NETOP™

RemoteControl

Secure Remote Management and Support

Multi-factor Authentication using RADIUS

Version 1.1

Netop

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

Starting with Netop Remote Control version 11.0, the Netop Security Server has been extended to offer authentication against RADIUS (Remote Authentication Dial-In User Service) environments. In this version, multi-factor authentication using automatically generated passcodes (e.g. from hardware or software tokens) was supported.

Netop Remote Control version 11.6 provides higher security by extending the existing integration with RADIUS. The integration now works also with on-demand generated passcodes, e.g. sent to mobile devices through SMS, or sent via e-mail.

In version 12.71, a new RADIUS authentication flow is supported, where the RADIUS authentication is done directly with the username and token passcode, instead of expecting a challenge before sending the passcode.

The Guest's access to the Host is validated based on two factors:

- Something the user knows (credentials)
- Something the user has (passcode received by phone or E-mail).

Version 12.76 comes with a new flow, which involves the ability for the RADIUS server to authorize the user via a 2nd factor authentication, independently from the authentication flow implemented by the Netop Security Server. This is achieved by triggering the 2nd factor authentication through additional channels such as push notifications and once the authorization is granted, inform the Netop Security Server of the outcome. This flow needs both the Netop Host and the Netop Security Server version 12.76.

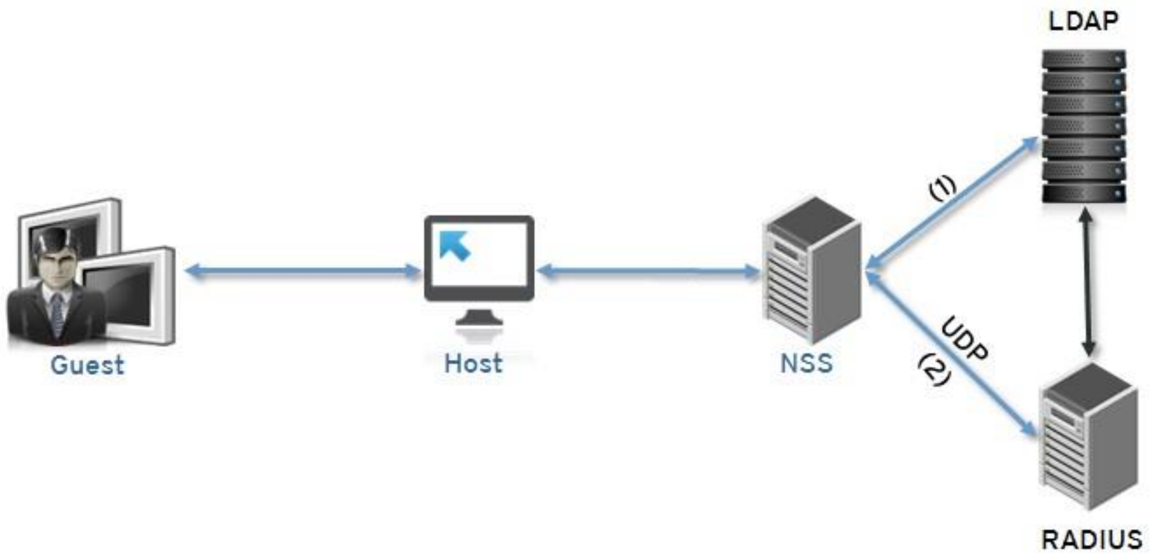
This document explains how to configure the Guest and the Host for RADIUS authentication, with the authentication flows supported in version 11.6, and extended in versions 12.71 and 12.76.

Pre-requisites

- LDAP and RADIUS servers are already setup
- NRC components (Guest, Host and Netop Security Server) and licenses, for a version supporting the required RADIUS flow

Figure 1 shows the high level NRC communication architecture with RADIUS based multi-factor authentication.

Figure 1 - Architecture of NRC multi-factor authentication using RADIUS



+

Steps:

1. LDAP authenticates the user based on the LDAP credentials. Once the Host is validated in LDAP, Netop Security Server sends an Access-Request to the RADIUS server.

