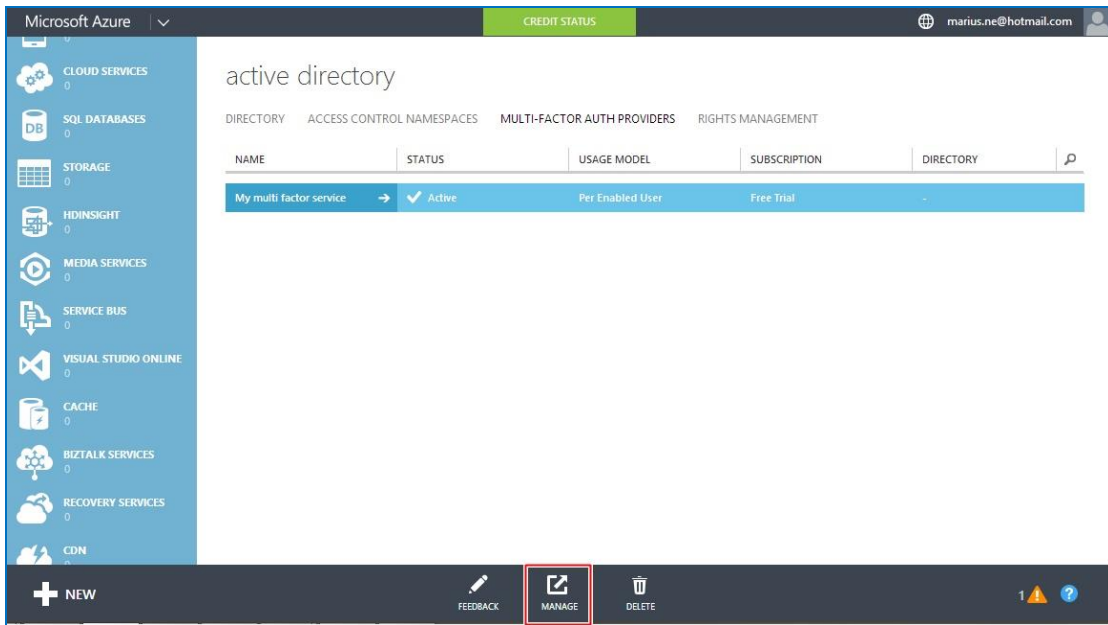
1. Sign up for a Windows Azure account ([link](#)) or use your existing Windows Azure account and login ([link](#)).
2. Go to Portal.
3. Go to **ACTIVE DIRECTORY > MULTI-FACTOR AUTH PROVIDERS** and click **CREATE A NEW MULTI-FACTOR AUTHENTICATION PROVIDER**.



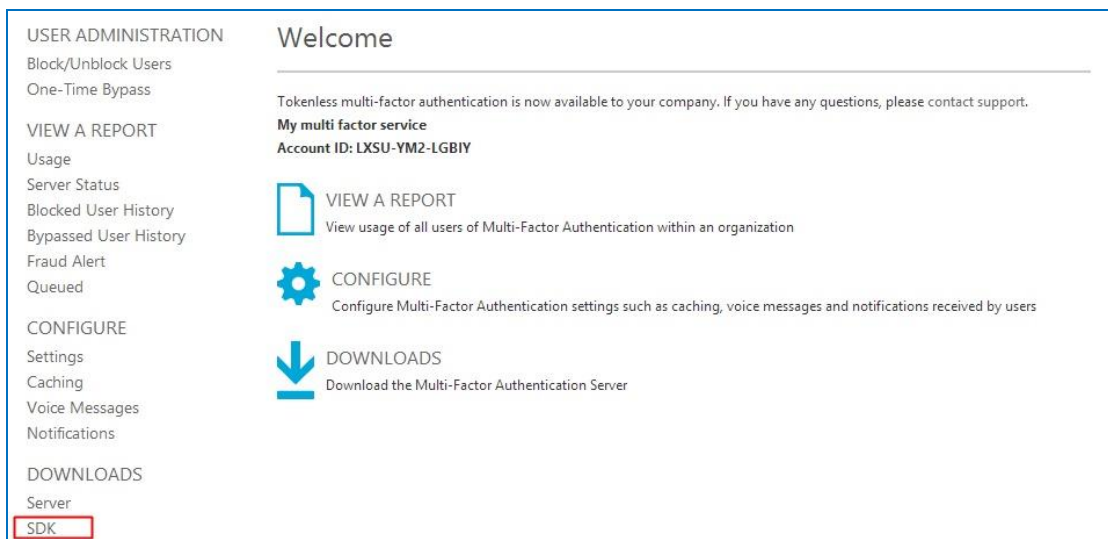
4. Configure a name and select the Usage model. You can also link to a directory (not mandatory). Click **CREATE**.

