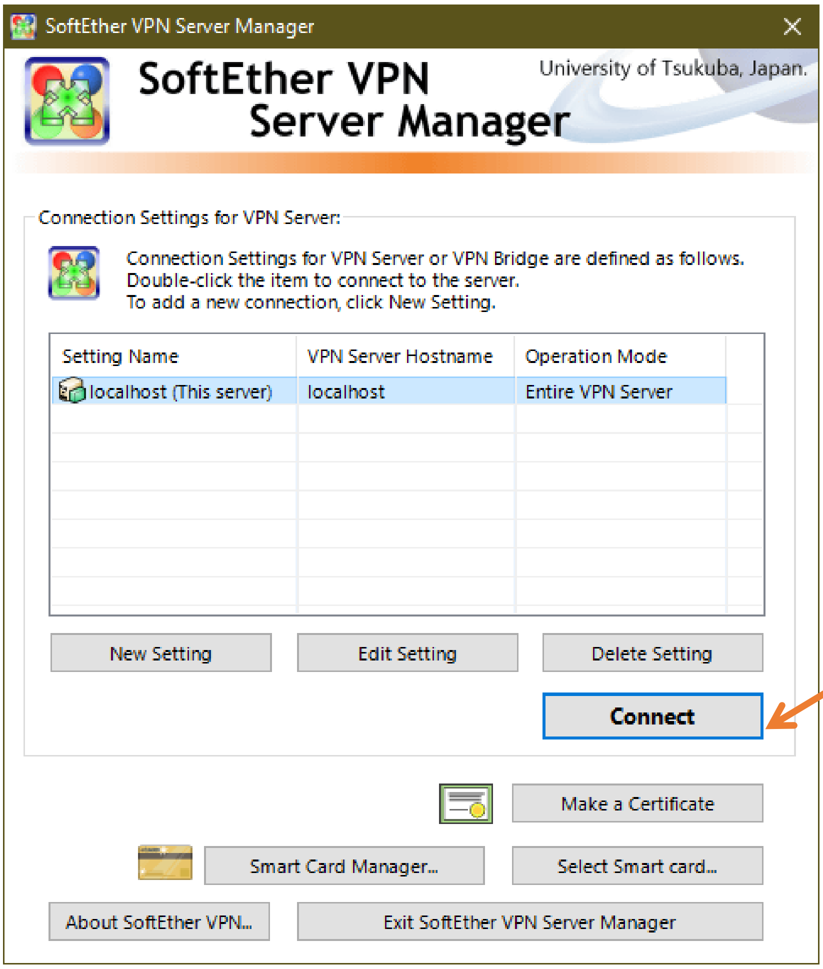
Create New User



SoftEther VPN Server Manager

SoftEther VPN Server Manager

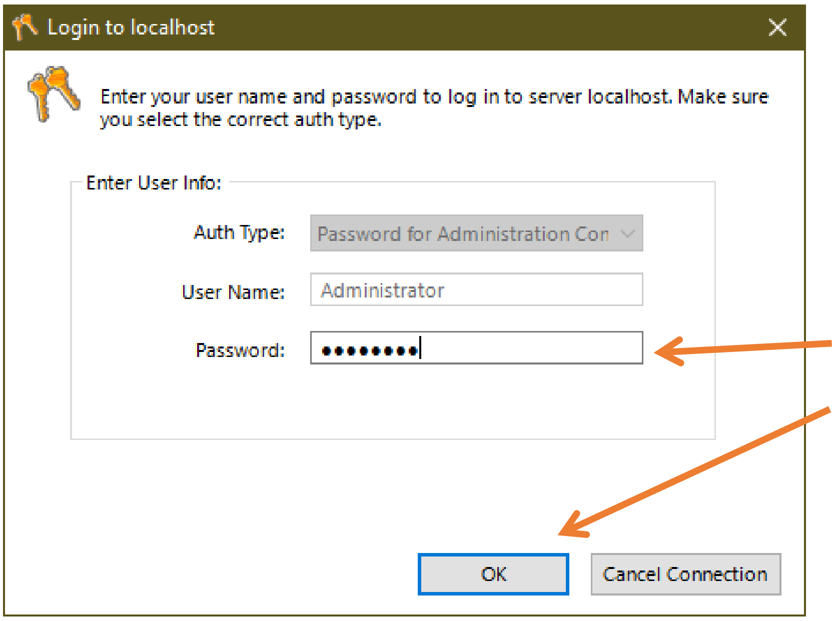
University of Tsukuba, Japan.

