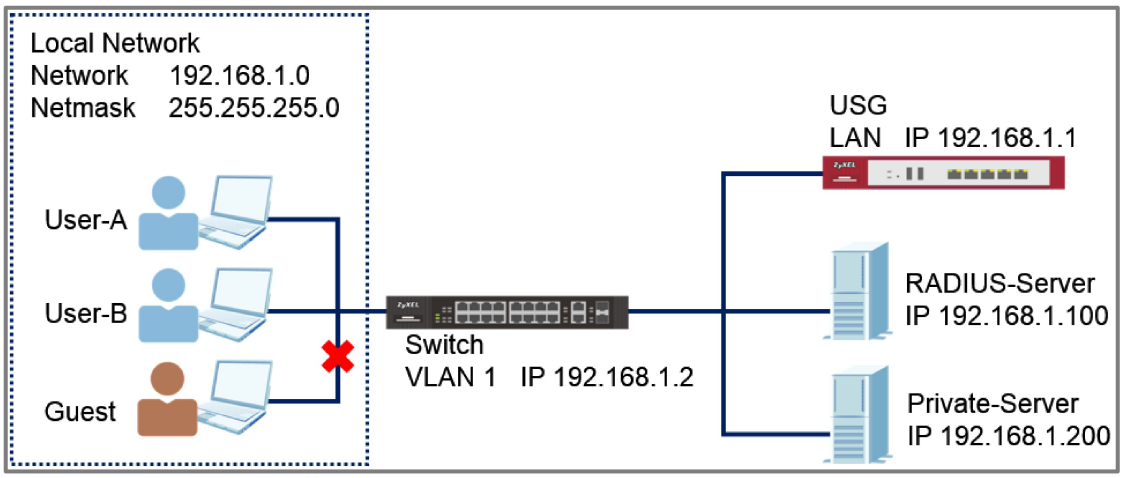
5.4 How to Configure the Switch and RADIUS Server to Provide Network Access through 802.1x Port Authentication

This example will instruct the administrator on how to configure the switch to provide access to machines that provides valid user credentials. With 802.1x Port Authentication, the organization can ensure that only authorized personnel can access core network resources.



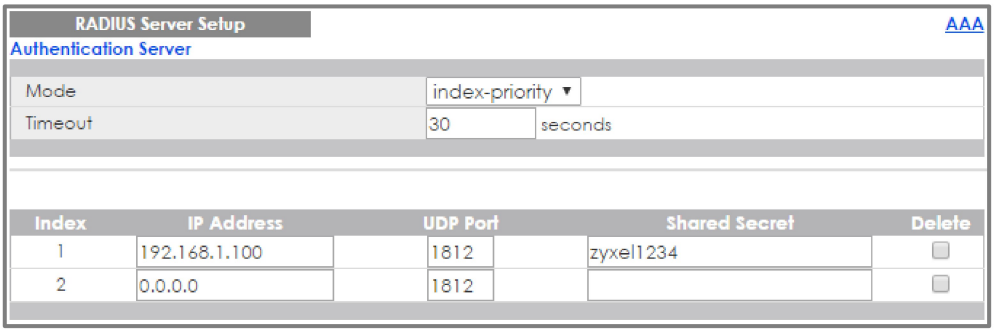
802.1x Port Authentication Providing Access to Authorized Users

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. The authentication server used in this example is FreeRADIUS running in Ubuntu server.
All UI displayed in this article are taken from the XGS4600 series switch.