   If using synchronously (one-time) generated passcodes, the RADIUS server generates a token code and sends it to the Guest user either by phone or e-mail.

   If using asynchronously (continuously) generated passcode, an automatically generated passcode (from a software or hardware token) is used instead.

2. The Guest is prompted to enter the token code previously received. Once the Guest enters the token, the remote session to the Host starts.

In order to achieve the multi-factor authentication, RADIUS needs to be integrated with other providers of such options. Some of the providers are: SMS Passcode, Duo Security and Dual Shield.

In the Netop Security Server version 12.71, depending on whether the checkbox for “token-only authentication” is set or not, the RADIUS authentication flow is as follows:

1. Full RADIUS flow (“token-only authentication” not selected)
   a. The LDAP credentials are sent to RADIUS in an Access-Request.
   b. RADIUS replies with either an Access-Accept (if the user is not configured to require token authentication), an Access-Reject (containing also the reason for reject), or an AccessChallenge.
   c. If an Access-Challenge is received, the username and passcode are sent to RADIUS in a new Access-Request.
   d. An Access-Accept or Access-Reject is received after RADIUS validates the passcode.

2. Token-only RADIUS flow (“token-only authentication” selected)
    a. The username and passcode are sent to RADIUS in an Access-Request.
    b. An Access-Accept or Access-Reject is received after RADIUS validates the passcode.

In the Netop Security Server version 12.76, depending on whether the checkbox for “token-only authentication” is set or not, the RADIUS authentication flow is as follows:

1. Full RADIUS flow (“token-only authentication” not selected)
    a. The LDAP credentials are sent to RADIUS in an Access-Request.
    b. RADIUS replies with either an Access-Accept (if the user is not configured to require token authentication), an Access-Reject (containing also the reason for reject), or an AccessChallenge.
        i. In the new flow, besides the possible answers described above, based on the RADIUS server configuration, it might initiate its own authorization mechanism, usually through a 2nd factor mechanism, for instance by sending the authenticating user a push notification asking him to confirm his identity or if he/she accepts/denies the connection request. While this is happening behind the scene, the Netop Security Server is waiting for an answer from the RADIUS server; as soon as the authorization mechanism is completed, RADIUS responds to the Netop Security Server with either an Access-Accept, or an Access-Reject (or possibly even an AccessChallenge).
    c. If an Access-Challenge is received, the username and passcode are sent to RADIUS in a new Access-Request.
    d. An Access-Accept or Access-Reject is received after RADIUS validates the passcode.
2. Token-only RADIUS flow (“token-only authentication” selected) – this flow is unchanged compared with version 12.71
    a. The username and passcode are sent to RADIUS in an Access-Request.
    b. An Access-Accept or Access-Reject is received after RADIUS validates the passcode.