Connection Settings for VPN Server:

Connection Settings for VPN Server or VPN Bridge are defined as follows.
Double-click the item to connect to the server.
To add a new connection, click New Setting.

Setting Name	VPN Server Hostname	Operation Mode
localhost (This server)	localhost	Entire VPN Server

Click Connect



Login to localhost

Enter your user name and password to log in to server localhost. Make sure you select the correct auth type.

Enter User Info:

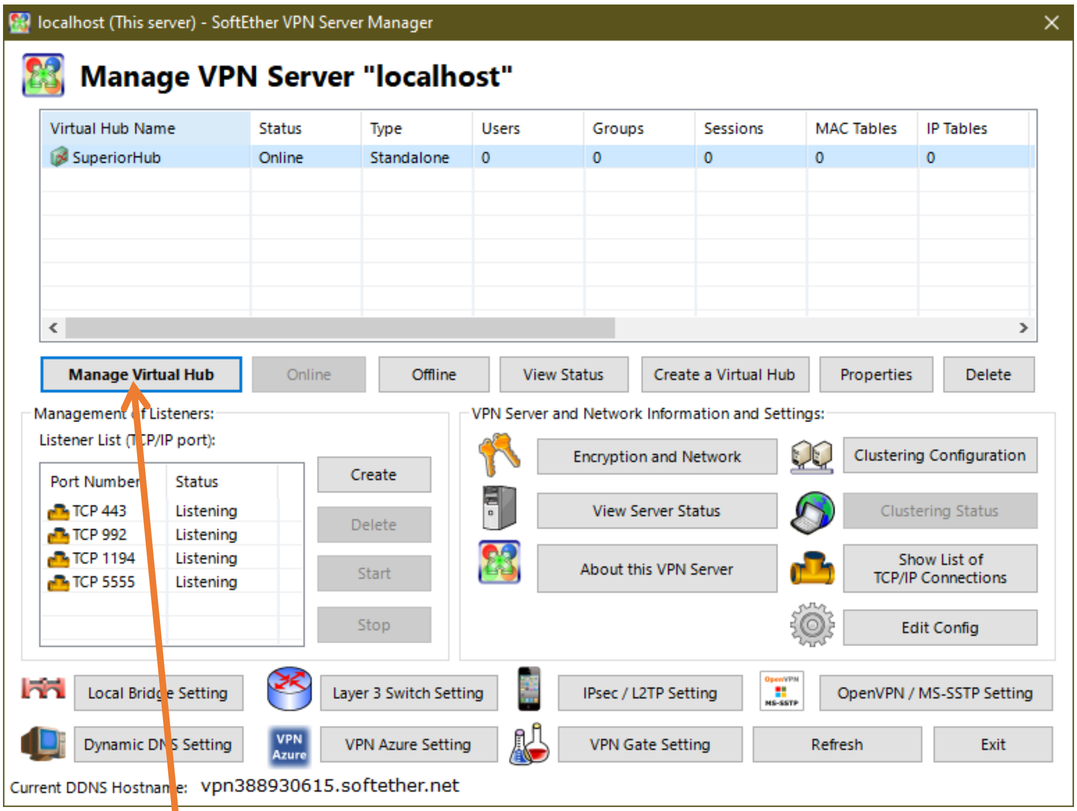
Auth Type: Password for Administration Con

User Name: Administrator

Password: ••••••••

Key in Password and click OK

Default is : superior


localhost (This server) - SoftEther VPN Server Manager

Manage VPN Server "localhost"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
SuperiorHub	Online	Standalone	0	0	0	0	0

Management of Listeners:

