



Information Leaflet

April 15th, 2024

User information about the introduction of Network Access Control at the University of Zürich

The University of Zurich is currently introducing Network Access Control (NAC) for access to its IT network. This information leaflet contains information for users to ensure that your devices with wired access to the wired UZH IT network (laptop- and desktop computers, network printers, lab equipment, etc.) can still connect to the network after the transition to NAC. Please note that devices with WLAN access are not affected.

For the preparation of your devices, the following use cases must be differentiated:

- Your devices were procured by Central IT
- Your devices were procured by the IT coordinator of your organization
- Your devices were procured by yourself

Your devices were procured by Central IT

In this case, nothing needs to be done. Central IT will ensure that your devices can still connect to the network after the transition to NAC.

Your devices were procured by the IT coordinator of your organization

In this case, nothing needs to be done. The IT coordinator of your organization will ensure that your devices can still connect to the network after the transition. In case any problems occur after the transition, please contact the IT coordinator of your organization to resolve the issue.

Your devices were procured by yourself

In case you procured your devices yourself, meaning without involvement of your IT coordinator or Central IT, it is your responsibility to make sure that the devices can connect to the UZH IT network after the transition to NAC. Please ensure the following:

1. «Dynamic Host Configuration Protocol» (DHCP) must be activated on your devices.
2. In case your devices use a user account (username/password) to connect to the UZH IT network, the authentication standard 802.1X must be activated on your devices.
3. In case your devices connect to the UZH Internet of Things (IoT) network without a user account, your device's MAC addresses need to be registered with Central IT.

The following sections contain information how to prepare your Windows10 (see section A), Windows11 (see section B) or MacOS (see section C) devices for the transition to NAC.

Note to IT coordinators

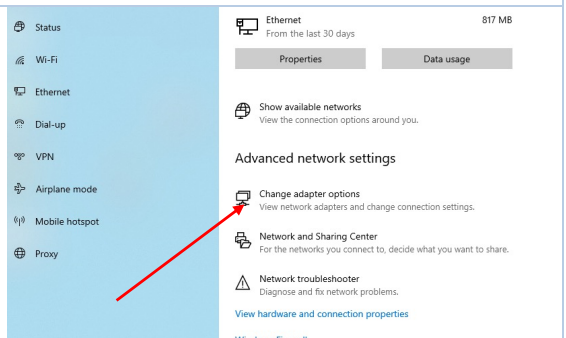
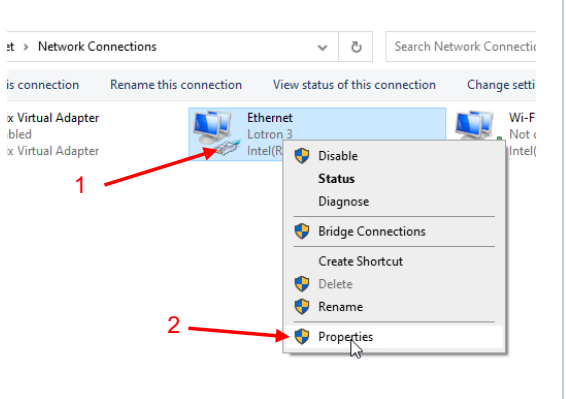