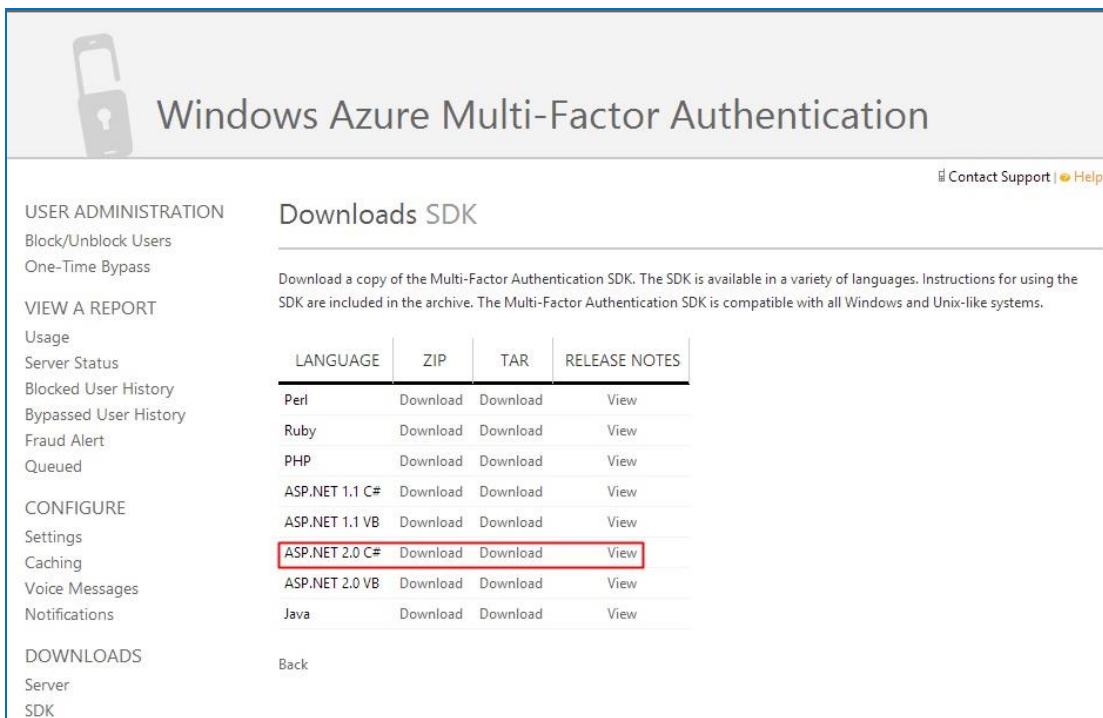


5. Click the **Manage** icon located at the bottom of the page.



6. Go to **Downloads > SDK**.



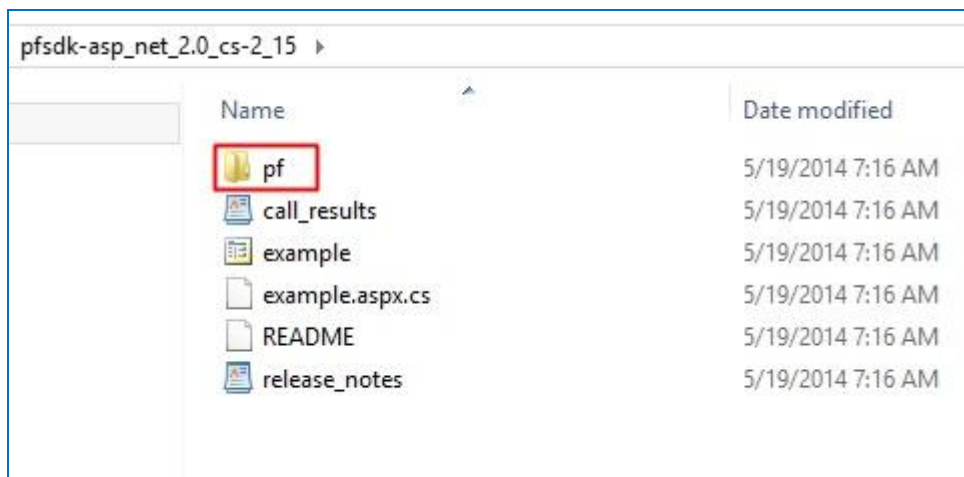


The screenshot shows the 'Downloads SDK' page for Windows Azure Multi-Factor Authentication. The page has a sidebar with navigation links: USER ADMINISTRATION (Block/Unblock Users, One-Time Bypass), VIEW A REPORT (Usage, Server Status, Blocked User History, Bypassed User History, Fraud Alert, Queued), CONFIGURE (Settings, Caching, Voice Messages, Notifications), and DOWNLOADS (Server, SDK). The main content area is titled 'Downloads SDK' and includes a description: 'Download a copy of the Multi-Factor Authentication SDK. The SDK is available in a variety of languages. Instructions for using the SDK are included in the archive. The Multi-Factor Authentication SDK is compatible with all Windows and Unix-like systems.' Below this is a table with columns: LANGUAGE, ZIP, TAR, and RELEASE NOTES. The table lists various languages and their corresponding download links. The row for 'ASP.NET 2.0 C#' is highlighted with a red box.

LANGUAGE	ZIP	TAR	RELEASE NOTES
Perl	Download	Download	View
Ruby	Download	Download	View
PHP	Download	Download	View
ASP.NET 1.1 C#	Download	Download	View
ASP.NET 1.1 VB	Download	Download	View
ASP.NET 2.0 C#	Download	Download	View
ASP.NET 2.0 VB	Download	Download	View
Java	Download	Download	View

Back

7. Download the zip version of **ASP.NET 2.0 C#** and unarchive it. Open the **pf** folder from the archive.



Name	Date modified	Type	Size
certs	5/16/2014 1:04 PM	File folder	
pf_auth.cs	5/16/2014 4:00 AM	CS File	46 KB

8. Open the **pf_auth.cs** file in a text editor (preferably a more advanced text editor like Word Pad). Look for **CERT_PASSWORD**. This represents the password for the certificate that will be used on the Host device.

```
private const string LICENSE_KEY = " ";  
private const string GROUP_KEY = " ";  
private const string CERT_PASSWORD = " ";
```

In the **pf > certs** folder you can find the certificate.

The certificate and the password for the certificate represent the 2 items required from the Windows Azure account.

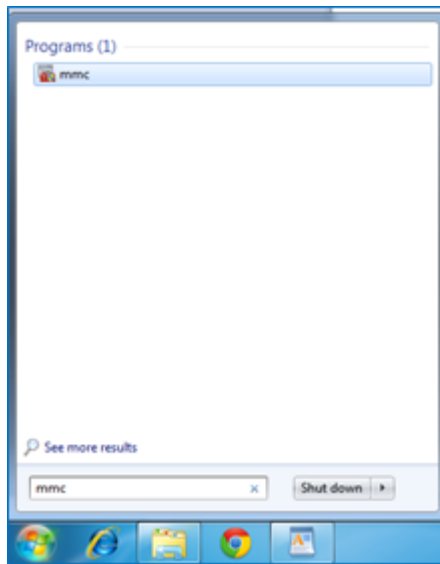
3 Configure the Host machine

3.1 Apply the Windows Azure information

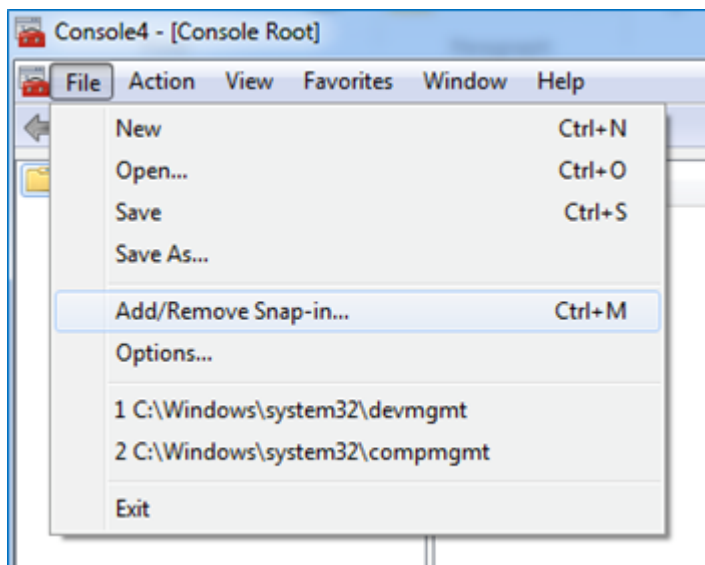
In order for the machine to use the Windows Azure multi factor authentication, it needs to be securely identified by Windows Azure. This is done by installing the Certificate obtained previously.