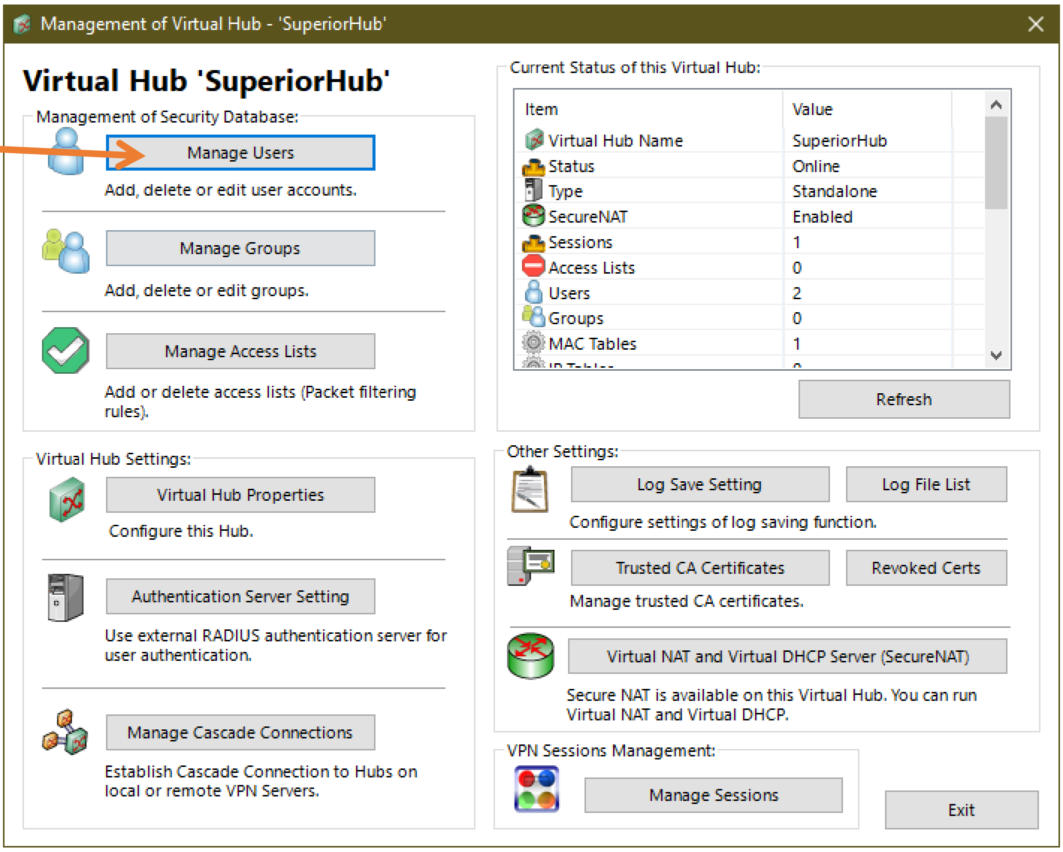
Listener List (TCP/IP port):

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening
TCP 5555	Listening

VPN Server and Network Information and Settings:

Current DDNS Hostname: vpn388930615.softether.net

Click “Manage Virtual Hub”


Management of Virtual Hub - 'SuperiorHub'

Virtual Hub 'SuperiorHub'

Management of Security Database:

Add, delete or edit user accounts.

Add, delete or edit groups.

Add or delete access lists (Packet filtering rules).

Virtual Hub Settings:

Configure this Hub.

Use external RADIUS authentication server for user authentication.

Establish Cascade Connection to Hubs on local or remote VPN Servers.