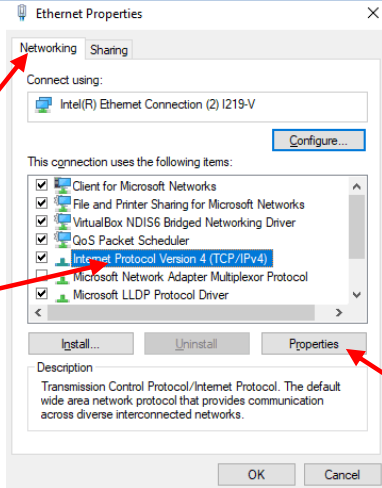
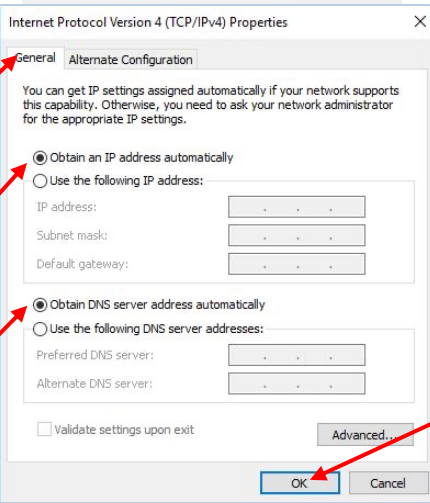
Note that the instructions below are specific to Bring-Your-Own-Devices (BYOD) and cannot be used unchanged for IT coordinators. During the activation of 802.1X, the UZH username and password of the device owner must be entered. In case the IT coordinator's username and password are entered during this step, these credentials will be used whenever the device connects to the UZH network! We therefore recommend making these settings computer-based with Group Policies or similar means.

A. Laptop and desktop computers with Windows10 operating system

Activation of DHCP

To activate DHCP on your Windows10 laptop and desktop computers, the steps below must be performed. Note that depending on your computer's configuration, an administrator password may be necessary.

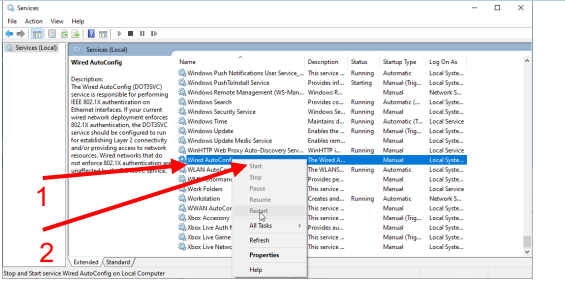
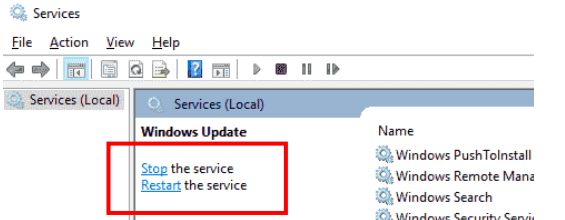
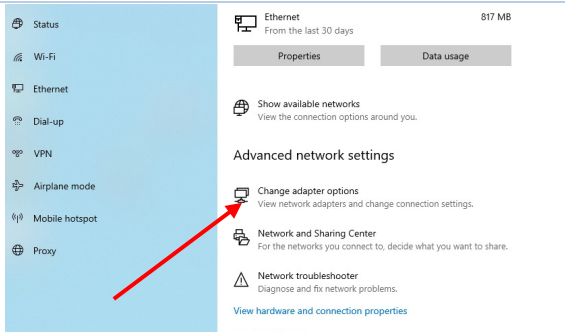
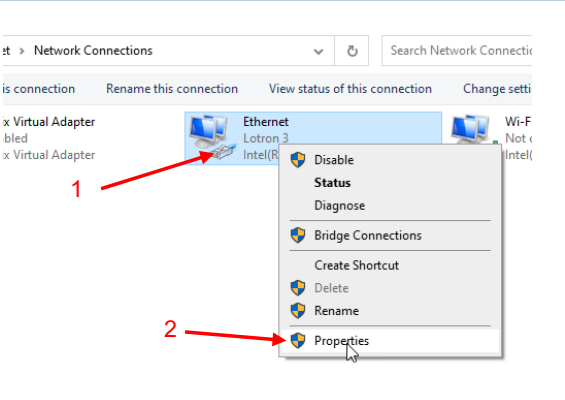
Step	Description	Illustration
1.	Right-click on the Windows symbol and click on «Network Connections».	
2.	Under «Advanced Network Settings», click on «Change adapter options»	
3.	Right-click on «Ethernet» (1) and select «Properties» (2).	