5.4.1 Configuration in the Switch

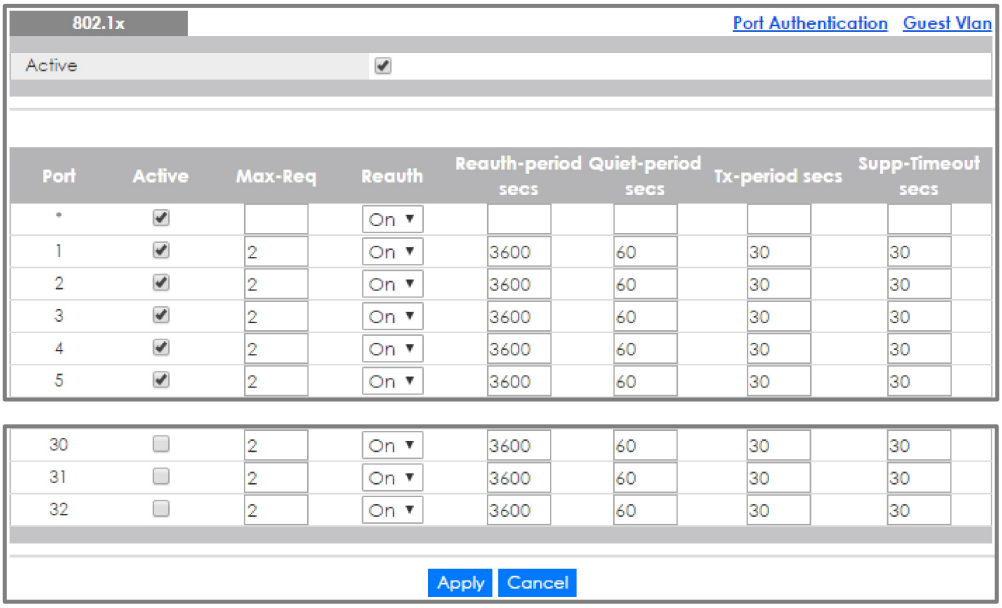
1 Access the **Switch**'s Web GUI.

2 Go to **Advance Application > AAA > RADIUS Server Setup**. Configure the RADIUS server's IP address and set the shared secret. Click **Apply**.



Note:
The shared secret must match the secret of your RADIUS server's client profile.

3 Go to **Advance Application > Port Authentication > 802.1x**. Check the 802.1x Active box as well as for all ports connected to end devices. Do not check active box of ports connected to either the **USG**, **RADIUS-Server**, or **Private-Server**.



802.1x

Port Authentication Guest Vlan

Active ☑

Port	Active	Max-Req	Reauth	Reauth-period secs	Quiet-period secs	Tx-period secs	Supp-Timeout secs
*	☑		On				
1	☑	2	On	3600	60	30	30
2	☑	2	On	3600	60	30	30
3	☑	2	On	3600	60	30	30
4	☑	2	On	3600	60	30	30
5	☑	2	On	3600	60	30	30
30	☐	2	On	3600	60	30	30
31	☐	2	On	3600	60	30	30
32	☐	2	On	3600	60	30	30

Apply Cancel

5.4.2 Configuration in the RADIUS-Server

1 Edit the client profile in **/etc/freeradius/clients.conf**. Save the file and exit.

```
client 192.168.1.2 {
        secret = zyxel1234
        shortname = Switch
        nastype = other
}
```

Note:
The client IP address and secret must match the management IP and shared secret of the Switch.

2 Add the following user profiles in **/etc/freeradius/users**. Save the file and exit.

```
User-A  Cleartext-Password := "zyxeluserA"
        Service-Type = Administrative-User

User-B  Cleartext-Password := "zyxeluserB"
        Service-Type = Administrative-User
```

3 Restart FreeRADIUS service.

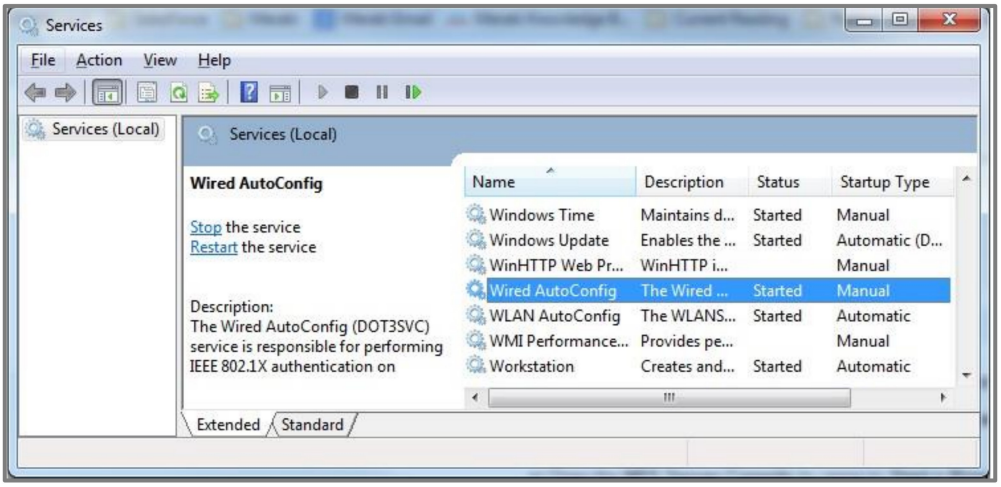
```
root@dhcppc68:/etc/freeradius# stop freeradius
stop: Unknown instance:
root@dhcppc68:/etc/freeradius# start freeradius
freeradius start/running, process 8800
root@dhcppc68:/etc/freeradius#
```

