NETOP™

RemoteControl

Secure Remote Management and Support

Release Notes

Product/version/build:	Remote Control 11.6 (2014145)
	ActiveX Guest 11.1 (2014145)
Shipping date:	3rd of June 2014

Introduction

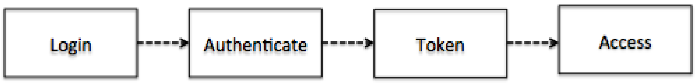
These release notes contain information relating to a new version of Netop Remote Control (Windows only) including the ActiveX Guest (nguestx.ocx). Version 11.6 introduces new multi-factor authentication options, including extending existing Radius capabilities and adding Windows Azure Multi-Factor authentication.

In order to use Netop Remote Control 11.6, new license keys are required. Customers who have a valid Netop Advantage annual support and upgrade agreement are eligible to upgrade to the new version at no additional cost and should receive their upgrade license keys shortly after the public release date.

If you have questions about your license or wish to purchase an upgrade to Netop Remote Control 11.6, please contact **Netop Customer Service** or your local **Netop Partner** for more information.

Multi-Factor authentication

With this release, Netop Remote Control offers new multi-factor authentication options, main focus being extending the services by providing phone based passcodes.



The new security flows implemented are:

- SMS token (passcode sent through a text message)
- Soft token (passcode is generated in an external application. E.g.: an app on the phone)
- Challenge-based token (server sends a challenge, the user inserts this challenge in the token generator and a token is generated)

Extended Radius support

The Netop Security Server has started offering authentication against RADIUS (Remote Authentication Dial In User Service) environments starting version 11.0.

RADIUS is a client/server protocol that is often used to centrally validate remote users and authorize their access to existing network resources integrating well with existing technologies including VPN, RAS, Active Directory and Token based authentication solutions.

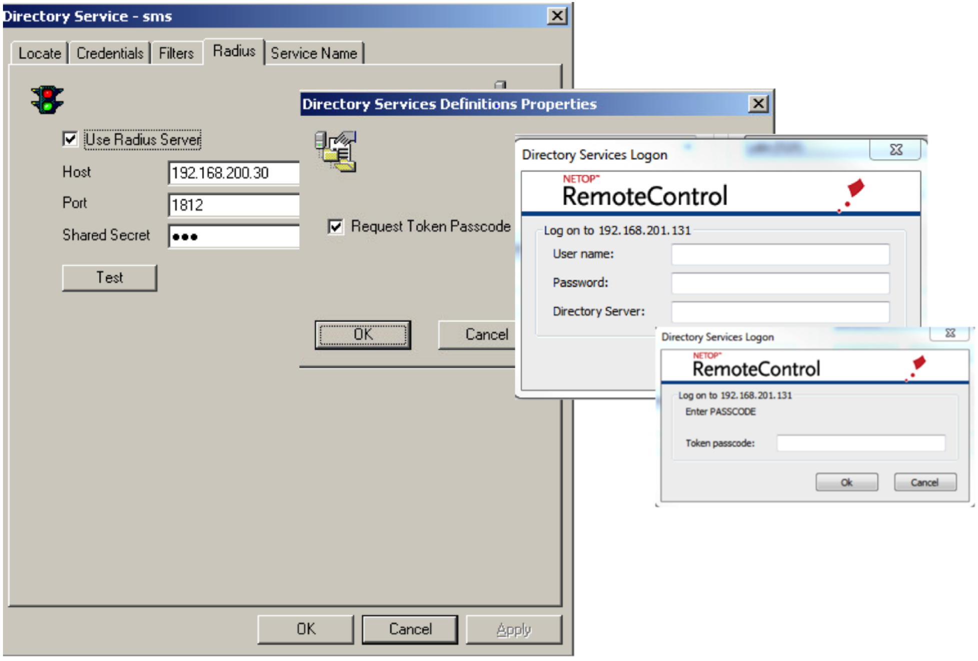
Starting this version of Netop Remote Control, using RADIUS with Netop Remote Control allows the Security Server to authenticate remote support sessions via compatible multi-factor authentication methods, where the Guest user needs to provide their username and password initially, followed by a one-time generated passcode that can be derived from a variety of sources including hardware devices or SMS tokens. In the previous integration all components had to be filled in by the user at the same time. The new security flow makes it possible for the authenticated user to receive a specific passcode.