Current Status of this Virtual Hub:

Item	Value
Virtual Hub Name	SuperiorHub
Status	Online
Type	Standalone
SecureNAT	Enabled
Sessions	1
Access Lists	0
Users	2
Groups	0
MAC Tables	1

Other Settings:

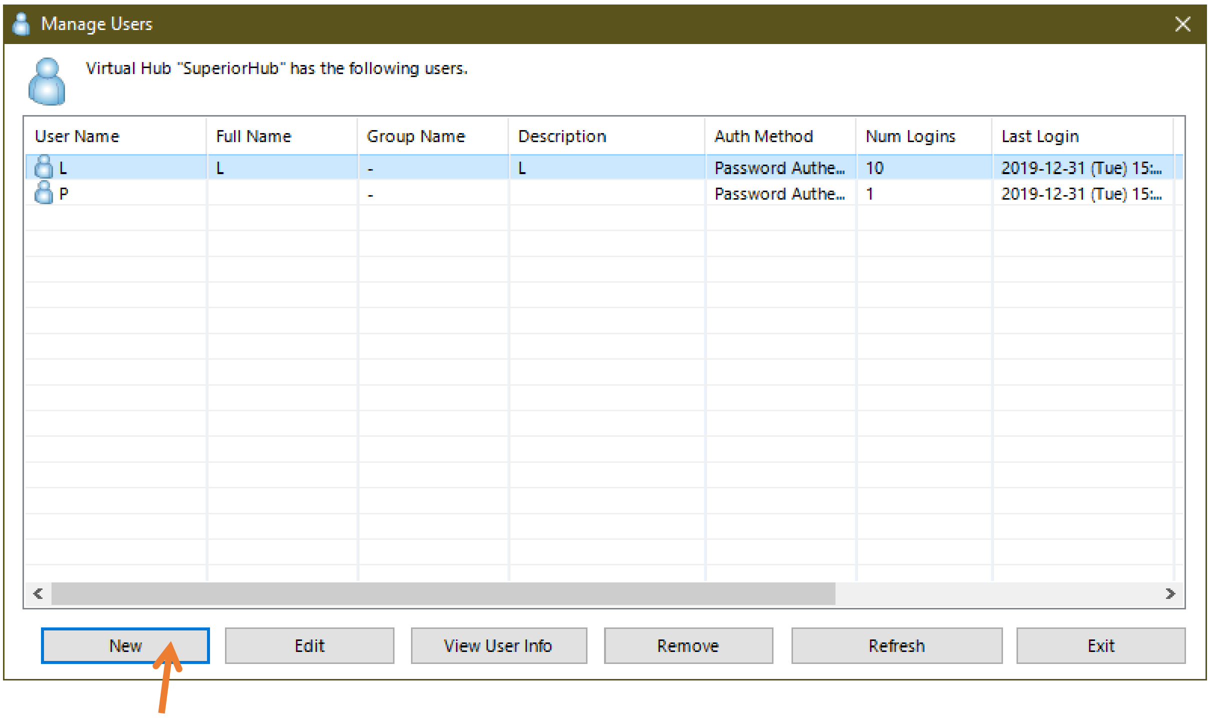
Configure settings of log saving function.

Manage trusted CA certificates.

Secure NAT is available on this Virtual Hub. You can run Virtual NAT and Virtual DHCP.

VPN Sessions Management:

Click “Manage Users”



Manage Users

Virtual Hub "SuperiorHub" has the following users.