2 Configure the Netop Security Server

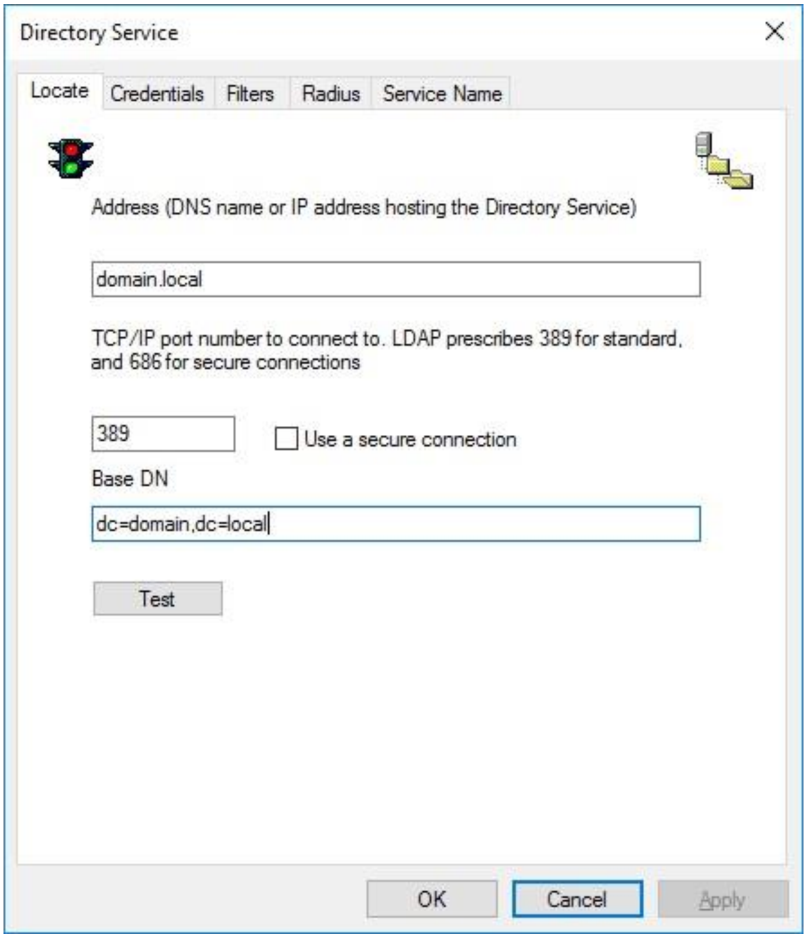
Make sure Netop Security Server version 11.6 or higher is installed. Use the Netop Security Manager (accessible from Start >Security Manager).in order to configure the Netop Security Server.

For detailed information on how to configure NSS for the first time, see Netop Remote Control Administrator's Guide. For details on how to configure the Host to connect to NSS, see Configure the Host machine.

If the Directory Service is already defined (the entry already exists under **Netop Security Management > Directory Services Definitions > Directory Services**), go to Update an existing Directory Service in order to add the RADIUS configuration.

2.1 Add a new Directory Service

1. Under **Netop Security Management > Directory Services Definitions > Directory Services**, right-click on the Records Pane and select **New...** The Locate window displays.
2. In the **Address** field enter the LDAP server name or the IP address hosting the LDAP.
3. In the **Base DN** field, enter the domain controller name in the format: *dc=domain name; dc=local.*



Address (DNS name or IP address hosting the Directory Service)

domain.local

TCP/IP port number to connect to. LDAP prescribes 389 for standard, and 686 for secure connections

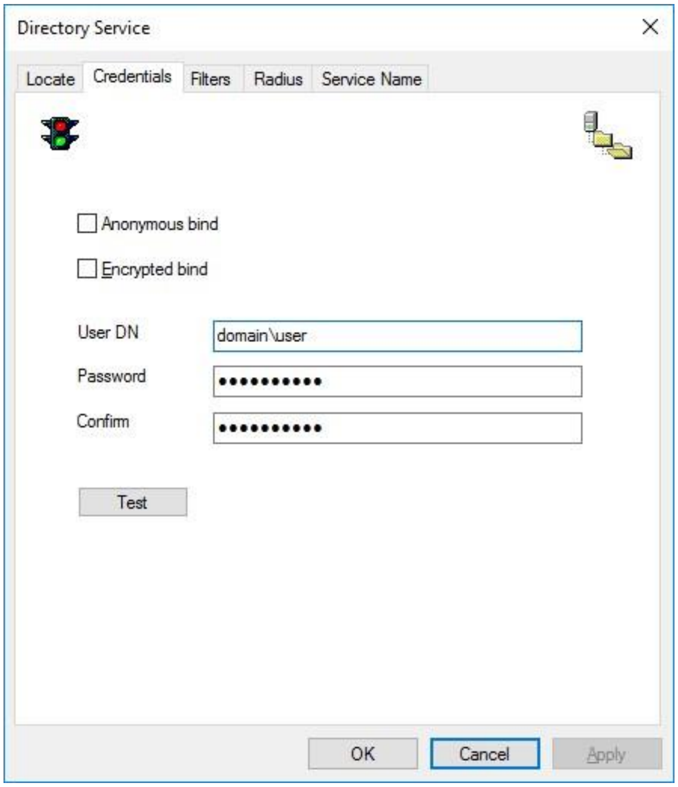
389

☐ Use a secure connection

Base DN

dc=domain,dc=local

4. Click the **Test** button in order to validate connection to the LDAP IP address then click **Next**.
5. Enter the Host credentials; the user who will send / receive requests from the LDAP server and click the **Test** button in order to validate Host credentials. Click **OK**, then **Next**.