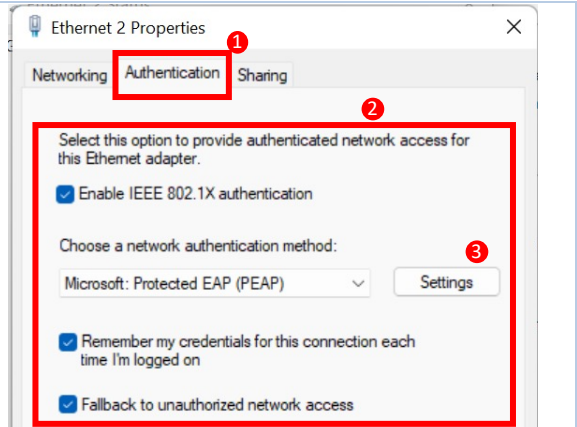
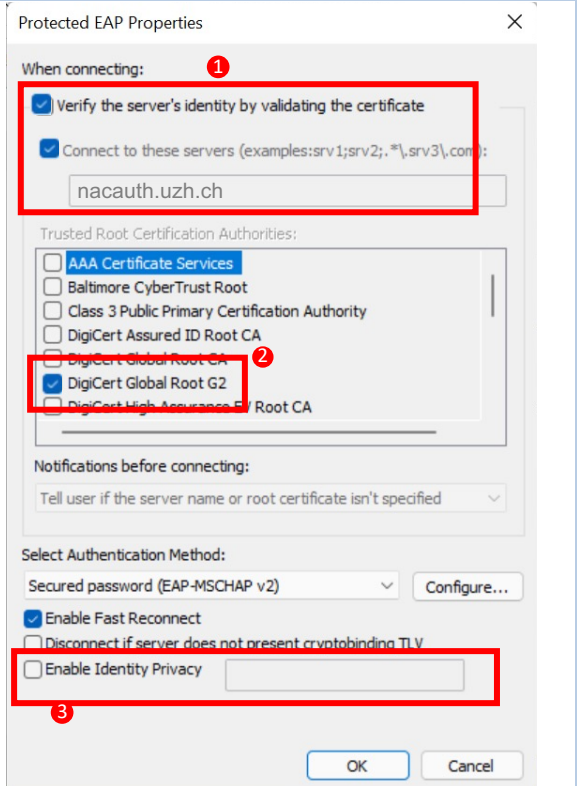
<p>4.</p>	<p>Switch to the tab «Networking» (1), click on «Internet Protocol Version 4 (TCP/IPv4)» (2) and click on «Properties» (3).</p>	
<p>5.</p>	<p>Switch to the tab «General» (1) and activate the options «Obtain an IP address automatically» (2) and «Obtain DNS server address automatically» (3). Click on «OK» (4).</p>	
<p>6.</p>	<p>Restart your computer to activate the changes.</p> <p>Note: In case you must activate 802.1X as well, restart your computer after you have activated 802.1X.</p>	