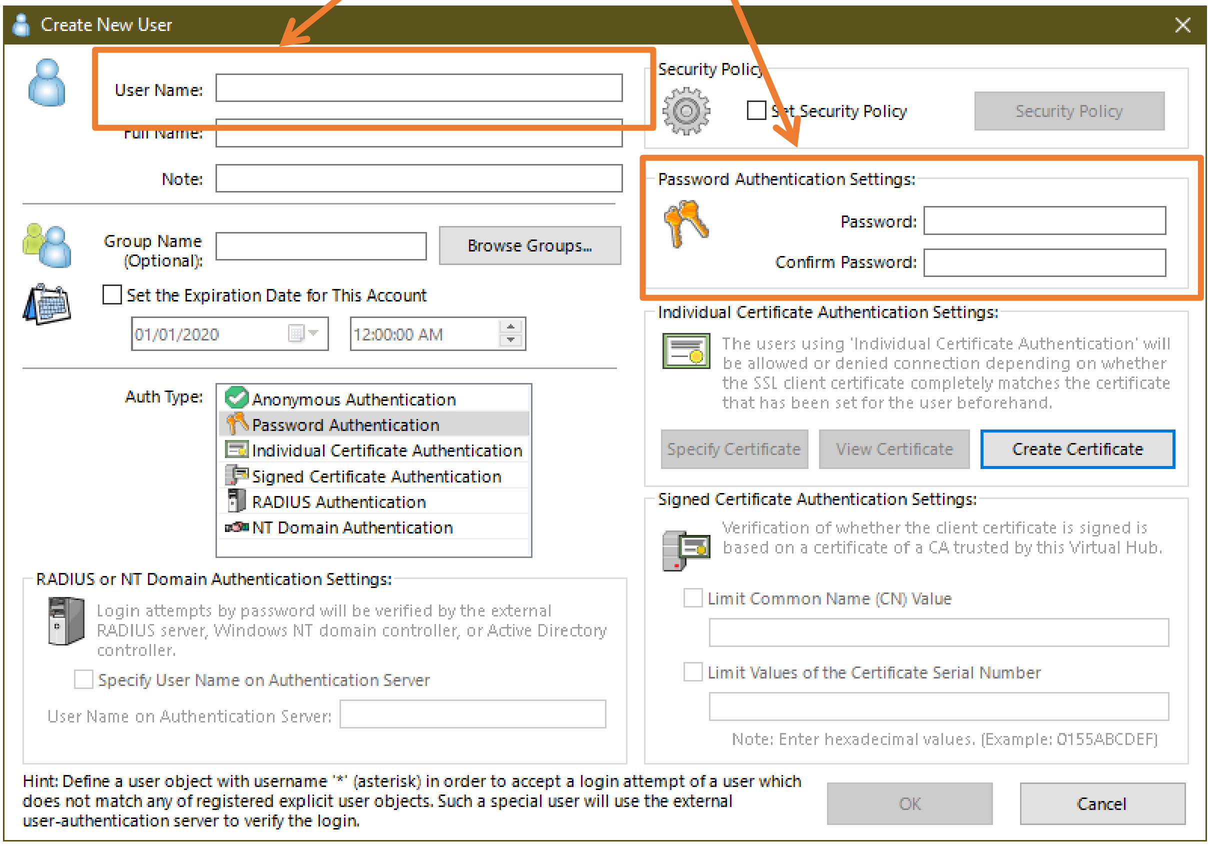
User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login
L	L	-	L	Password Authe...	10	2019-12-31 (Tue) 15:...
P		-		Password Authe...	1	2019-12-31 (Tue) 15:...

Click New

Key in “User Name” and “Password”

Recommend Password : {fullname}{first 6 digit of IC}{.}

* Use complex password to increase security



Create New User

User Name:

Full Name:

Note:

Group Name (Optional):

□ Set the Expiration Date for This Account

01/01/2020 12:00:00 AM

Auth Type:
- Anonymous Authentication
- Password Authentication
- Individual Certificate Authentication
- Signed Certificate Authentication
- RADIUS Authentication
- NT Domain Authentication

RADIUS or NT Domain Authentication Settings:

Login attempts by password will be verified by the external RADIUS server, Windows NT domain controller, or Active Directory controller.

□ Specify User Name on Authentication Server

User Name on Authentication Server:

Security Policy

□ Set Security Policy

Password Authentication Settings:

Password:

Confirm Password:

Individual Certificate Authentication Settings:

The users using 'Individual Certificate Authentication' will be allowed or denied connection depending on whether the SSL client certificate completely matches the certificate that has been set for the user beforehand.