5.4.3 Test the Result

1 Access **User-A**, **User-B**, and **Guest** device.

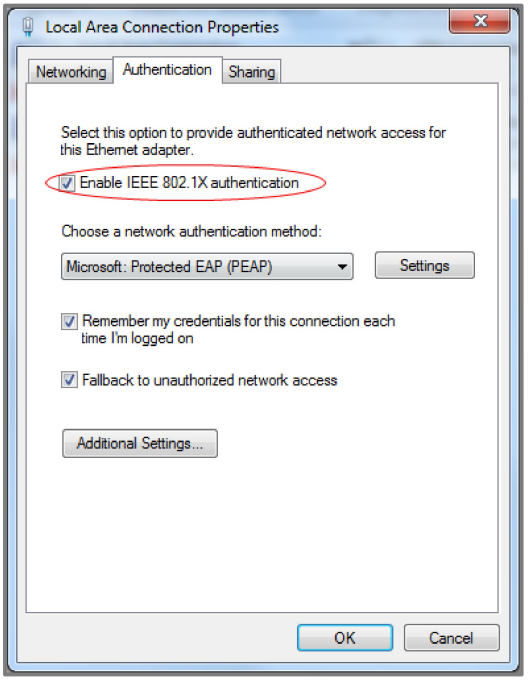
2 If using Windows OS, click the **Start button** and type **services.msc** into the search box.

3 In the Services window, locate the service named **Wired AutoConfig**. Make sure the service status is "**Started**".

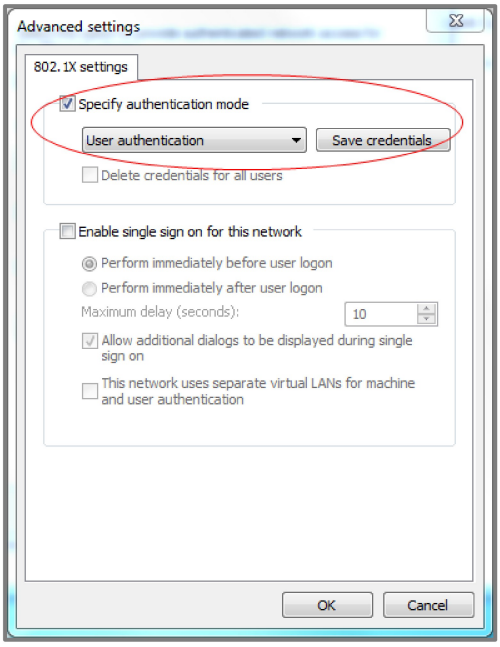


4 Right-click on your network adapter and select **Properties**.

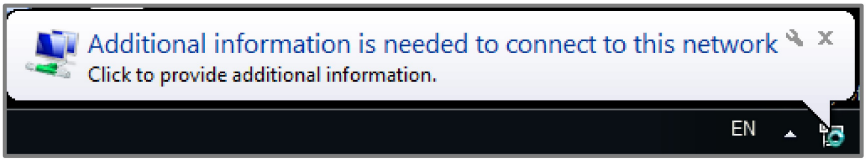
5 Click on the Authentication tab and check "**Enable IEEE 802.1X authentication**". Make sure that the network authentication method is **Microsoft: Protected EAP (PEAP)**



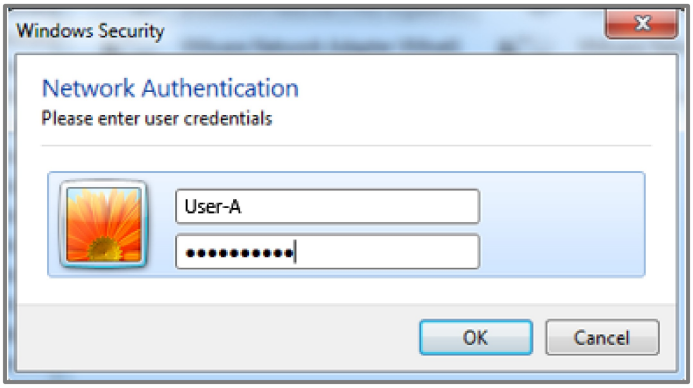
6 Click on **Additional Settings**, select **Specify authentication mode** and specify **User authentication**.