The steps below are for installing the Certificate on a Windows 7 machine. This can be done also using various mass deployment techniques (e.g.: Group Policy).

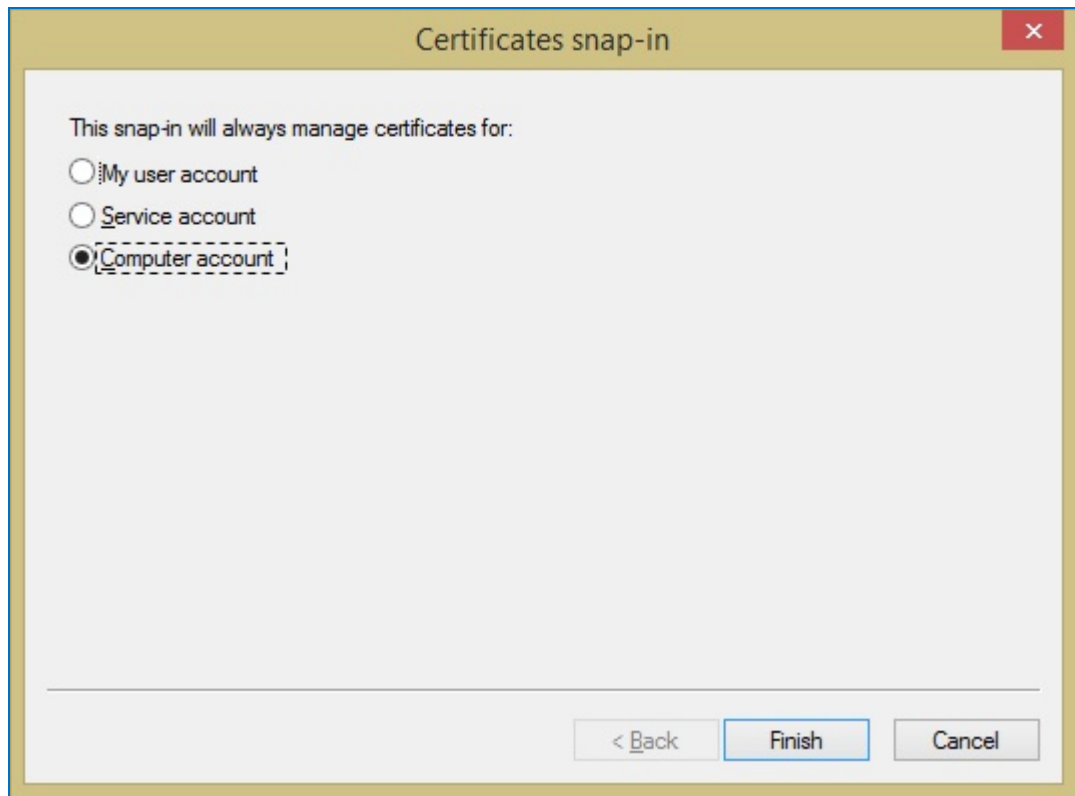
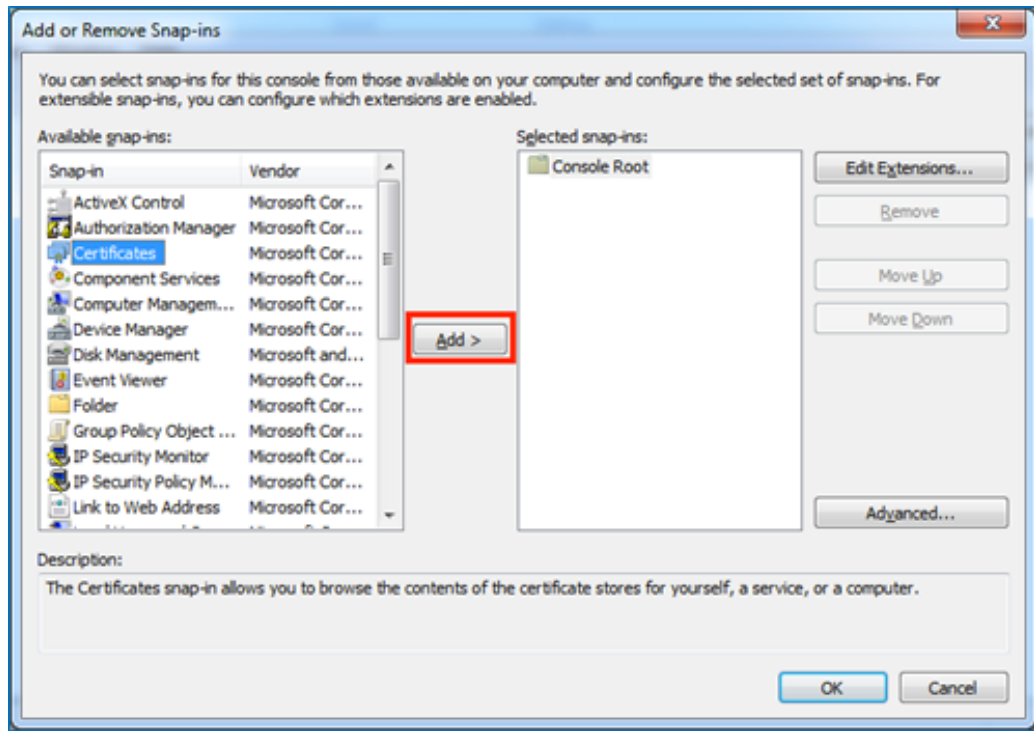
1. Run **mmc.exe** in order to install the certificate.