Signed Certificate Authentication Settings:

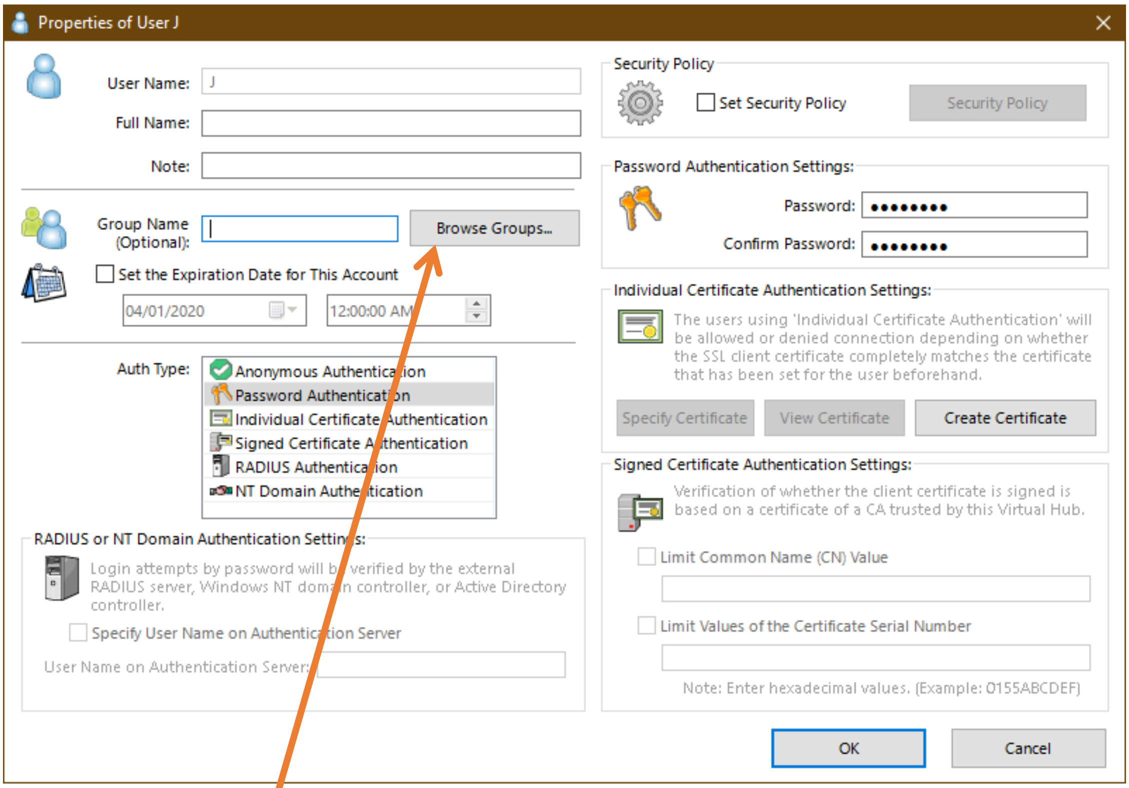
Verification of whether the client certificate is signed is based on a certificate of a CA trusted by this Virtual Hub.

□ Limit Common Name (CN) Value

□ Limit Values of the Certificate Serial Number

Note: Enter hexadecimal values. (Example: 0155ABCDEF)

Hint: Define a user object with username '*' (asterisk) in order to accept a login attempt of a user which does not match any of registered explicit user objects. Such a special user will use the external user-authentication server to verify the login.



Properties of User J

User Name: J

Full Name:

Note:

Group Name (Optional):

☐ Set the Expiration Date for This Account

04/01/2020 12:00:00 AM

Auth Type:

- Anonymous Authentication
- Password Authentication
- Individual Certificate Authentication
- Signed Certificate Authentication
- RADIUS Authentication
- NT Domain Authentication

RADIUS or NT Domain Authentication Settings:

Login attempts by password will be verified by the external RADIUS server, Windows NT domain controller, or Active Directory controller.

☐ Specify User Name on Authentication Server

User Name on Authentication Server:

Security Policy

☐ Set Security Policy

Password Authentication Settings:

Password: ••••••••

Confirm Password: ••••••••

Individual Certificate Authentication Settings:

The users using 'Individual Certificate Authentication' will be allowed or denied connection depending on whether the SSL client certificate completely matches the certificate that has been set for the user beforehand.

