

Zentrale Informatik

Universität Zürich Zentrale Informatik Pfingstweidstrasse 60B 8005 Zürich Schweiz Telefon +41 44 634 33 33 www.zi.uzh.ch

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 me 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.
- 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»	Image: Status Image: Ethernet 817 MB Image: Status Image: From the last 30 days Data usage Image: Status Properties Data usage Image: Status Image: Status Image: Status Image: Stat
3.	Right-click on «Ethernet» (❶) and select «Properties» (❷).	tt > Network Connections v v Search Network Connection is connection Rename this connection View status of this connection Change setti x Virtual Adapter bled x Virtual Adapter 1 virtual Adapter 2 virtual Adapter 1 virtual Adapter 2 virtual Adapter 1 virtual Adapter 2 virtual Adapter 1 virtual Adapter 1 virtual Adapter 2 virtual Adapter 2 virtual Adapter 1 virtual Adapter 2 virtual Adapter 3 virtual Adapt



4.	Switch to the tab «Networking» (1), click on «Internet Protocol Version 4 (TCP/IPv4) » (2) and click on «Properties» (3).	Image: Connect using: Image: Connect using: Image: Connect using: Image: Connect using:
5.	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» (3).	Internet Protocol Version 4 (TCP/IPv4) Properties X General Alternate Configuration You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. Obtain an IP address automatically Use the following IP address: IP address: Subnet mask: Default gateway: Obtain DNS server addresses: Preferred DNS server: . Alternate DNS server: . Alternate DNS server: . Validate settings upon exit Advanced. OK Cancel
6.	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.	Open the application «Services».	



2.	Right-click on the service «Wired AutoConfiguration» (1) and select «Start» (2).	Overet
3.	Make sure that the options «Stop the service» and «Restart the service» are visible on the left side of the window.	Image: Services File Action Yiew Help Image: Services Image: Services Image: Services Image: Services Image: Services Image: Services Image: Services Name Image: Services Image: Services Image: Services Name Image: Stop the service Image: Services Image: Services Name Image: Stop the service Image: Services Image: Services Name Image: Stop the service Image: Services Image: Services Image: Services Image: Stop the service Image: Services Image: Services Image: Services Image: Services Image: Stop the service Image: Services Image: Services Image: Services Image: Services Image: Stop the service Image: Services Image: Services Image: Services Image: Services Image: Stop the service Image: Services Image: Services Image: Services Image: Services Image: Stop the service Image: Services Image: Services Image: Services Image: Services Image: Stop the service Image: Services Image: Services Image: Service
4.	Close the window «Services».	
5.	Right-click on the Windows symbol and click on «Network Connections».	
6.	Under «Advanced Network Settings», click on «Change adapter options»	Image: Status Ethernet 817 MB Image: Min-Fi Properties Data usage Image: Dial-up Image: Dial-up Image: Dial-up Image: Dial-up Image: Dial-up Image: Dial-up </td
7.	Right-click on «Ethernet» (1) and select «Properties» (2).	t > Network Connections is connection Rename this connection View status of this connection Change setti x Virtual Adapter bled x Virtual Adapter 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2



8.	Switch to the tab «Authentication» (0) and	Ethernet 2 Properties
	make sure that the settings are identical to	Networking Authentication Sharing
	the settings in the picture on the right (2).	
	Click on « Settings» (8).	Select this option to provide authenticated network access for this Ethemet adapter.
	Note: In case the tab «Authentication» is not	Enable IEEE 802.1X authentication
	visible, the service was not properly started	Choose a network authentication method:
	in step 2, and the steps from step 2 onwards	Microsoft: Protected EAP (PEAP) V Settings
	must be repeated.	Remember my credentials for this connection each time I'm logged on
		Fallback to unauthorized network access
9.	Make sure that the options "Verify the	Protected EAP Properties X
	server's identity by validating the certificate"	When connecting:
	and "Connect to these servers" are	Verify the server's identity by validating the certificate
	activated, and the server is set to	Connect to these servers (examples:srv1;srv2;.*srv3\.com):
	"nacauth.uzh.ch" (0).	nacauth.uzh.ch
	Make sure that under "Trusted Root	Trusted Root Certification Authorities:
	Certification Authorities" the option "DigiCert	AAA Certificate Services Baltimore CyberTrust Root
	Global Root G2" is activated	Class 3 Public Primary Certification Authority
		DigiCert Assured ID Root CA
	Make sure that the option "Enable Identity	DigiCert Global Root G2
	Privacy" (9) is deactivated	DigiCert High Accurance 57 Root CA
		Notifications before connecting:
	Click "OK".	Tell user if the server name or root certificate isn't specified $\qquad \lor$
		Select Authentication Method:
		Secured password (EAP-MSCHAP v2) Configure
		Enable Fast Reconnect Disconnect if server does not present cryptobinding T V
		Enable Identity Privacy
		8
		OK Cancel