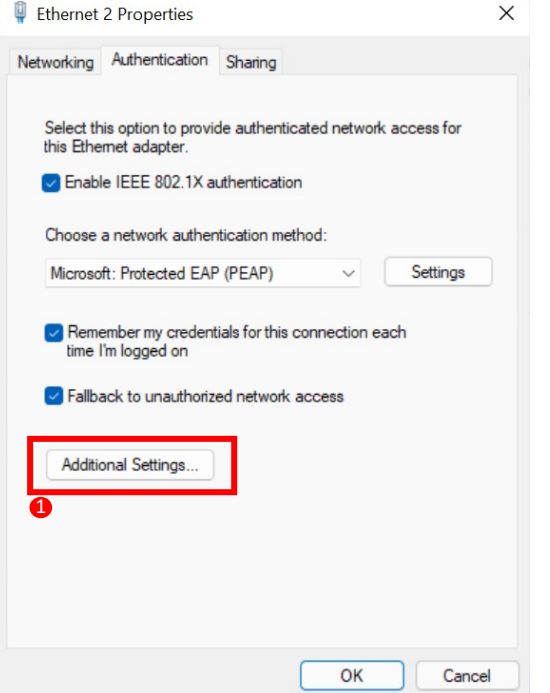
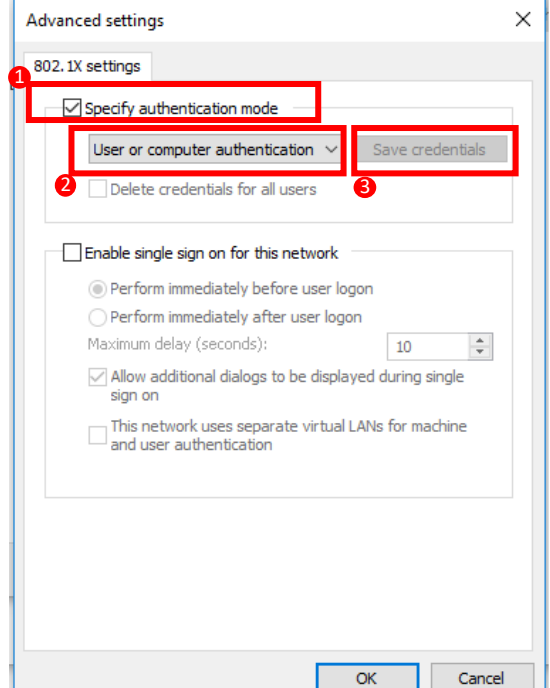
Activation of 802.1X

To activate 802.1X on your Windows 10 laptop and desktop computers, the steps below must be performed. Note that depending on your computer's configuration, an administrator password may be necessary.


Step	Description	Illustration
1.	Open the application «Services».	

<p>2.</p>	<p>Right-click on the service «Wired AutoConfiguration» (1) and select «Start» (2).</p>	
<p>3.</p>	<p>Make sure that the options «Stop the service» and «Restart the service» are visible on the left side of the window.</p>	
<p>4.</p>	<p>Close the window «Services».</p>	
<p>5.</p>	<p>Right-click on the Windows symbol and click on «Network Connections».</p>	
<p>6.</p>	<p>Under «Advanced Network Settings», click on «Change adapter options»</p>	
<p>7.</p>	<p>Right-click on «Ethernet» (1) and select «Properties» (2).</p>	

<p>8.</p>	<p>Switch to the tab «Authentication» (1) and make sure that the settings are identical to the settings in the picture on the right (2). Click on « Settings» (3).</p> <p>Note: In case the tab «Authentication» is not visible, the service was not properly started in step 2, and the steps from step 2 onwards must be repeated.</p>	
<p>9.</p>	<p>Make sure that the options “Verify the server’s identity by validating the certificate” and “Connect to these servers” are activated, and the server is set to “nacauth.uzh.ch” (1).</p> <p>Make sure that under “Trusted Root Certification Authorities”, the option “DigiCert Global Root G2” is activated.</p> <p>Make sure that the option “Enable Identity Privacy” (2) is deactivated.</p> <p>Click “OK”.</p>	

<p>10.</p>	<p>Click on “Additional Settings” (1)</p>	 <p>Ethernet 2 Properties</p> <p>Networking Authentication Sharing</p> <p>Select this option to provide authenticated network access for this Ethernet adapter.</p> <p><input checked="" type="checkbox"/> Enable IEEE 802.1X authentication</p> <p>Choose a network authentication method:</p> <p>Microsoft: Protected EAP (PEAP) Settings</p> <p><input checked="" type="checkbox"/> Remember my credentials for this connection each time I'm logged on</p> <p><input checked="" type="checkbox"/> Fallback to unauthorized network access</p> <p>Additional Settings...</p> <p>OK Cancel</p>
<p>11.</p>	<p>Activate the check box «Specify authentication mode» (1) and select «User or computer authentication» from the drop-down list (2). Click on «Save credentials» (3).</p>	 <p>Advanced settings</p> <p>802.1X settings</p> <p><input checked="" type="checkbox"/> Specify authentication mode</p> <p>User or computer authentication Save credentials</p> <p><input type="checkbox"/> Delete credentials for all users</p> <p><input type="checkbox"/> Enable single sign on for this network</p> <p>Perform immediately before user logon</p> <p>Perform immediately after user logon</p> <p>Maximum delay (seconds): 10</p> <p><input checked="" type="checkbox"/> Allow additional dialogs to be displayed during single sign on</p> <p><input type="checkbox"/> This network uses separate virtual LANs for machine and user authentication</p> <p>OK Cancel</p>



