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 <u>www.netop.com</u>.

Contents

| 1 | Introduct | tion | 2 |
|---|-----------|---------------------------------------|------|
| 2 | Retrieve | the Windows Azure information | 3 |
| 3 | Configur | e 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 | Troubles | hoot | . 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 multifactor 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 (<u>link</u>) or use your existing Windows Azure account and login (<u>link</u>).
- 2. Go to Portal.
- 3. Go to ACTIVE DIRECTORY > MULTI-FACTOR AUTH PROVIDERS and click CREATE A NEW MULTI-FACTOR AUTHENTICATION PROVIDER.

| Microsoft Azure 🗸 🗸 🗸 🗸 🗸 🗸 | CREDIT STATUS |
|-----------------------------|-----------------------------------------------------------------------------------|
| | active directory |
| | DIRECTORY ACCESS CONTROL NAMESPACES MULTI-FACTOR AUTH PROVIDERS RIGHTS MANAGEMENT |
| | You have no Multi-Factor Authentication providers. Add one |
| | |
| | |
| | |
| | |
| | |
| ACTIVE DIRECTORY | |
| | |
| | |

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

| NEW | | | | ۲ |
|------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ∎ 8 () | VISUAL STUDIO CHEME VISUAL STUDIO CHEME VISUAL STUDIO CHEME CON | DRECTORY ACCESS CONTROL MULTI-FACTOR AUTH PROVIDER | У QUICK СМАТІ | NAME My multi factor service URACE MODEL Per Enabled User DBECTORY Do not link a directory The usage model cannot be changed after the Multi-Packor Authentication provider has been created. |
| | | | | CREATE 🕑 |

- Microsoft Azure 🛛 🗸 🌐 marius.ne@hotmail.com 🗕 active directory 00 DIRECTORY ACCESS CONTROL NAMESPACES MULTI-FACTOR AUTH PROVIDERS RIGHTS MANAGEMENT DB STATUS SUBSCRIPTION DIRECTORY NAME USAGE MODEL My multi factor service 🛛 🔿 🗸 Active ß
- 5. Click the Manage icon located at the bottom of the page.

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

X 4

11

NEW

| USER ADMINISTRATION | Welcome | | | | | |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
| Block/Unblock Users | | | | | | |
| One-Time Bypass | Tokenless multi-factor authentication is now available to your company. If you have any questions, please contact support. | | | | | |
| VIEW A REPORT | My multi factor service | | | | | |
| Usage | Account ID: LXSU-YM2-LGBIY | | | | | |
| Server Status | | | | | | |
| Blocked User History | VIEW A REPORT | | | | | |
| Bypassed User History | View usage of all users of Multi-Factor Authentication within an organization | | | | | |
| Fraud Alert | | | | | | |
| Queued | CONFIGURE | | | | | |
| CONFIGURE | Configure Multi-Factor Authentication settings such as caching, voice messages and notifications received by users | | | | | |
| Settings | DOWNLOADS | | | | | |
| Caching | Download the Multi-Factor Authentication Server | | | | | |
| Voice Messages | | | | | | |
| Notifications | | | | | | |
| DOWNLOADS | | | | | | |
| Server | | | | | | |
| SDK | | | | | | |

DELETE

Z

P

11 🕐

| Wind | ows Azu | ire N | lulti- | Factor A | uthentication | |
|---------------------------|------------------|----------------|---------------|-------------------------|--------------------------------------------------------------------|--|
| USER ADMINISTRATION | Downloa | de SDI | / | | | |
| Block/Unblock Users | Downloads SDK | | | | | |
| One-Time Bypass | Download a conv | of the Multi | Eastor Autho | atication SDK The SDK | is available in a variety of languages. Instructions for using the | |
| VIEW A REPORT | SDK are included | in the archive | . The Multi-F | actor Authentication SI | DK is compatible with all Windows and Unix-like systems. | |
| Usage | | | | | | |
| Server Status | LANGUAGE | ZIP | TAR | RELEASE NOTES | | |
| Blocked User History | Perl | Download | Download | View | | |
| Bypassed User History | P.L. | Developed | Developed | View | | |
| Fraud Alert | киру | Download | Download | View | | |
| Queued | PHP | Download | Download | View | | |
| | ASP.NET 1.1 C# | Download | Download | View | | |
| CONFIGURE | ASP.NET 1.1 VB | Download | Download | View | | |
| Settings | ASP.NET 2.0 C# | Download | Download | View | | |
| Caching Voice Messages | ASP.NET 2.0 VB | Download | Download | View | | |
| Notifications | Java | Download | Download | View | | |
| DOWNLOADS | De els | | | | | |
| Server | DACK | | | | | |
| SDK | | | | | | |

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

| pfsdk-asp_net_2. | 0_cs-2_15 ⊧ | | | |
|------------------|-----------------|-------------------|-------------|-------------------|
| | Name | <u>^</u> | | Date modified |
| | 🕕 pf | | 1 | 5/19/2014 7:16 AM |
| | Call_results | | | 5/19/2014 7:16 AM |
| | 📴 example | | | 5/19/2014 7:16 AM |
| | example.aspx.c | :s | | 5/19/2014 7:16 AM |
| | README | | | 5/19/2014 7:16 AM |
| | 📃 release_notes | | | 5/19/2014 7:16 AM |
| | | | | |
| ame | | Date modified | Туре | 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.