10.	Click on "Additional Settings" (1)	Ethernet 2 Properties X
		Networking Authentication Sharing
		Select this option to provide authenticated network access for this Ethemet adapter.
		Enable IEEE 802.1X authentication
		Choose a network authentication method:
		Microsoft: Protected EAP (PEAP) V Settings
		Remember my credentials for this connection each time I'm logged on
		Fallback to unauthorized network access
		Additional Settings
		0
		OK Cancel
11.	Activate the check box «Specify	Advanced settings X
	authentication mode» (1) and select «User	802.1X settings
	or computer authentication» from the drop-	Specify authentication mode
	(8).	User or computer authentication V Save credentials Delete credentials for all users
		Enable single sign on for this network
		Perform immediately before user logon
		Perform immediately after user logon Maximum delay (seconds):
		Allow additional dialogs to be displayed during single
		This network uses separate virtual LANs for machine
		and user authentication



12.	Enter shortname and password of your UZH user account and click «OK». 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».	Windows Security × Save credentials Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates). User name Password OK Cancel	
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.	Richard Leaf Account Network & internet Find a setting Image: Connected System Connected Bluetooth & devices Connected Metwork & internet Connected Network & internet Connected Materication, IP and DRI settings, metwork network Image: Correct, namage Accounts Correct, namage Time & language Correct, namage Charlen mode Connected Network & Burdity Correct, namage
2.	Scroll down to "IP assignment" and click on "Edit".	
3.	Under "Edit network settings", select "Automatic (DHCP) (❶). Click on "Save" (❷).	Network & internet > Ethernet Edit IP settings Automatic (DHCP) Save Cancel
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".	



2.	Right-click on the service «Wired AutoConfiguration» (❶) and select «Start» (❷).	Provide land land land land land land land land
3.	Make sure that the options «Stop the service» and «Restart the service» are visible on the left side of the window.	Services File Action ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ Services (Local) ✓ Windows Update Name ✓ ✓ Windows Remote Mana ✓ Windows Search
4.	Double-click on the service "Wired autoconfiguration" and under "Startup type", activate "Automatic".	Automatische Konfiguration (verkabelt) Properties (Local Computer) X General Log On Recovery Dependencies Service name: dot3svc Display name: Automatische Konfiguration (verkabelt) Description: The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X Bauthantication on Ethernal interfaces If your ournant Path to executable: C:Windows/system32/svchost.exe -k Local/SystemNetworkRestricted -p Startup type: Automatic Automatic Versul Disabled Versul Service status: Vumming Start Stop Pause Resume You can specify the start parameters that apply when you start the service from here. Start Start Dot Start parameters: OK Cancel Apply
5.	Close the window «Services».	
6.	Click the Windows key and enter "Control Panel" in the search field. Click on "Control Panel" and then on "Network and Internet"	
7.	Click on "Network and Sharing Center", on the UZH Ethernet-network.	Image and plane settings Lettern Control Planel Home View your basic network information and set up connections Control Planel Home View your basic network information and set up connections Change adapter settings Lettern Public network Access type: Ohange adapter settings Lettern Public network Connections: Otange your networking settings Change your networking settings Otange your networking settings Set up a household, dail-up, or VPR connection; or set up a noter or access point. Set up a household, get in theories Diagnose and repair network; or get troubleshooting information.