7 Connect User-A device to the **Switch**. User-A should show an "**Additional information is needed to connect to this network.**" pop-up message.



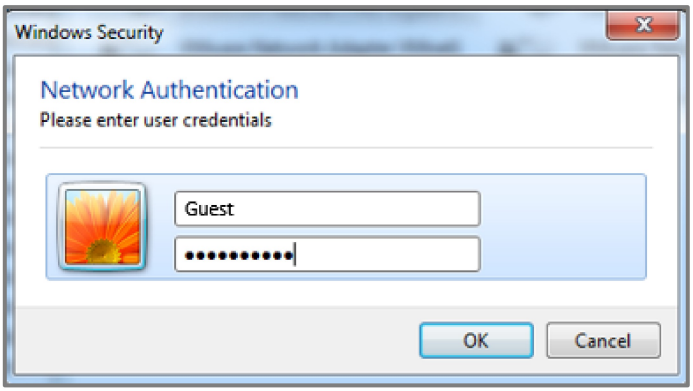
8 Enter the username (**User-A**) and password (**zyxeluserA**) which must be consistent with the RADIUS-Server's user profile settings.



9 Devices using User-A and User-B credentials can communicate with **USG** and **Private-Server**.

10 Connect User-A device to the **Switch**. User-A should show an "**Additional information is needed to connect to this network.**" pop-up message.

11 Enter the username (**Guest**) and a random password.



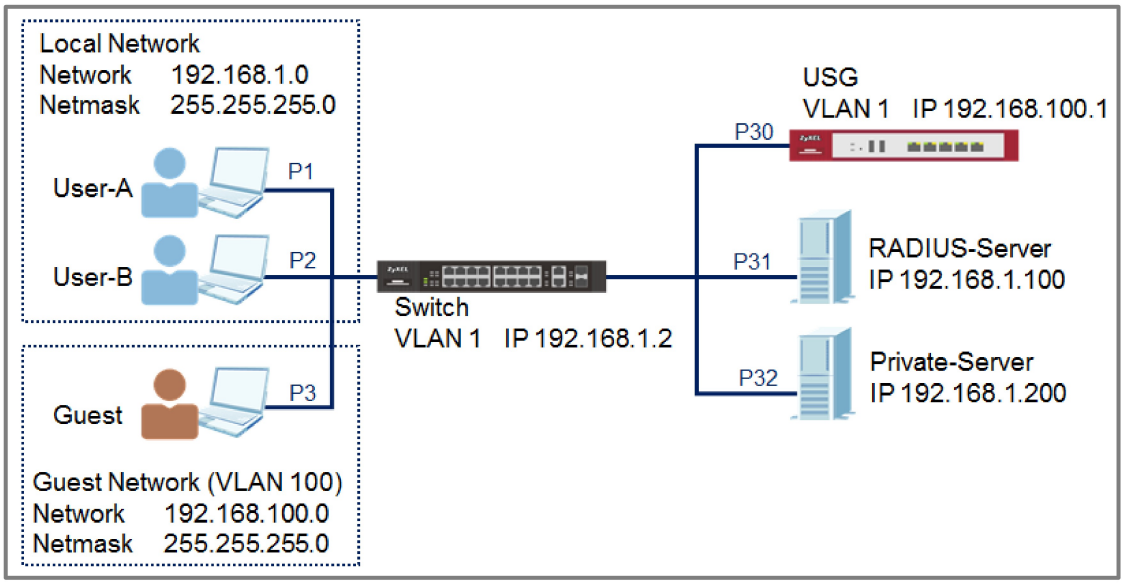
12 Device using Guest credentials cannot communicate with **USG** and **Private-Server**.

5.4.4 What May Go Wrong?

1 If the Switch does not allow access to users that submitted the correct credentials, the following problems may have occurred:
   a. Usernames and passwords are case-sensitive. Make sure that the user input the correct lower-case or upper-case characters.
   b. The RADIUS-server is unreachable. The Switch should be able to ping the RADIUS-Server at all times. Make sure network settings were configured correctly between Switch and RADIUS-Server.
   c. The shared secret between the Switch and RADIUS-Server is not identical.