12.	<p>Enter shortname and password of your UZH user account and click «OK».</p> <p>Note: In case you don't know the shortname of your UZH user account, log into the UZH Identity Management (identity.uzh.ch). The shortname is displayed as «User ID» under «Change password» for the entry «Active Directory».</p>	
13.	Restart your computer to activate the changes.	

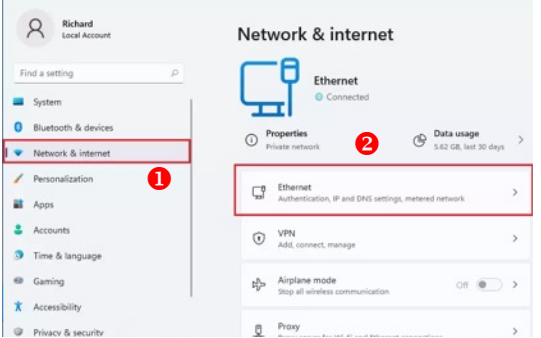
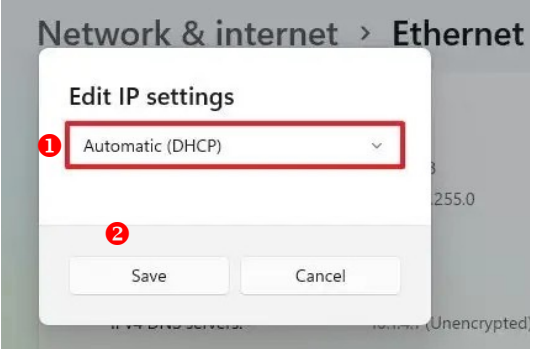
Register the MAC addresses of your devices with Central IT

To register your device's MAC addresses with Central IT, follow the steps described in section 0 at the end of this document.

B. Laptop and desktop computers with Windows11 operating system

Activation of DHCP

To activate DHCP on your Windows11 laptop and desktop computers, the steps below must be performed. Note that depending on your computer's configuration, an administrator password may be necessary.