No change is required for the integration with Radius.

That is in order to use the RADIUS implementation the Security Server should be configured to use Directory Services authentication. This requires that the Preferred Guest type is set to ‘Guests enter Directory Services username and password’ in the Security Policies section of the Security Manager.

In addition, a connection to a RADIUS server should also be configured in the ‘Radius Server’ tab under the Directory Service settings.

Finally, under the Directory Services definitions in the Security Manager, the ‘Request Token Passcode’ option should be enabled. This is available in the Properties section.



☑ Use Radius Server

Host: 192.168.200.30

Port: 1812

Shared Secret: •••

☑ Request Token Passcode

Log on to 192.168.201.131

User name:

Password:

Directory Server:

Log on to 192.168.201.131

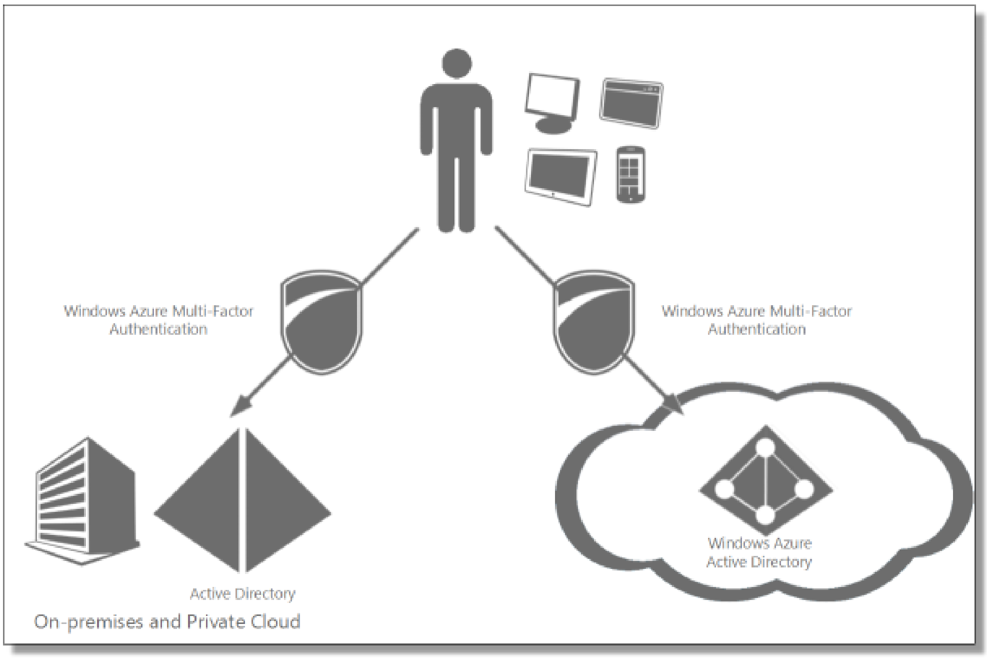
Enter PASSCODE

Token passcode:

Windows Azure Multi-Factor Authentication

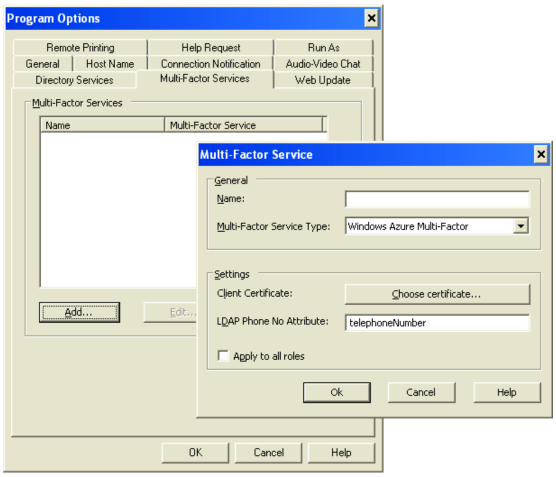
Windows Azure Multi-Factor Authentication reduces organizational risk and helps enable regulatory compliance by providing an extra level of authentication, in addition to a user's account credentials, to secure employee, customer, and partner access. Azure Multi-Factor Authentication can be used for both on-premises and cloud applications.

Netop Remote Control provides integration to this service. Companies can now use their own Windows Azure Multi-Factor Authentication in Netop Remote Control.