☐ Anonymous bind

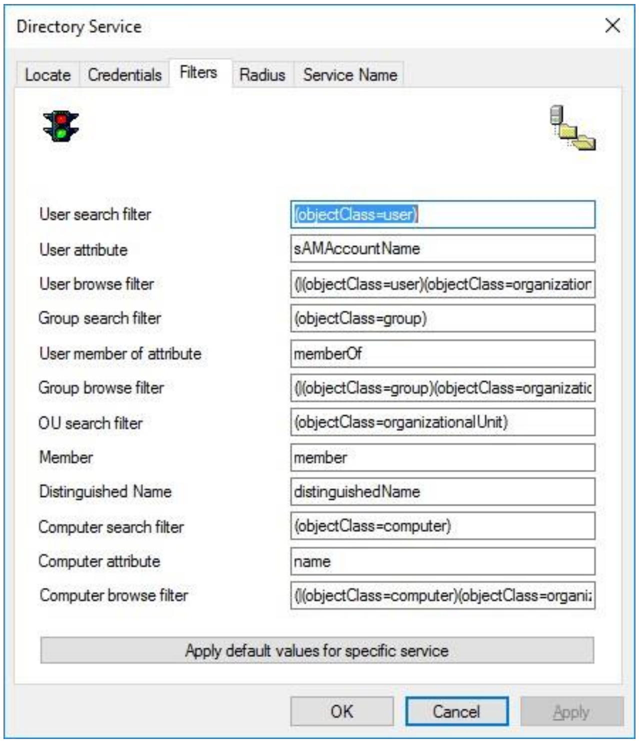
☐ Encrypted bind

User DN: domain\user

Password: ●●●●●●●●●●●

Confirm: ●●●●●●●●●●●

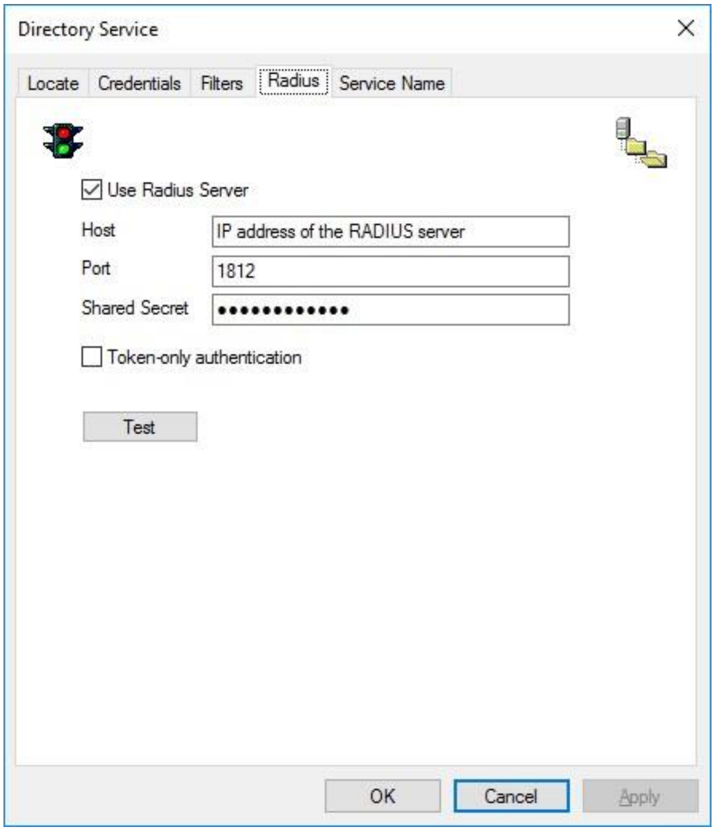
6. In the Filters window, either click the **Apply values for specific service** button and select **Microsoft Active Directory** or fill-in the values manually.