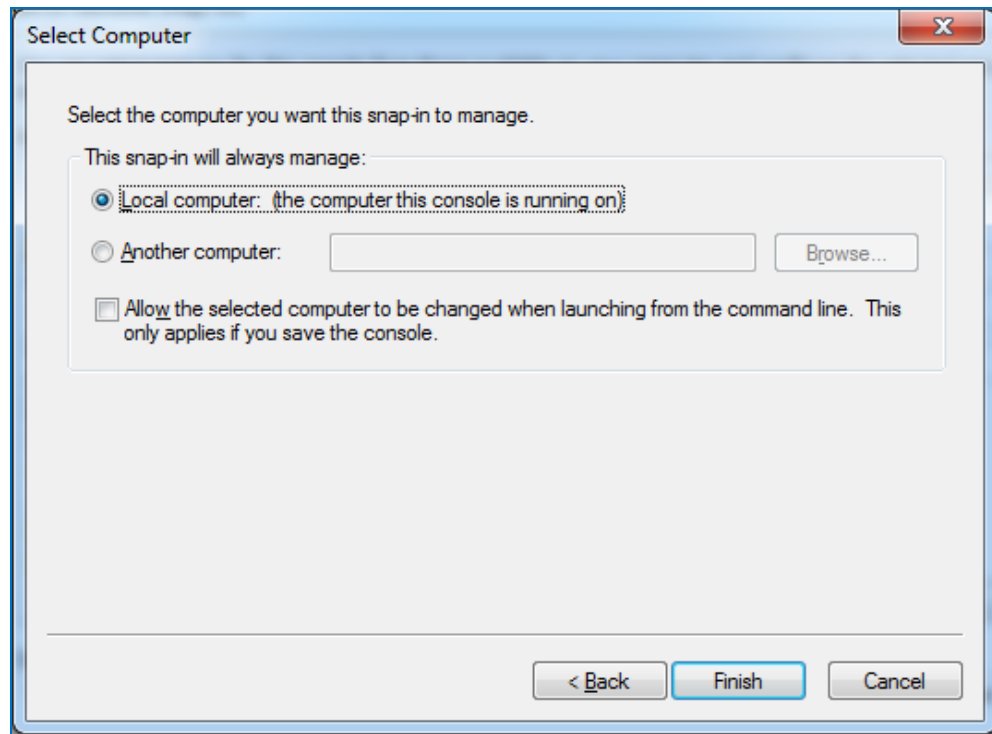
2. Click **File > New**. Then click **File> Add/Remove Snap-in...**



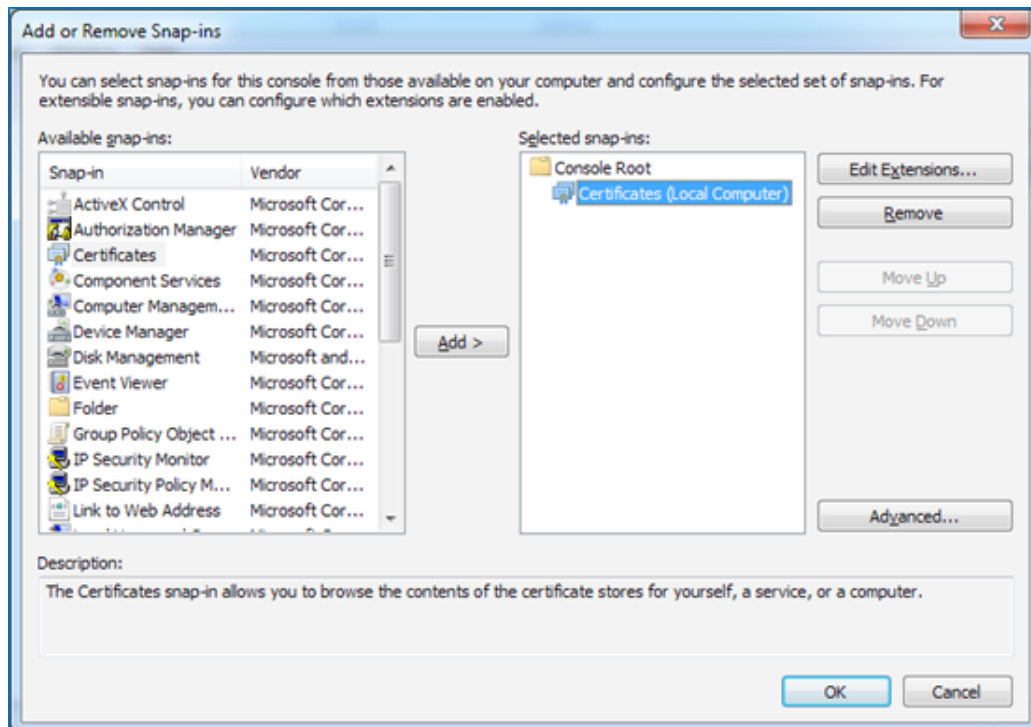
3. Choose **Certificates** and click **Add**



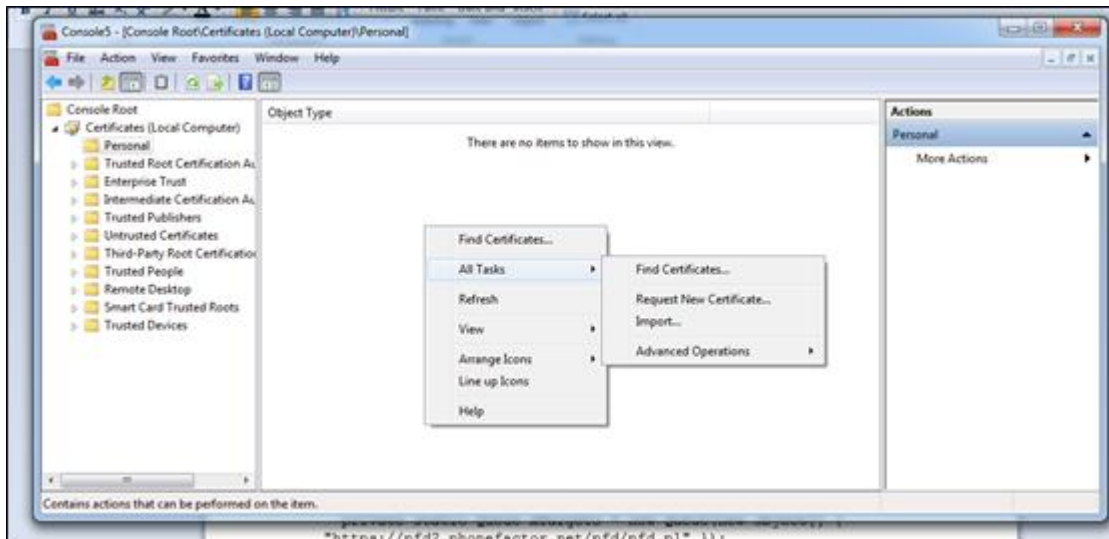
4. Choose **Computer account** and click **Next**.