| Programs (1) | |
|--------------------|---------------|
| 🐻 mmc | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| P See more results | |
| mmc | X Shut down > |
| Ľ | |
| 🔊 🖉 📋 | O |
| | |

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

| - | Console4 - [Console Root] | |
|---|---------------------------------|----------|
| | File Action View Favorites Wind | low Help |
| ¢ | New | Ctrl+N |
| | Open | Ctrl+O |
| | Save | Ctrl+S |
| | Save As | |
| | Add/Remove Snap-in | Ctrl+M |
| | Options | |
| | 1 C:\Windows\system32\devmgmt | |
| | 2 C:\Windows\system32\compmgn | nt |
| | Exit | |
| | | |

3. Choose Certificates and click Add

| ap-in | Vendor | - | Console Root | Edit Extensions |
|------------------------------------------|--------------------------------|---|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ActiveX Control Authorization Manager | Microsoft Cor Microsoft Cor | | | Bemove |
| Certificates | Microsoft Cor | Е | | |
| Component Services | Microsoft Cor | | | Move Up |
| Computer Managem | Microsoft Cor | | | Move Down |
| Device Manager | Microsoft Cor | | Add > | Contraction of the second seco |
| Disk Management | Microsoft and | | | |
| Event Viewer | Microsoft Cor | | | |
| Folder | Microsoft Cor | | | |
| Group Policy Object | Microsoft Cor | | | |
| IP Security Monitor | Microsoft Cor | | | |
| IP Security Policy M | Microsoft Cor | | | |
| Link to Web Address | Microsoft Cor | + | | Advanced |
| cription: | | | | |
| | | | | |

| Certificates snap-in | × |
|---------------------------------------------------------------------------------------------------------------------|---|
| This snap-in will always manage certificates for: . My user account . Service account . Computer account . | |
| < <u>B</u> ack Finish Cance | |

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

| elect Computer | × |
|-----------------------------------------------------|-----------------------------------------------------------------------------------|
| Select the computer you war | nt this snap-in to manage. |
| This snap-in will always ma | nage: |
| Local computer: (the c | computer this console is running on) |
| O Another computer: | Browse |
| Allow the selected corr only applies if you save | nputer to be changed when launching from the command line. This e the console. |
| | |
| | |
| | |
| | |
| | |
| | |
| | < <u>B</u> ack Finish Cancel |

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

| Snap-in Vi ActiveX Control M | /endor | 1 | | Console Root | | Edit Extensions |
|---------------------------------|---------------|---|-------|-------------------|----------------|---------------------|
| ActiveX Control M | | | | Carlifornian A. | and Committee) | man ellise and pro- |
| | ficrosoft Cor | | | ugr Ceroncates (L | ocar computer) | Remove |
| Authorization Manager M | ficrosoft Cor | | | | | Genere |
| Certificates M | ficrosoft Cor | E | | | | |
| Component Services M | ficrosoft Cor | | | | | Move Up |
| Computer Managem M | ficrosoft Cor | | | | | Maura Davier |
| Device Manager M | ficrosoft Cor | | < bba | | | Move Down |
| Disk Management M | ficrosoft and | | | | | |
| 👌 Event Viewer 🛛 🕅 | ficrosoft Cor | | | | | |
| Folder M | ficrosoft Cor | | | | | |
| Group Policy Object M | ficrosoft Cor | | | | | |
| JP Security Monitor 👘 M | ficrosoft Cor | | | | | |
| 🛃 IP Security Policy M M | ficrosoft Cor | | | | | |
| Link to Web Address M | ficrosoft Cor | - | | | | Advanced |
| • · · · · · · · | | | 1 | | | |
| | | Ŧ | | L | | Advanced |

6. 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.

| File to Import Specify the file a | G + pfsdk-asp_net_2.0_cs-2_15 + pf + certs | • + search | certs |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|--------------------|
| | Organize - New folder | | 🗉 • 🗔 🛭 |
| File name: | 🔆 Favorites | Date modified | Туре S |
| | E Desktop | 5/16/2014 4:00 AM | Personal Informati |
| Note: More the Personal Info Cryptograph Microsoft Ser | 22 Recent Places 32 Libraries 3 Documents J Music Situres Yideos | | |
| Learn more about <u>ce</u> | 1 Computer | | |
| Learn more about <u>ce</u> | Computer Local Disk (C:) + | m | |

8. Click **Next**. Fill in the certificate password retrieved at <u>Step 8</u>.

NRC – Windows Azure Multi-Factor Authentication

| rtificate I | mport Wizard |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Passwor | d |
| Tor | naintain security, the private key was protected with a password. |
| Тур | e the password for the private key. |
| | Password: |
| | |
| | |
| [| Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option. |
| [| Mark this key as exportable. This will allow you to back up or transport your keys at a later time. |
| [| ✓ Include <u>a</u> ll extended properties. |
| Learn mo | pre about <u>protecting private keys</u> |
| | < <u>B</u> ack <u>N</u> ext > Cancel |