5.5 How to configure the switch to send unauthorized users in a guest VLAN

The example shows administrators how to use Guest VLAN for users that fails or used an invalid user credential during 802.1x port authentication. In a real application, we may need to allow guests to access the USG so that they can access the Internet, but still isolated from Private-Server. On the contrary, we have to allow the users with valid credentials to only access the Private-Server.



Configure the switch to send unauthorized user in Guest VLAN

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using XGS4600-32 (Firmware Version: V4.50).

5.5.1 Configure 802.1x Port Authentication on the Switch

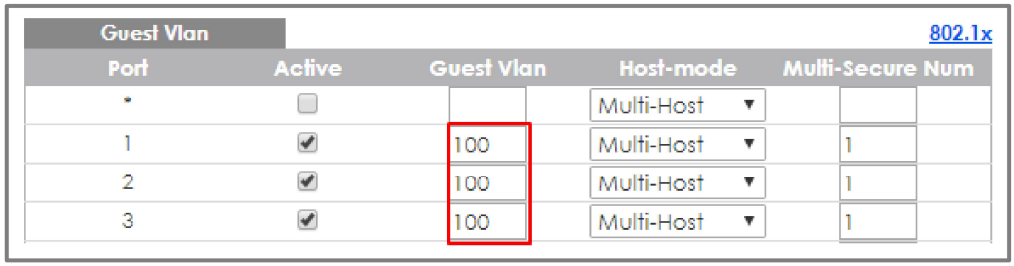
1 Configure 802.1x on all towards users. Do not enable Port Authentication on ports to the USG, RADIUS-Server, and Private-Server. To configure Port Authentication, please refer to the topic: **5.4 How to Configure the Switch and RADIUS Server to Provide Network Access through 802.1x Port Authentication.**

5.5.2 Configure VLAN for Guest VLAN

1 Configure the VLAN for Guest VLAN (**VLAN 100**) on Switch. **VLAN 100**: Set fixed port: 1, 2, 3, 30; untagged port: 1, 2, 3, 30; forbidden port: 31, 32; port 30: pvid=100. **VLAN 1**: Set forbidden port: 30. For isolating VLAN 1 and 100, please refer to the topic: **2.1 How to configure the switch to separate traffic between departments**.

5.5.3 Configure Guest VLAN for Failed Authentication

1 Go to **Menu > Advanced Application > Port Authentication > 802.1x > Guest Vlan**. Activate the Guest Vlan on port 1-3 and type the guest Vlan as **100**. Press "Apply".



5.5.4 Configure the RadiusServer

1 Edit the client profile in **/etc/freeradius/clients.conf**. Save the file and exit.

```
client 192.168.1.1 {
        secret = thisisasecret
        shortname = Switch
        nastype = other
}
```

Note:
The client IP address and secret must match the management IP and shared secret of the Switch.

2 Add the following user profiles in **/etc/freeradius/users**. Save the file and exit.

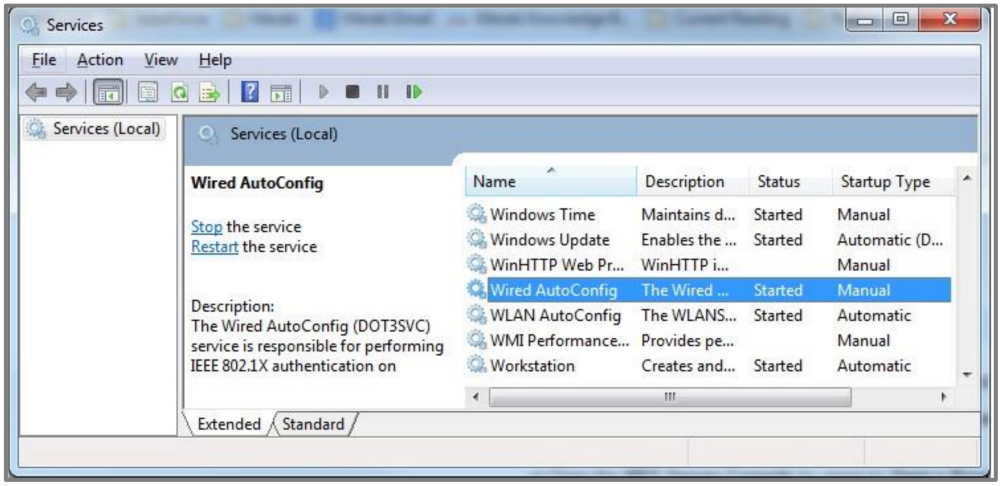
```
user  Cleartest-Password :="user1234"
      Service-Type = Administrative-User
```