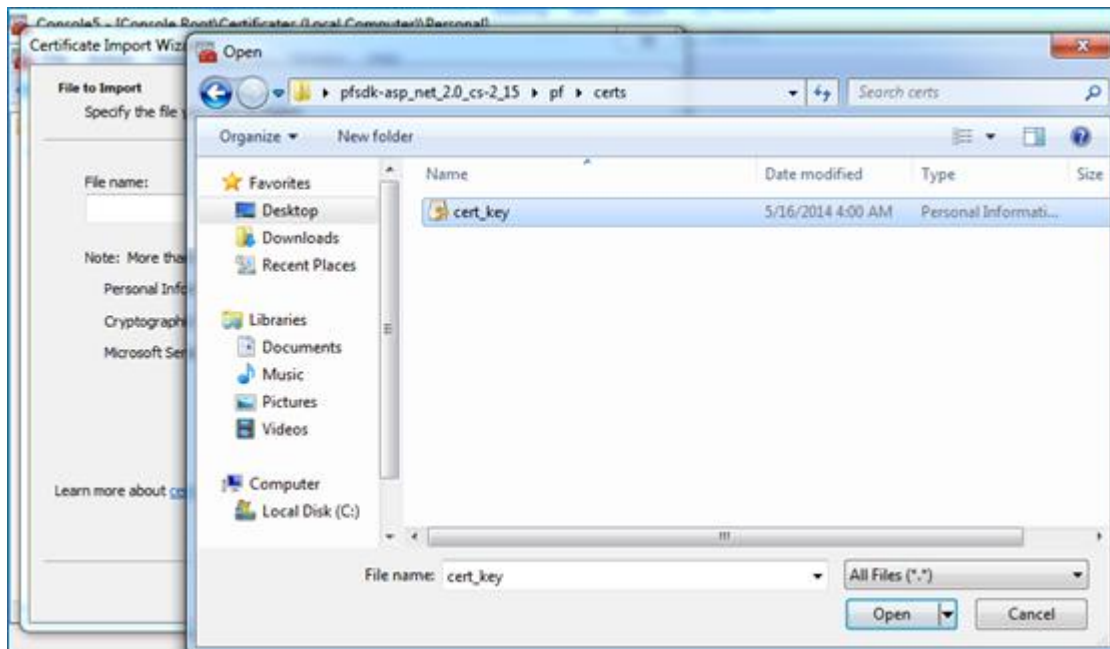
5. Choose **Local computer**, click **Finish** then click **OK**.



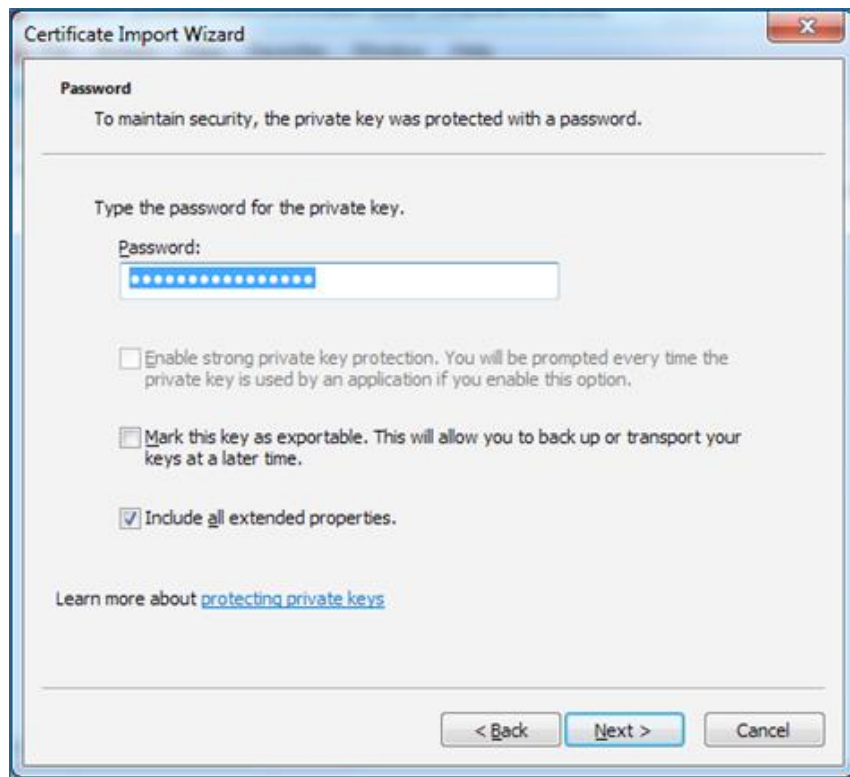
- Click **OK** and go to **Certificates > Personal**. Right-click and choose **All Tasks > Import...**



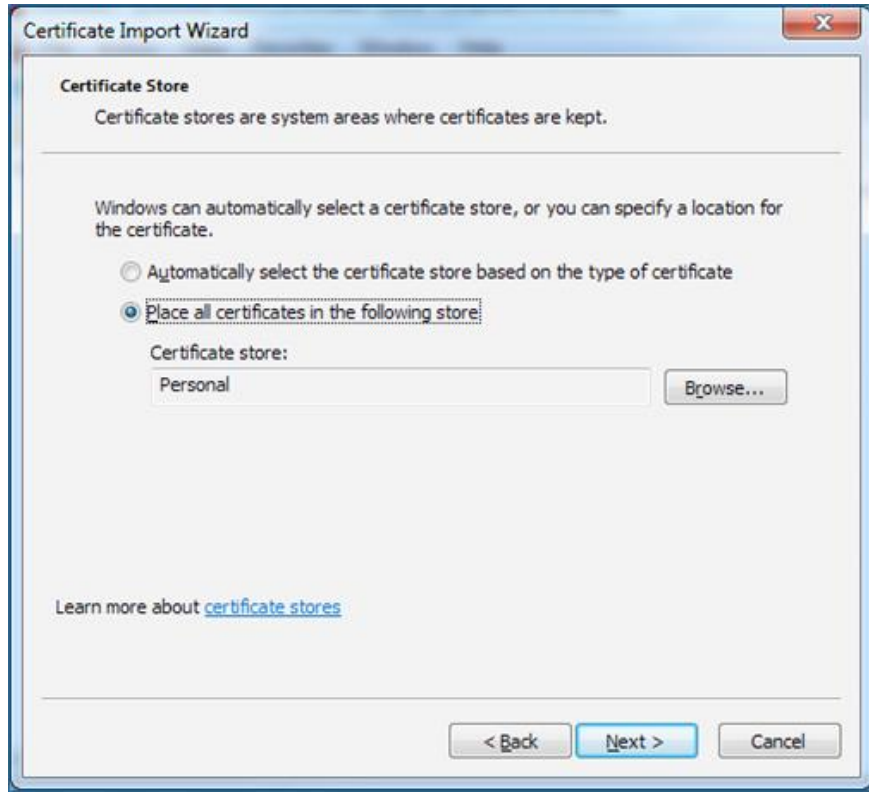
- Click **Next**. Click **Browse** and go to the unarchived folder and open the **pf > certs** folder. Make sure **All files** is selected in the drop-down filter. Select the **cert_key.p12** file.