Signed Certificate Authentication Settings:

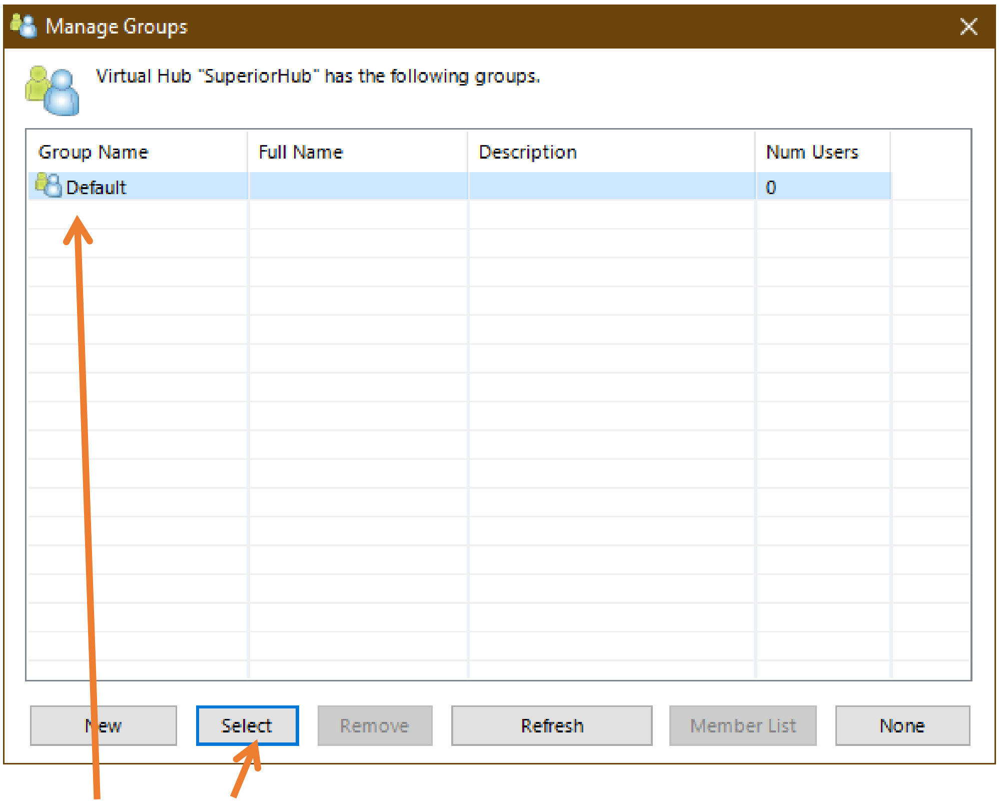
Verification of whether the client certificate is signed is based on a certificate of a CA trusted by this Virtual Hub.

☐ Limit Common Name (CN) Value

☐ Limit Values of the Certificate Serial Number

Note: Enter hexadecimal values. (Example: 0155ABCDEF)

Click “Browse Groups”