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

| Certificate Store | |
|-------------------------------------------------------|------------------------------------------------------|
| Certificate stores are system areas v | where certificates are kept. |
| Windows can automatically select a c the certificate. | certificate store, or you can specify a location for |
| Automatically select the certific | cate store based on the type of certificate |
| Place all certificates in the follo | owing store |
| Certificate store: | |
| Personal | Browse |
| | |
| Learn more about <u>certificate stores</u> | |

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

| Console5 - [Console Root)Certificates | s (Local Computer)/Personal/Certificates] | - | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|------------------------|-----------------|------------|----------------|
| Console Root | Issued To | Issued By | Expiration Date | Intended P | Actions |
| a 🧊 Certificates (Local Computer) | 2 | THE OWNER AND ADDRESS. | The second | | Certificates |
| Personal Certification Au Certification Au Enterprise Trust Untrusted Root Certification Au Trusted Publishers Untrusted Certification Trusted Publishers Trusted Peript Root Certification Trusted People Remote Desktop Smart Card Trusted Roots Trusted Devices | | | | | More Actions • |
| Personal store contains 1 contificate | | | | | |
| Personal store contains 1 certificate. | | | | - | |

3.2 Configure the Host

- 1. Make sure the Netop Remote Control Host version 11.6 is installed.
- 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.

| Program Options | New 1 . N | × |
|------------------------------------------------------------|------------------------------------------------------------------|------------------------------------------|
| Remote Printing General Host Name Directory Services | Help Request Connection Notification Multi-Factor Services | Run As Audio-Video Chat Web Update |
| Name | Multi-Factor Service | |
| <u>Add</u> | <u>E</u> dit | Delete |
| | OK Can | cel Help |

- 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*.

| Multi-Factor Service | × | | | | |
|------------------------------------------|----------------------------|--|--|--|--|
| General | | | | | |
| <u>N</u> ame: | My service | | | | |
| Multi-Factor Service Type: | Windows Azure Multi-Factor | | | | |
| Settings | | | | | |
| Client Certificate: | Choose certificate | | | | |
| LDAP Phone No Attribute: telephoneNumber | | | | | |
| Apply to all roles | | | | | |
| Ok Cancel Help | | | | | |

- 4. Click **Ok** and then **OK**. This will finalize the configuration of the authentication service on the Host machine.
- 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.

NRC – Windows Azure Multi-Factor Authentication

| Guest Access Security | - | — × | | | | | |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
| Guest Access Privileges Guest Privileges Guest Access Method | Guest Access Privileges Guest Policy MAC/IP Address List Setup Encryption Smart Card Guest Access Method | | | | | | |
| Grant each Guest individual a | ccess privileges using Windo ges assigned | ws Security Management Receive files from host Run programs Redirect print Remote Manage Retrieve Inventory Send Message Demonstrate Join multi Guest session Act as multi Guest session Administrator Confirm access: No Yes, except when Computer locked No user logged on | | | | | |
| Add security role | Add Grou <u>p</u> | ○ No ③ Yes, use the following service: | | | | | |
| <u>D</u> elete | <u>A</u> dd User | My service | | | | | |
| | | OK Cancel Help | | | | | |

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

| 🅭 Netop Guest 📃 | |
|---------------------------------------------------------------------------------------------------|---|
| Eile <u>C</u> onnection <u>E</u> dit <u>Vi</u> ew <u>T</u> ools <u>H</u> elp | |
| | |
| 🔟 Phonebook 🐚 Quick Connect 🦂 Connections 🤣 History 🤣 Help Request 🐟 Recordings f Script 🗟 Invent | y |
| - Host | |
| TCP/IP Address: | |
| Name (Optional, use with gat Permoto Control | |
| Delete | |
| Log on to 192.168.204.70 | |
| Soft Hunder | |
| Browse list | |
| | - |
| Ok Cancel | |
| | |
| | |
| | 2 |
| Netop Network / Windows Network / Intel vPro / | |
| | |
| | |

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

| 🥭 Netop Guest 📃 🗖 🔀 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Eile Connection Edit View Tools Help |
| 1211日 - 12111日 - 1211101 - 1211101 - 1211101 - 1211101 - 1211101 - 1211101 - 1211101 - 1211100 - 1211100 - 12111000 - 12111000 - 121110000000000 |
| Host Connect Connect Connections Recordings Connections Connections Connections Connections Connections Communication profile |
| TCP/IP Address: |
| Log on using Windows authentication |
| RemoteControl |
| Sconnect Cog on to 192.168.204.70 A passcode was sent at ******047. Please enter it below. Browse list Host ID U |
| Ok Cancel |
| |
| Netop Network / Windows Network / Intel vPro / |
| |

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 | | | | | | |
| | 1000 | | - | 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.

| Password | x |
|---------------------------|--------------|
| Error connecting to Host. | Error = 193. |
| | ОК |

- 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.