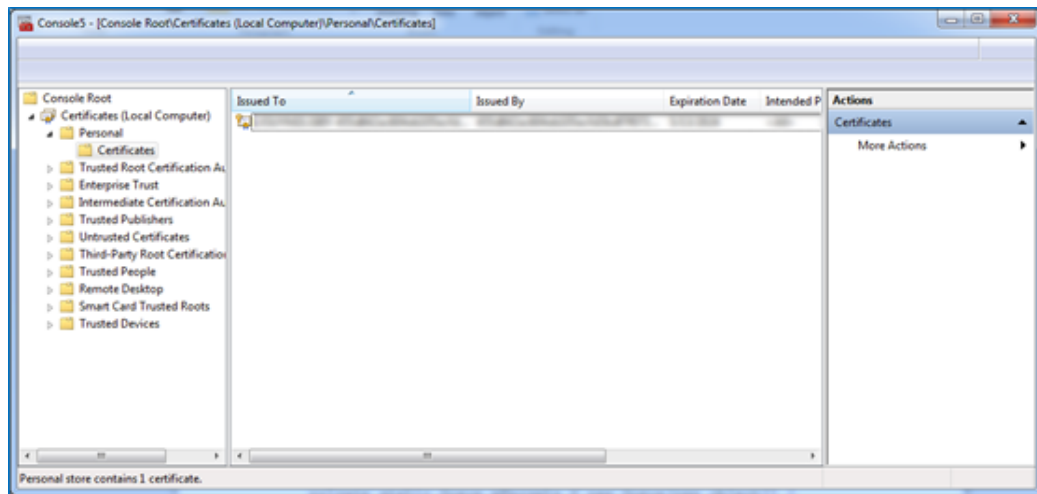
- Click **Next**. Fill in the certificate password retrieved at [Step 8](#).



9. Click **Next**, then click **Finish**.
10. Click **Next**. Make sure the **Personal** store is selected.

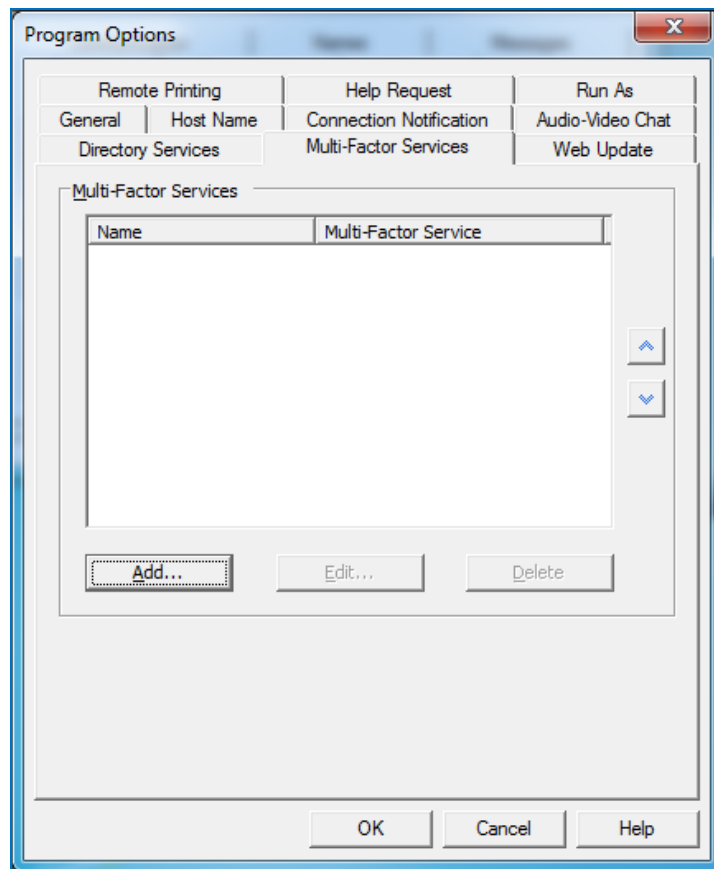


11. Click **Next** and then **Finish**. The certificate is now installed and it should appear in the **Personal** folder.



3.2 Configure the Host

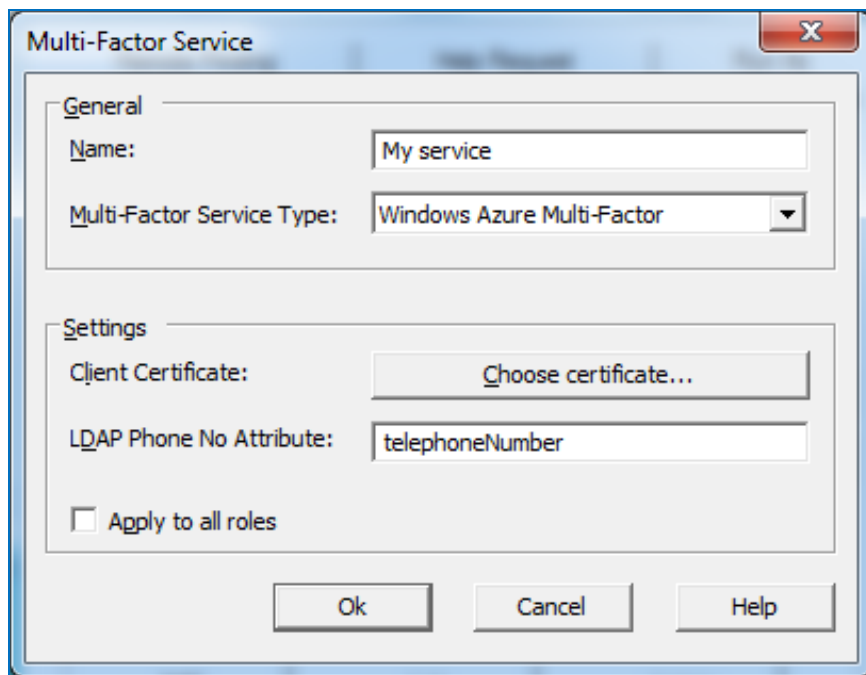
1. Make sure the Netop Remote Control Host version 11.6 is installed.
2. Go to **Tools > Program Options > Multi-Factor Services**. This area allows you to add multiple multi-factor authentication services.
Note: Once defined in this area they can be applied to different role groups as presented below.