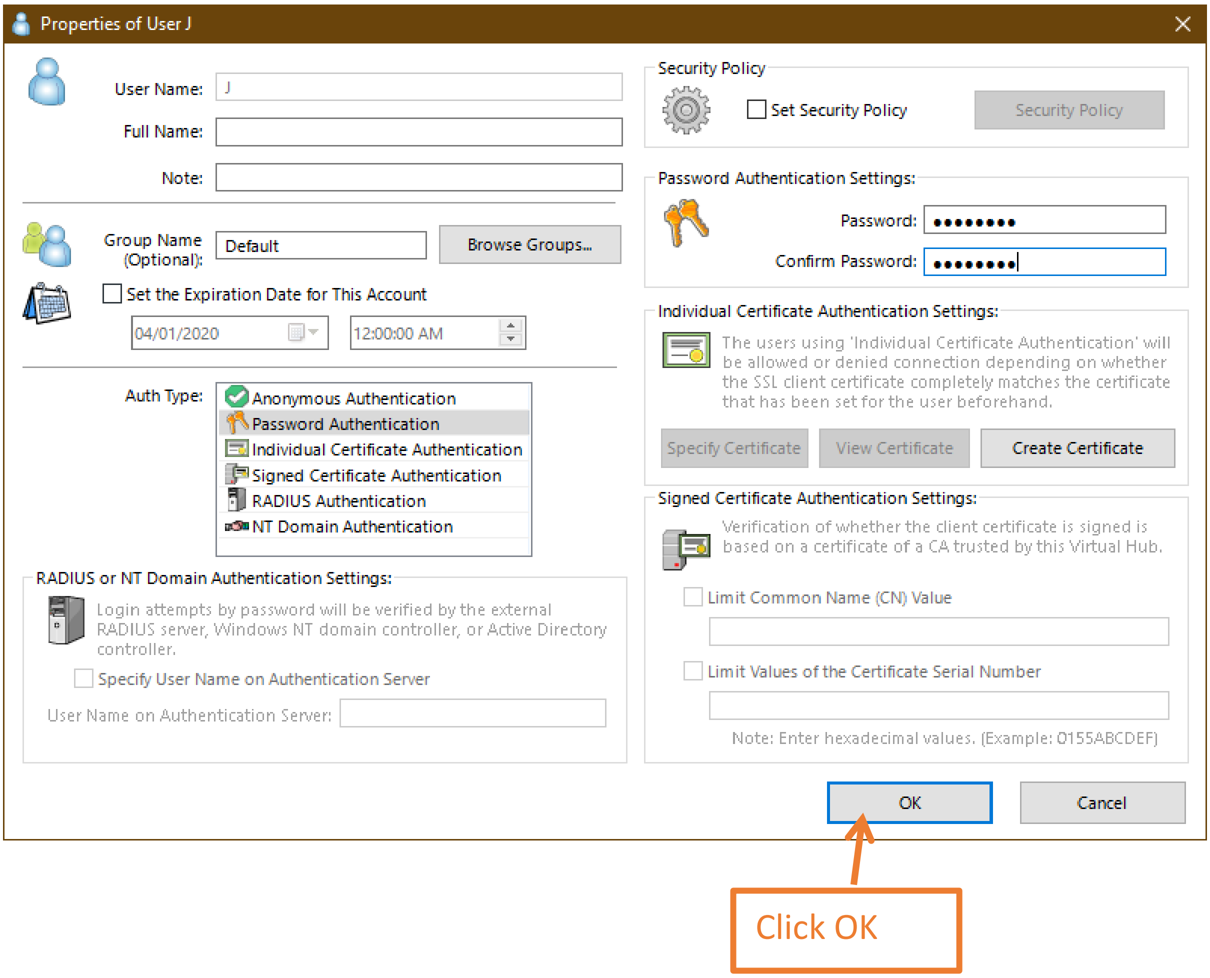


Manage Groups

Virtual Hub "SuperiorHub" has the following groups.

Group Name	Full Name	Description	Num Users
Default			0

Select Default and click “Select”



Properties of User J

User Name: J

Full Name:

Note:

Group Name (Optional): Default

Browse Groups...

□ Set the Expiration Date for This Account

04/01/2020 12:00:00 AM

Auth Type:

- Anonymous Authentication
- Password Authentication
- Individual Certificate Authentication
- Signed Certificate Authentication
- RADIUS Authentication
- NT Domain Authentication

RADIUS or NT Domain Authentication Settings:

Login attempts by password will be verified by the external RADIUS server, Windows NT domain controller, or Active Directory controller.

□ Specify User Name on Authentication Server

User Name on Authentication Server:

Security Policy

□ Set Security Policy

Security Policy

Password Authentication Settings:

Password: ••••••••

Confirm Password: ••••••••

Individual Certificate Authentication Settings:

The users using 'Individual Certificate Authentication' will be allowed or denied connection depending on whether the SSL client certificate completely matches the certificate that has been set for the user beforehand.

Specify Certificate | View Certificate | Create Certificate

Signed Certificate Authentication Settings:

Verification of whether the client certificate is signed is based on a certificate of a CA trusted by this Virtual Hub.

□ Limit Common Name (CN) Value

□ Limit Values of the Certificate Serial Number

Note: Enter hexadecimal values. (Example: 0155ABCDEF)

OK | Cancel

Click OK