•		Printing / Status
	Click on "Properties", change to the tab "Authentication" (•), and make sure that your settings are identical to the ones shown in the picture on the right (•). 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.	 Ethernet 2 Properties Networking Authentication Sharing Select this option to provide authenticated network access for this Ethernet adapter. Enable IEEE 802.1X authentication Choose a network authentication method: Microsoft: Protected EAP (PEAP) Settings Remember my credentials for this connection each time I'm logged on Fallback to unauthorized network access
9.	Under "Choose a network authentication Method:", click on "Settings".	Ethernet 2 Properties Networking Authentication Sharing Select this option to provide authenticated network access for this Ethernet adapter. Select this option to provide authenticated network access for this Ethernet adapter. Select this ethernet adapter. Select this option to provide authenticated network access for this Ethernet adapter. Select this option to provide authenticated network access for this Ethernet adapter. Select this option to provide authenticated network access for this Ethernet adapter. Select this option to provide authentication Choose a network authentication Choose a network authentication method: Microsoft: Protected EAP (PEAP) Settings Remember my credentials for this connection each time I'm logged on Fallback to unauthorized network access
10.	 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" (•). Make sure that under "Trusted Root Certification Authorities", the option "DigiCert Global Root G2" is activated. Make sure that the option "Enable Identity Privacy" (•) is deactivated. Click "OK". 	Protected EAP Properties When connecting: Werify the server's identity by validating the certificate Connect to these servers (examples:srv1;srv2;.*srv3\.cor): nacauth.uzh.ch Trusted Root Certification Authorities: AAA Certificate Services Baltimore CyberTrust Root Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA BigGert Global Root G2 DigiCert Global Root G2 DigiCert Global Root G2 DigiCert Global Root G2 DigiCert High Accurate Root CA Secured password (EAP-MSCHAP v2)



11.	Click on "Additional Settings".	Ethernet 2 Properties ×
		Networking Authentication Sharing
		Select this option to provide authenticated network access for this Ethemet adapter.
		Enable IEEE 802.1X authentication
		Choose a network authentication method:
		Microsoft: Protected EAP (PEAP) V Settings
		Remember my credentials for this connection each time I'm logged on
		Fallback to unauthorized network access
		Additional Settings
12.	Activate the check box «Specify	Advanced settings X
	authentication mode» (0) and select «User	1 802. 1X settings
	authentication» from the drop-down list (2).	Specify authentication mode
	vour UZH username and password. Click on	User or computer authentication $$
	"OK" and leave all open dialogues by	2 Delete credentials for all users
	clicking "OK".	Enable single sign on for this network
		Perform immediately before user logon
	NOTE: The UZH username and password	Perform immediately after user logon Maximum delay (seconds):
	that are entered in this step will be used for every future connection to the LIZH Ethernet	Allow additional dialogs to be displayed during single
	Network. Make sure that you enter	This network uses separate virtual LANs for machine
	username and password of your personal	and user authentication
	UZH account!	
		OK Cancel
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	O C C C C C C C C C C C C C C C C C
	Preferences" and click on "Network" (1).	Test User Apple ID. Cloud, Meden # App Store
		General Desktop & Dock & Menu Bar Control Siri Spotlight Language Motifications & Focus
		Internet Passwords Wallet & Apple Pay Least Users & Groups Colorest Accessibility Screen Time Extensions Security & Privacy
		Software Updeter Network Bluetooth Sound Touch ID Keyboard Trackpad Mouse
		Displays Printers & Energy Date & Time Sharing Time Startup Displays Printers & Energy Date & Time Sharing Machine Disk
2.	Select the network connection "Ethernet" (1)	• • • < > IIII Network
	down menu "Configure IPv4".	Vertice Vertice Vertice
		+ - 0 - Advanced ?
		Revert Apply



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).	Image: Search Image: System Preferences Image: Search Image: Search Image: Search Image: Search Image: Search Image: Search Image: Search Image: Search Image: Search Image: Search Image: Search Ima
2.	Select the network connection "Ethernet" (1) and click on "Advanced…" (2).	Image: Constant of the second of
3.	Switch to the tab "802.1X" (•) and activate the checkbox "Enable automatic connection" (•). Click "OK".	Conception of the second secon



4.	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».	
	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	

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 not that you can always print your documents on any UZH Print Plus printer by using <u>mail to</u> <u>print</u>.

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.