3 Restart FreeRADIUS service.

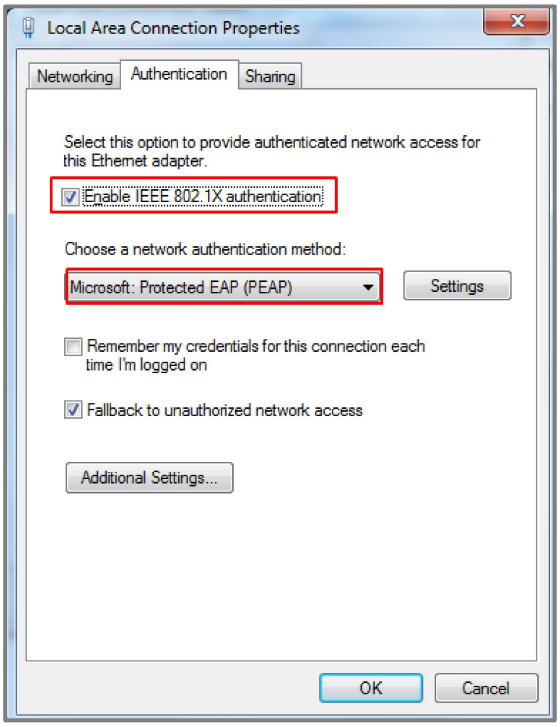
```
root@dhcppc68:/etc/freeradius# stop freeradius
stop: Unknown instance:
root@dhcppc68:/etc/freeradius# start freeradius
freeradius start/running, process 8800
```

5.5.5 Configure the setting on User-A, User-B and Guest

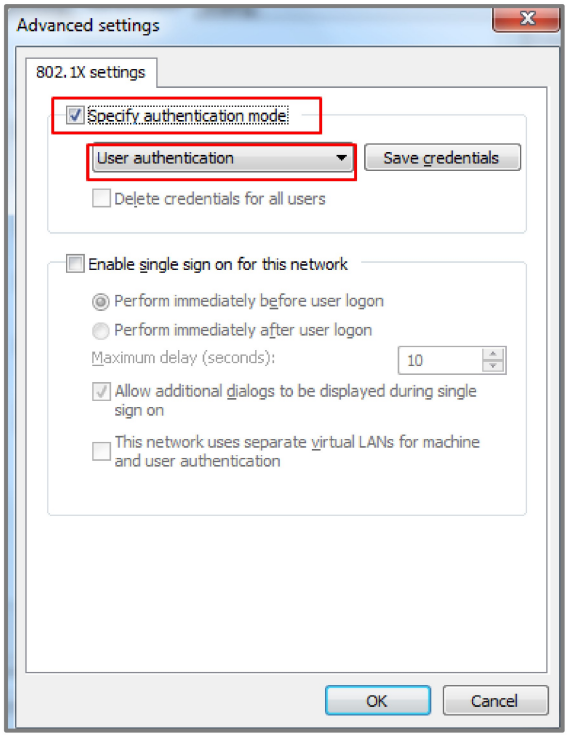
1 In the **Services** window, locate the service named **Wired AutoConfig**. Make sure the service status is "Started".



2 Right-click on your network adapter and select **Properties**. Click on the Authentication tab and check "**Enable IEEE 802.1X authentication**". Make sure that the network authentication method is "**Microsoft: Protected EAP (PEAP)**".