User search filter	(objectClass=user)
User attribute	sAMAccountName
User browse filter	(|(objectClass=user)(objectClass=organizatior
Group search filter	(objectClass=group)
User member of attribute	memberOf
Group browse filter	(|(objectClass=group)(objectClass=organizatic
OU search filter	(objectClass=organizationalUnit)
Member	member
Distinguished Name	distinguishedName
Computer search filter	(objectClass=computer)
Computer attribute	name
Computer browse filter	(|(objectClass=computer)(objectClass=organi:

7. Click **Next**. The RADIUS window displays. Select the **Use Radius Server** checkbox and enter the RADIUS server settings:
   1. In the **Host** field fill in the IP address of the device hosting the RADIUS server.
   2. Optionally, you can change the default RADIUS port. The default value is 1812.
   3. Enter the **Shared Secret** for communication between the NSS and the RADIUS server.

4. Select the **Token-only authentication** checkbox if your RADIUS server expects directly the token passcode in Access-Request messages.



Directory Service

☑ Use Radius Server

Host: IP address of the RADIUS server

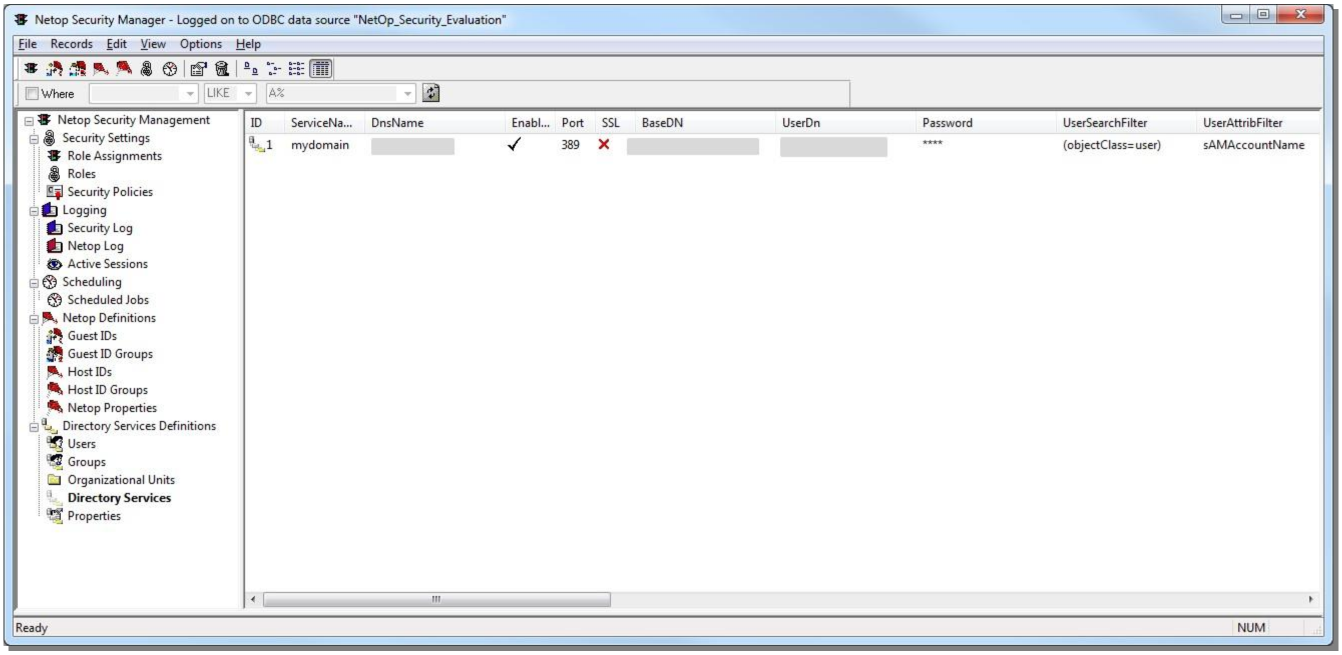
Port: 1812

Shared Secret: ●●●●●●●●●●●●

☐ Token-only authentication

5. Click the **Test** button in order to validate connection to the RADIUS server. Click **OK** then **Next**.

6. Enter the **Name**, an alias name for this Directory Service and click **Finish**. The directory service definition displays in the Records Pane.