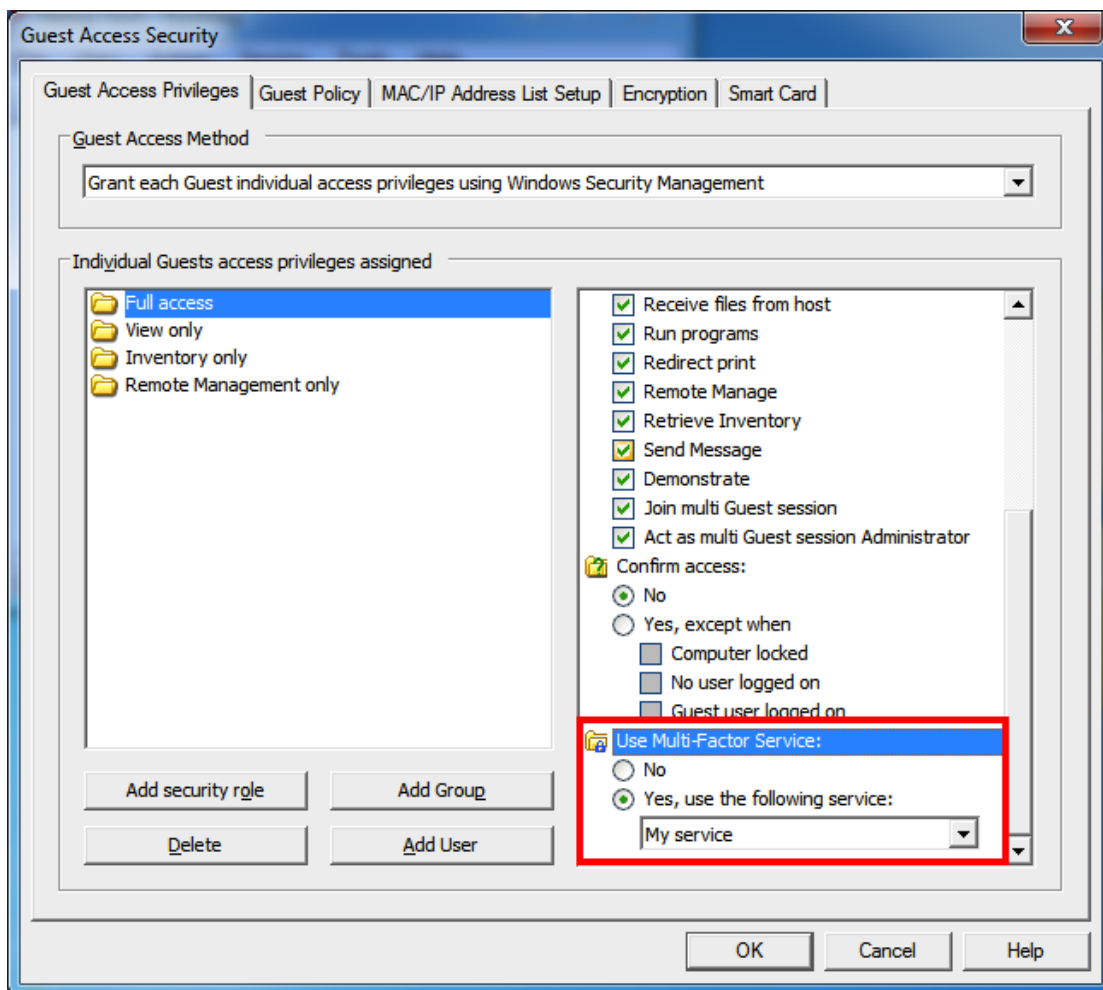
3. Click **Add**.

- Provide the service a **name**.
- Select **Windows Azure Multi-Factor** for the **Multi-Factor Service Type**.
- Choose the certificate that was previously installed under **Client Certificate**.
- The **LDAP Phone No Attribute** identifies the user's telephone number. It will be used to send user the token to be used for multi-factor authentication.
- Select the **Apply to all roles** check box to apply the multi-factor authentication to all roles defined in the Directory Services.

Note: Multi-factor authentication applies to all roles only if the Guest Access Method selected from **Tools > Guest Access Security** is either *Grant each Guest individual access privileges using Windows Security Management* or *Grant each Guest individual access privileges using Directory services*.



4. Click **Ok** and then **OK**. This will finalize the configuration of the authentication service on the Host machine.
5. In order to associate the service with actual users, go to **Tools > Guest Access Security**. If **Directory Services** or **Windows Management** is used, a new area is displayed under the access privileges area.

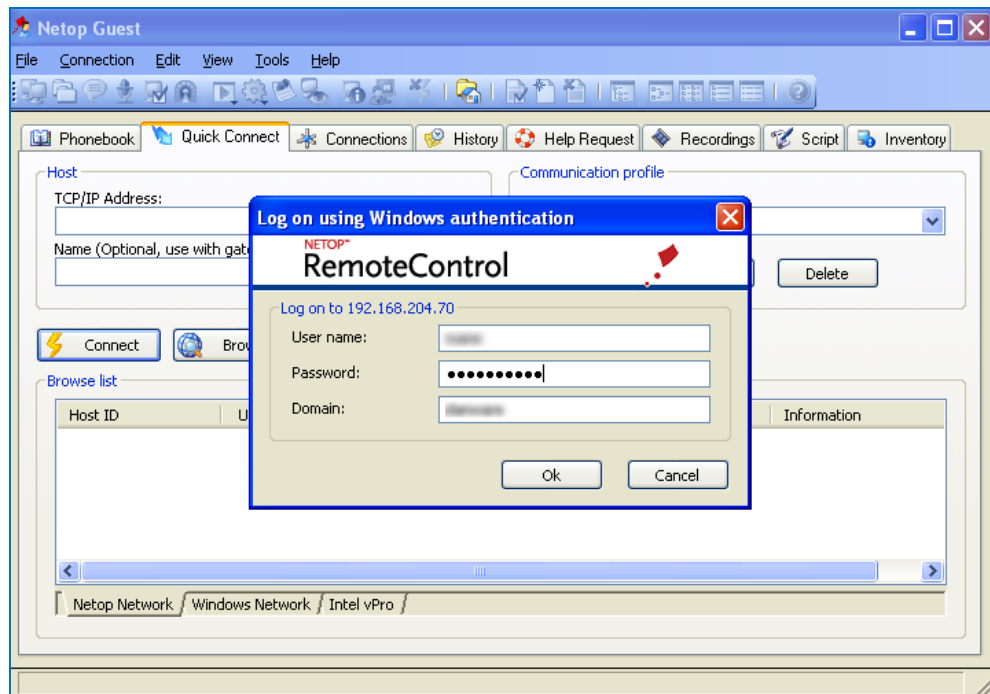


This allows enabling/disabling of the Multi-Factor Authentication services per role.