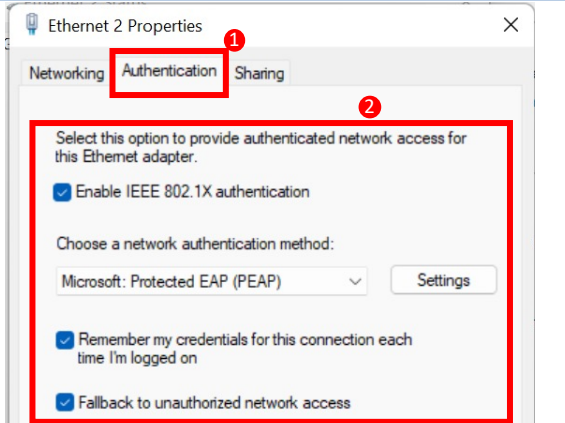
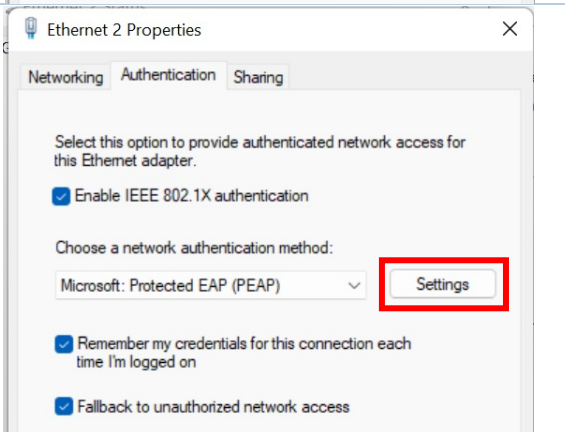
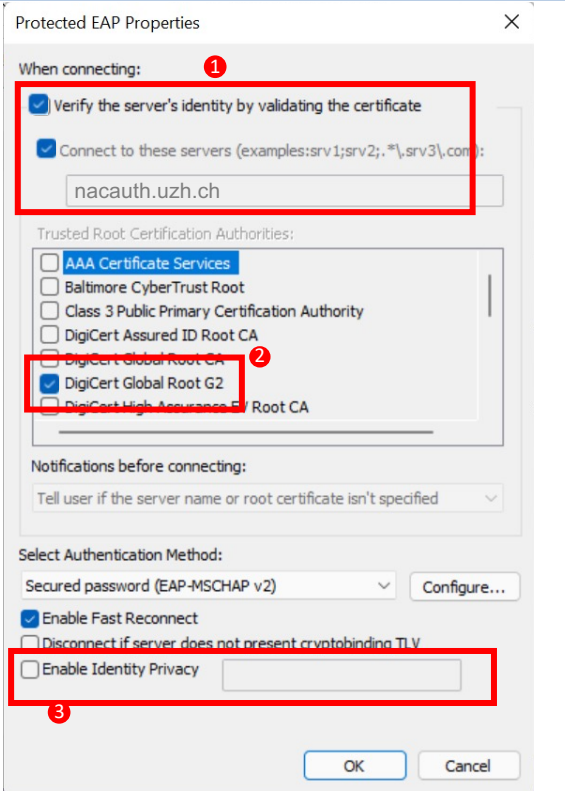
Step	Description	Illustration
1.	Click the Windows key and enter "Settings" in the search field. Select "Settings", "Network & internet" (1), "Ethernet" (2) and then select the UZH ethernet network.	
2.	Scroll down to "IP assignment" and click on "Edit".	
3.	Under "Edit network settings", select "Automatic (DHCP) (1)". Click on "Save" (2).	
4.	Restart your computer to activate the changes. NOTE: In case you must activate 802.1X as well, restart your computer after you have activated 802.1X.	

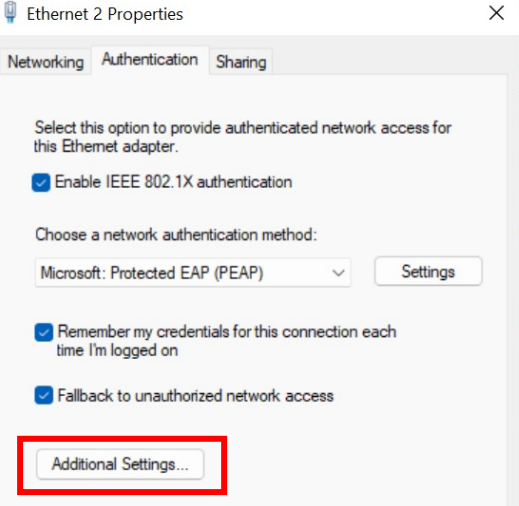
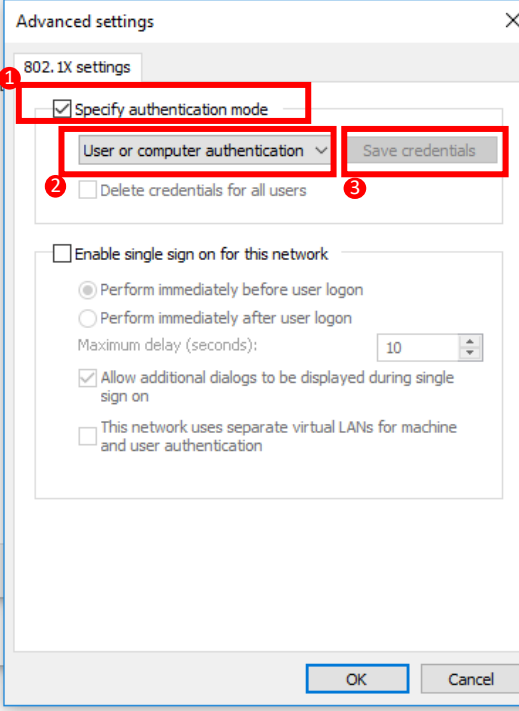
Activation of 802.1X