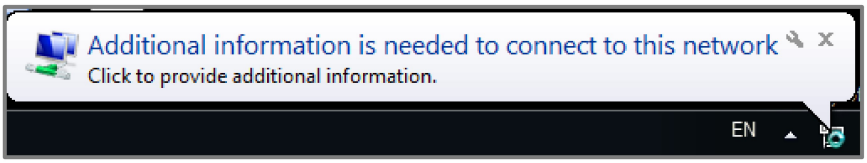


3 Click on **Additional Settings**, select **Specify authentication mode** and specify **User authentication**.

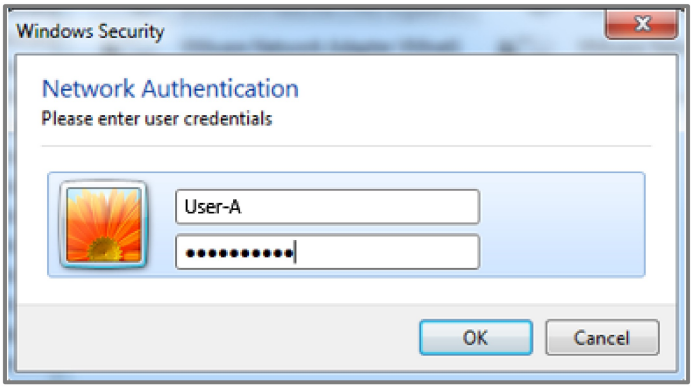


5.5.6 Test the Result

1 Disconnect and connect the PC with Switch. PC should show an "**Additional information is needed to connect to this network**." pop-up message.



2 Enter the username (**User-A**) and password (**zyxeluserA**) which must be consistent with the RADIUS-Server's user profile settings.



3 Devices using User-A and User-B credentials can communicate with Private-Server.

4 Connect User-A device to the Switch. User-A should show an "**Additional information is needed to connect to this network.**" pop-up message.

5 Enter the username (Guest) and a random password.

6 Device using Guest credentials cannot communicate with Private-Server, but it can communicate with USG.

7 Check the MAC table of the Switch. The device of users with wrong credentials are assigned to VLAN 100. (**Menu > Management > MAC Table > Search**)

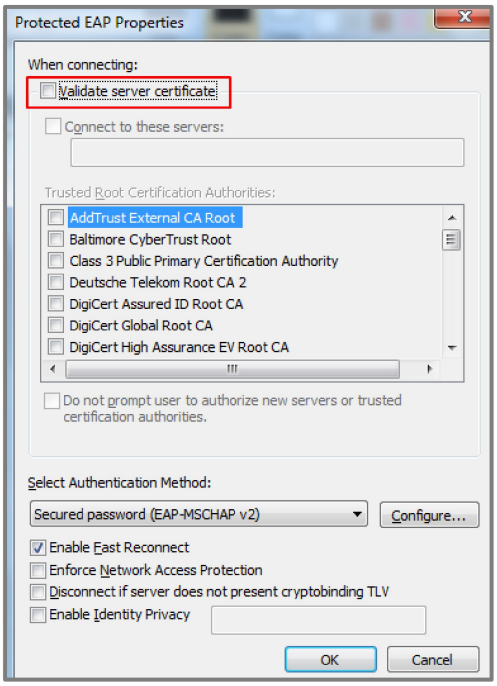
Index	MAC Address	VID	Port	Type
1	00:1e:33:27:04:93	100	3	Dynamic
2	20:6a:8a:39:fe:a9	1	12	Dynamic
3	3c:97:0e:30:0e:b8	1	12	Dynamic
4	42:73:74:20:55:56	1	CPU	Static
5	42:73:74:20:55:56	100	CPU	Static
6	60:31:97:71:6d:15	1	12	Dynamic
7	60:31:97:71:6d:21	1	12	Dynamic
8	74:d4:35:f4:6b:4e	1	12	Dynamic
9	84:ef:18:95:08:e4	1	12	Dynamic
10	a0:8c:fd:1c:c0:b1	1	12	Dynamic
11	b8:ec:a3:0f:cf:9f	1	12	Dynamic
12	c8:6c:87:9f:51:f0	1	12	Dynamic
13	f0:de:f1:91:74:f8	100	1	Dynamic
14	fc:3f:db:39:66:80	1	12	Dynamic

5.5.7 What Could Go Wrong

1 If the PC doesn't pop up the authentication message after connecting the PC to the switch:

a. Try to use the Switch to ping Radius-Server. The Switch should be able to ping Radius-Server.

b. Right-click on your network adapter and select **Properties > Authentication > Additional settings**. Uncheck the "**Validate server certificate**".



2 If the shared secret setting of Switch and PC does **NOT** match, the authentication will fail.

3 If the authentication is fine, but the PC cannot ping Server, please check 801.1X Port Authentication configurations. Do **NOT** activate the authentication on the uplink port (port 2, 3, and 12).

4 If devices sent to the Guest VLAN cannot reach the USG, make sure that the switch has created and configured the Guest VLAN in **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**.