ID	ServiceNa...	DnsName	Enabl...	Port	SSL	BaseDN	UserDn	Password	UserSearchFilter	UserAttribFilter
1	mydomain	[redacted]	✓	389	✗	[redacted]	[redacted]	****	(objectClass=user)	sAMAccountName

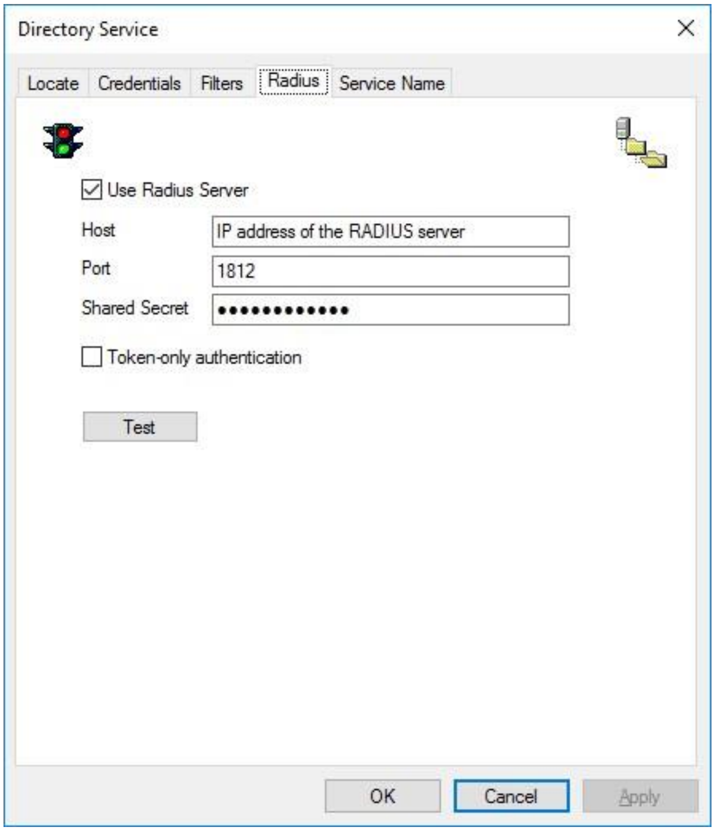
7. Go to Activate RADIUS Multi-Factor Authentication

2.2 Update an existing Directory Service

Go to Netop Security Management > Directory Services Definitions > Directory Services.

1. Double click the specific entry in the Records pane.
2. Click the **Radius** tab. Select the **Use Radius Server** checkbox and enter the RADIUS server settings:
    1. In the **Host** field fill in the IP address of the device hosting the RADIUS server.
    2. Optionally, you can change the default RADIUS port. The default value is 1812.
    3. Enter the **Shared Secret** for communication between the NSS and the RADIUS server.

4. Select the **Token-only authentication** checkbox if your RADIUS server expects directly the token passcode in Access-Request messages.



☑ Use Radius Server

Host: IP address of the RADIUS server

Port: 1812

Shared Secret: ●●●●●●●●●●●●●

□ Token-only authentication

3. Click **OK**.

2.3 Activate RADIUS Multi-Factor Authentication

If using Netop Security Server version 12.60 to 12.70:

1. Under Netop Security Management > Directory Services Definitions > **Properties**, double-click on the **Request Token Passcode** property. The **Directory Services Definition Properties** window displays.
2. Check the **Request Token Passcode** option and click **OK**.

If using Netop Security Server version 12.71 or newer, whenever the **Use Radius Server** option is enabled on a Directory Services definition, RADIUS multi-factor authentication is by default enabled.

2.4 Save Netop Security Server settings

In order for the Netop Security Server configuration to take effect, you need to restart the Netop Security Server.