To activate 802.1X on your Windows 10 laptop and desktop computers, the steps below must be performed. Note that depending on your computer's configuration, an administrator password may be necessary.

Step	Description	Illustration
1.	Press the Windows key and enter "Services" in the search field. Click on "Services".	

<p>2.</p>	<p>Right-click on the service «Wired AutoConfiguration» (1) and select «Start» (2).</p>	
<p>3.</p>	<p>Make sure that the options «Stop the service» and «Restart the service» are visible on the left side of the window.</p>	
<p>4.</p>	<p>Double-click on the service “Wired autoconfiguration” and under “Startup type”, activate “Automatic”.</p>	
<p>5.</p>	<p>Close the window «Services».</p>	
<p>6.</p>	<p>Click the Windows key and enter “Control Panel” in the search field. Click on “Control Panel” and then on “Network and Internet”.</p>	
<p>7.</p>	<p>Click on “Network and Sharing Center”, on the UZH Ethernet-network.</p>	

<p>8.</p> <p>Click on “Properties”, change to the tab “Authentication” (❶), and make sure that your settings are identical to the ones shown in the picture on the right (❷).</p> <p>NOTE: IN case the tab “Authentication” is not visible, the corresponding service was not started correctly in step 2 above. Repeat all steps starting at step 2.</p>		
<p>9.</p>	<p>Under “Choose a network authentication Method:”, click on “Settings”.</p>	
<p>10.</p>	<p>Make sure that the options “Verify the server’s identity by validating the certificate” and “Connect to these servers” are activated, and the server is set to “nacauth.uzh.ch” (❶).</p> <p>Make sure that under “Trusted Root Certification Authorities”, the option “DigiCert Global Root G2” is activated.</p> <p>Make sure that the option “Enable Identity Privacy” (❷) is deactivated.</p> <p>Click “OK”.</p>	

11.	Click on “Additional Settings...”.	
12.	<p>Activate the check box «Specify authentication mode» (1) and select «User authentication» from the drop-down list (2). Click on «Save credentials» (3) and enter your UZH username and password. Click on “OK” and leave all open dialogues by clicking “OK”.</p> <p>NOTE: The UZH username and password that are entered in this step will be used for every future connection to the UZH Ethernet Network. Make sure that you enter username and password of your personal UZH account!</p>	
13.	Restart your computer to activate the changes.	

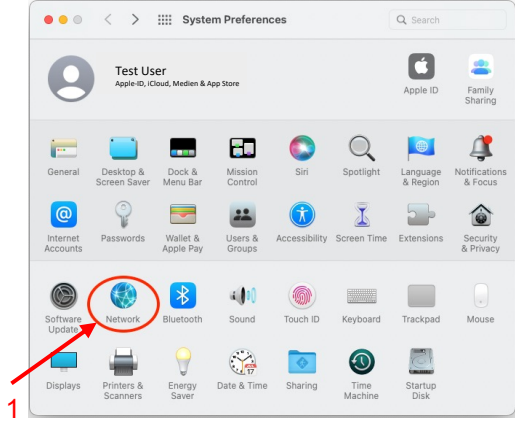
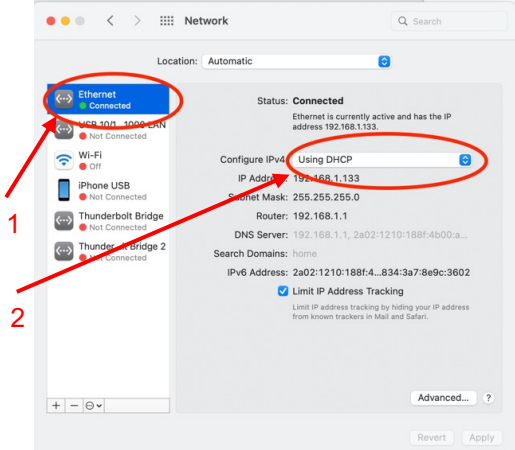
Register the MAC addresses of your devices with Central IT