Windows Azure Multi-Factor Authentication
Windows Azure Multi-Factor Authentication
Windows Azure Active Directory
Active Directory
On-premises and Private Cloud

Source: http://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication/

This service is configured on the Host side. First step is to add the corresponding Windows Azure Multi-Factor service. This is achieved from the new Multi-Factor Services tab from Tools > Program Options.



Name:

Multi-Factor Service Type: Windows Azure Multi-Factor

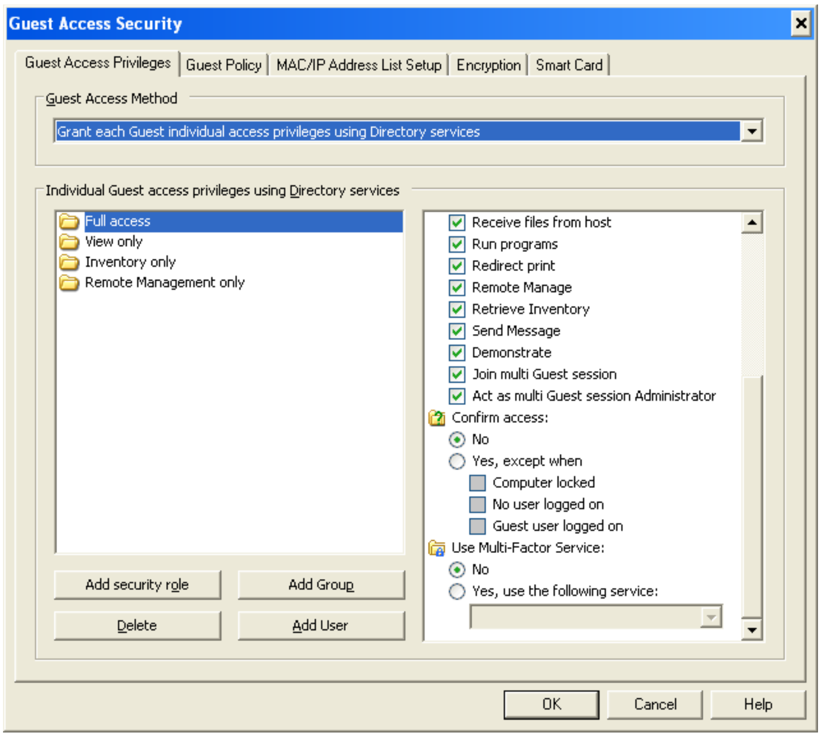
Client Certificate:

LDAP Phone No Attribute: telephoneNumber

☐ Apply to all roles

Netop™ is a trademark of Netop Business Solutions A/S. All other products mentioned in this document are trademarks of their respective manufacturers. Netop Business Solutions A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

Then the service needs to be added to the corresponding Role from Guest Access Security. In this way different multi factor authentication providers can be used for different security roles, allowing security to be very granular.



Guest Access Method: Grant each Guest individual access privileges using Directory services

Individual Guest access privileges using Directory services

- Full access
- View only
- Inventory only
- Remote Management only

☑ 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
□ Guest user logged on

Use Multi-Factor Service:
● No
○ Yes, use the following service:

Screen transfer

In this version, Netop Remote Control comes with screen transfer improvements. The improvements are related to better speed and better overall performance especially when higher latency is involved. Our tests show speed improvements of up to 50%.

Security fix

Heartbleed is a security bug in the OpenSSL library (more info here). This version of Netop Remote Control comes with a fix for it. Affected modules: Host, Security Server, Connection Server, Gateway and Name Server.

Defects resolved

- The demonstrate Feature does not work when using a Host with version 11.5+. *Support case ref: 64208*
- Host version 11.5 does not start on embedded XP. *Support case ref: 85050*
- 64-bit registry keys do not display in Remote Management. *Support case ref: 77662*
- Nowutil fails when defining Sentinel license. *Support case ref: 72861*
- Host installation fails on Windows 8.1 32-bit. *Support case ref: 90878*
- Host doesn't log on Netop Security Server if the name or the IP is not specified. *Support case ref: 65096*

Netop™ is a trademark of Netop Business Solutions A/S. All other products mentioned in this document are trademarks of their respective manufacturers. Netop Business Solutions A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

May 2014 Page 4 of 4