3 Configure the Host machine

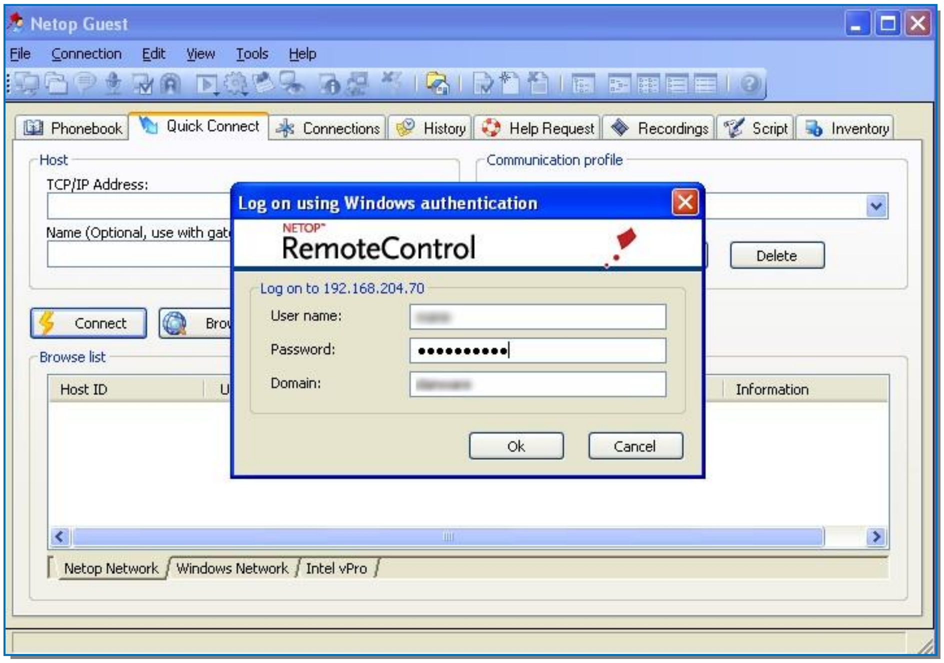
You must use Netop Remote Control Host version 11.6 or higher. Go to **Tools > Guest Access Security** and make sure the Host is configured for NSS.

For detailed information on how to configure the Host to work with NSS, see Netop Remote Control User's Guide.

4 Multi-Factor Authentication – how it works

You must use Netop Remote Control Guest version 11.6 or higher.