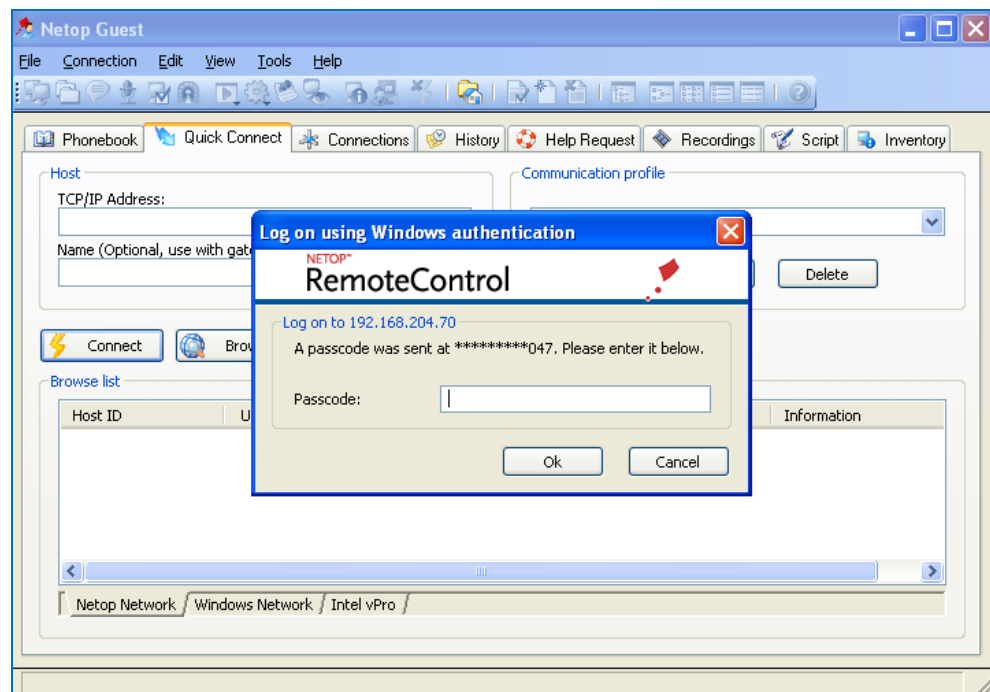
4 Connect to the Host machine

Make sure that the Guest is updated to the 11.6 version.

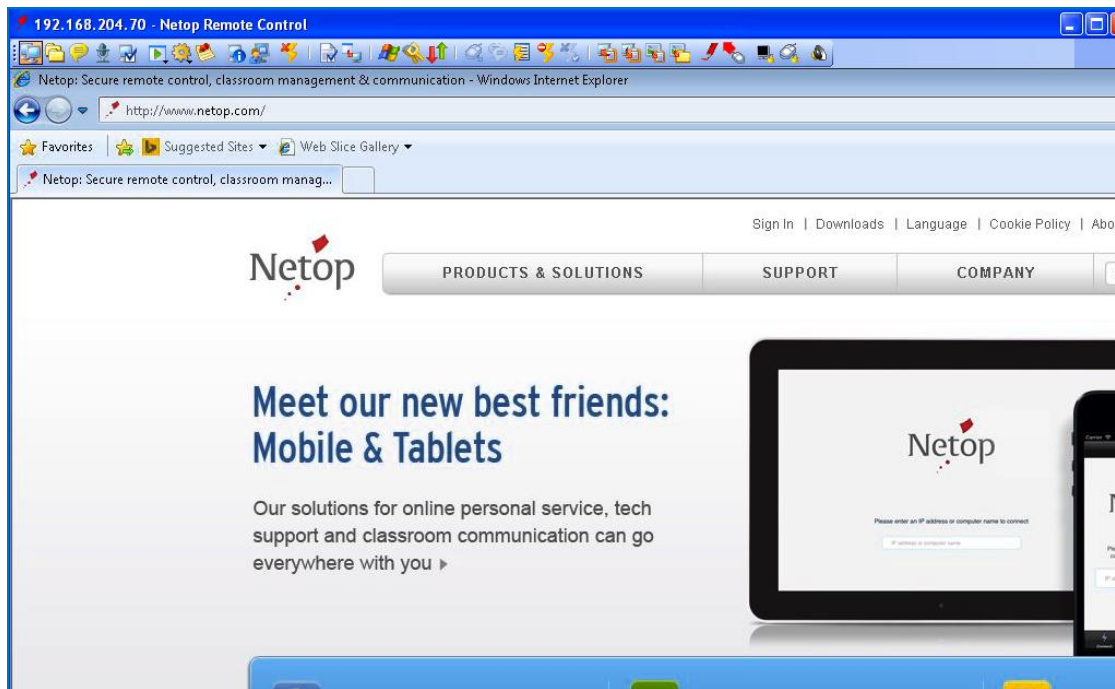
1. Connect to the device by filling in the credentials



2. A passcode will be sent to your mobile phone. Fill in the passcode.



The remote session has started



5 Troubleshoot

5.1 I do not receive any text message.

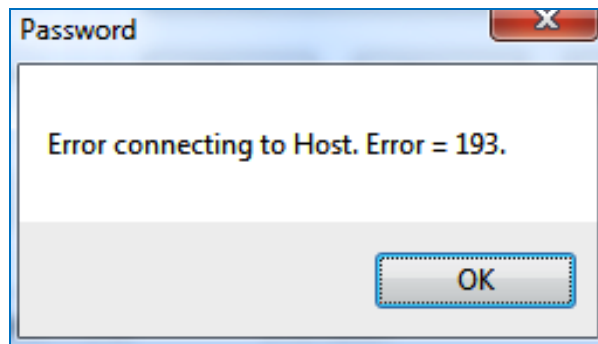
1. Check the **Usage** report in the **Manage** area. Generate a report for that timeframe and then go to **Queued** area and see if the message has been sent.

USERNAME	AUTHENTICATION DATE	PHONE NUMBER	AUTH'D	CALL RESULT	AUTH TYPE	APPLICATION	MODE	INITIATING IP	COMPUTER	SERVER IP
				Text Message Sent						
				Text Message Sent						
				Text Message Sent						
				Text Message Could Not Be Sent						
				Text						

2. Check the phone number. It should not contain any spaces.

5.2 Error connecting to Host. Error = 100

After filling in the credentials, I get a message similar to this: **Error connecting to Host. Error = 100.**



1. Double-check the Windows Azure information. Make sure that the certificate you downloaded and the password are correct.
2. Check [I do not receive any text message.](#)