To register your device's MAC addresses with Central IT, follow the steps described in section D at the end of this document.

C. Laptop and desktop computer with Mac OS

Activation of DHCP

To activate DHCP on your MacOS laptop and desktop computers, the steps below must be performed. Note that depending on your computer's configuration, an administrator password may be necessary.

Step	Description	Illustration
1.	In the Apple menu, select "System Preferences" and click on "Network" (❶).	
2.	Select the network connection "Ethernet" (❶) and activate "Using DHCP" (❷) in the drop-down menu "Configure IPv4".	

Activation of 802.1X

To activate 802.1X on your MacOS laptop and desktop computers, the steps below must be performed. Note that depending on your computer's configuration, an administrator password may be necessary.

Step	Description	Illustration
1.	In the apple menu, select "System Preferences" and click on "Network" (1).	
2.	Select the network connection "Ethernet" (1) and click on "Advanced..." (2).	
3.	Switch to the tab "802.1X" (1) and activate the checkbox "Enable automatic connection" (2). Click "OK".	



4.	<p>The next time you connect to the UZH IT network a dialog will pop up, asking you to enter username and password. Enter shortname and password of your UZH user account and click «OK».</p> <p>Note: In case you don't know the shortname of your UZH user account, log into the UZH Identity Management (identity.uzh.ch). The shortname is displayed as «User ID» under «Change password» for the entry «Active Directory».</p>	
----	--	--

Register the MAC addresses of your devices with Central IT

To register your device's MAC addresses with Central IT, follow the steps described in section D below.

D. Register the MAC addresses of your devices with Central IT

The registration of your device's MAC addresses is necessary if you are connecting devices to the UZH IT network without an UZH user account (username and password).

To register a MAC address with Central IT, the following information is required:

- Ethernet MAC address
- Device designation

Report this information for all your devices to your IT coordinator prior to the transition to NAC. Your IT coordinator will register this information with Central IT.

The Ethernet MAC address can normally be found on the device's manufacturer label and consists of 12 symbols between 0 and F. As an example, the manufacture label of a printer is shown below with the MAC addresses for WLAN and Ethernet.



In case the MAC address can't be found on the device, consult the user documentation, or contact the manufacturer.

Windows Devices (MAC Authentication Bypass)

Note that for Windows devices, which are authenticated with their MAC address, the Windows service "802.1X" must be deactivated. Proceed analogously to the description in chapters A/B under "Activation of 802.1X". If this service is not deactivated, you will be asked to enter username and password whenever connecting to the network.

Printers

Printers normally use DHCP and MAC addresses to connect to the UZH IT network. Due to the vast number of printers, it is not possible to describe a universally valid procedure. Consult your printer's user documentation or contact the manufacturer how to activate DHCP and report the MAC address to your IT coordinator.

Please note that you can always print your documents on any UZH Print Plus printer by using [mail to print](#).

Internet of Things (IoT) Devices

IoT devices normally use DHCP and MAC addresses to connect to the UZH IT network. Due to the vast number of IoT devices, it is not possible to describe a universally valid procedure. Consult your IoT device's user documentation or contact the manufacturer to learn how to activate DHCP and



report the MAC addresses to your IT coordinator so he can register the MAC address in IPAM Self Service.