1. Connect to the device by filling in the credentials:



Log on using Windows authentication

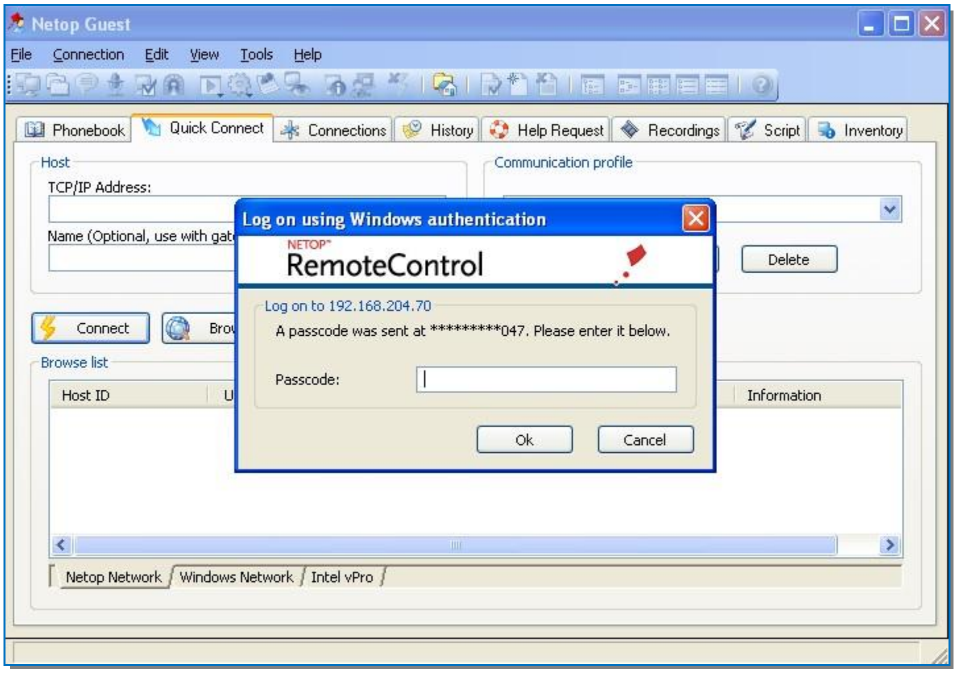
Log on to 192.168.204.70

User name: [redacted]

Password: ●●●●●●●●●●●

Domain: [redacted]

2. Depending on your configuration, a passcode will be sent to your mobile phone or E-mail, or can be read from your software or hardware token. Fill in the passcode.



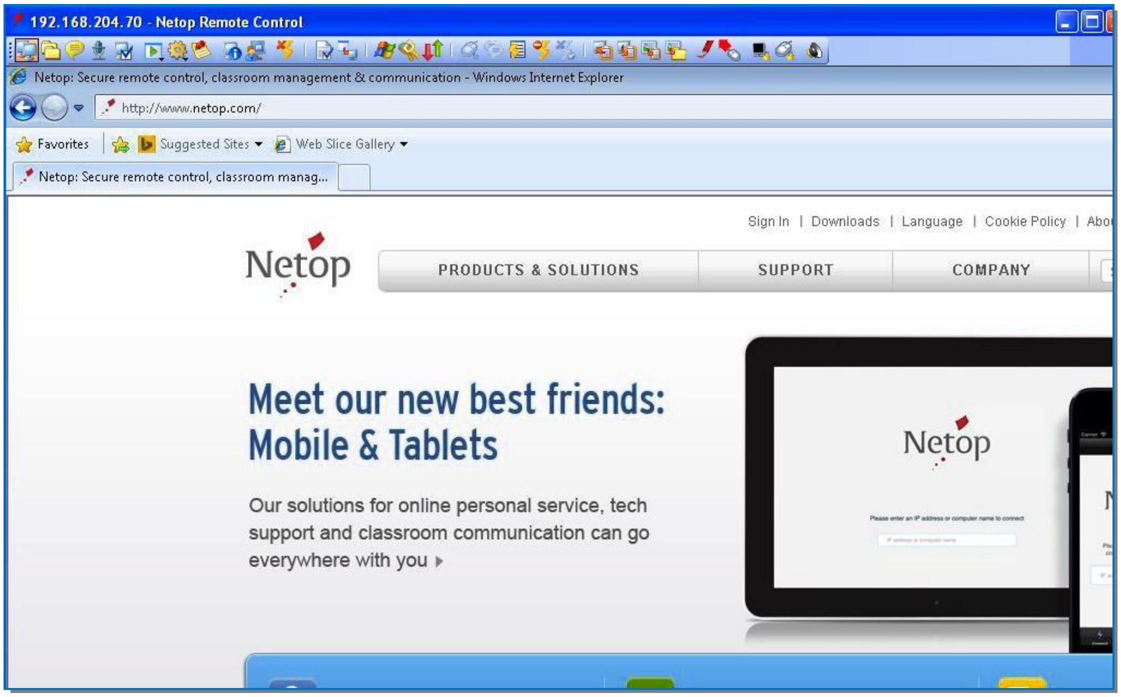
Log on using Windows authentication

Log on to 192.168.204.70

A passcode was sent at *********047. Please enter it below.

Passcode:

The remote session starts:


192.168.204.70 - Netop Remote Control
Netop: Secure remote control, classroom management & communication - Windows Internet Explorer
http://www.netop.com/
Favorites
Suggested Sites
Web Slice Gallery
Netop: Secure remote control, classroom manag...
Sign In | Downloads | Language | Cookie Policy | Abo
Netop
PRODUCTS & SOLUTIONS
SUPPORT
COMPANY
Netop

Meet our new best friends: Mobile & Tablets

Our solutions for online personal service, tech support and classroom communication can go everywhere with you