

Gehe auf «idm.lab.local»

Gib deine erhaltenen daten ein und ändere dein Passwort, falls du dazu aufgefordert wirst

The screenshot shows the Red Hat Identity Management login interface in a web browser. The browser's address bar displays 'https://idm.lab.local/ipa/ui/'. The page features the Red Hat logo in the top right corner. Below the logo, the text 'RED HAT® IDENTITY MANAGEMENT' is visible. The login form includes two input fields: 'Username' and 'Password'. The 'Password' field has a hint: 'Password or Password+One-Time Password'. To the right of the input fields, there are three instructions for different login methods: 1. 'To log in with username and password, enter them in the corresponding fields, then click 'Log in'.' 2. 'To log in with Kerberos, please make sure you have valid tickets (obtainable via kinit) and configure the browser correctly, then click 'Log in'.' 3. 'To log in with certificate, please make sure you have valid personal certificate.' Below the instructions, there are links for 'Log In Using Certificate' and 'Sync OTP Token', followed by a blue 'Log In' button.

Klicke auf Authentication

The screenshot shows the navigation menu of the Red Hat Identity Management interface. The menu is titled 'RED HAT® IDENTITY MANAGEMENT'. It contains several tabs: 'Identity', 'Policy', 'Authentication', 'Network Services', and 'IPA Server'. The 'Authentication' tab is highlighted with a red rectangle. Below the main tabs, there is a secondary row of links: 'Users', 'Hosts', 'Services', 'Groups', 'ID Views', 'Automember', and 'Subordinate IDs'. The 'Users' link is underlined. Below this row, there is a section titled 'User categories' with a list of categories: 'Active users' (which is highlighted in blue and has a right-pointing arrow), and 'Inactive users'.

Du solltest jetzt eine Liste mit Zertifikaten sehen klicke auf das mit der Nummer 1.

Certificates

Serial Number	Subject	Issuing CA	
1	CN=Certificate Authority,O=LAB.LOCAL	ipa	VALID
2	CN=OCSP Subsystem,O=LAB.LOCAL	ipa	VALID
3	CN=idm.lab.local,O=LAB.LOCAL	ipa	VALID
4	CN=CA Subsystem,O=LAB.LOCAL	ipa	VALID
5	CN=CA Audit,O=LAB.LOCAL	ipa	VALID
6	CN=ipa-ca-agent,O=LAB.LOCAL	ipa	VALID
7	CN=IPA RA,O=LAB.LOCAL	ipa	VALID
8	CN=idm.lab.local,O=LAB.LOCAL	ipa	VALID
9	CN=idm.lab.local,O=LAB.LOCAL	ipa	VALID
10	CN=idm.lab.local,O=LAB.LOCAL	ipa	VALID
11	CN=idm2.lab.local,O=LAB.LOCAL	ipa	VALID
12	CN=idm2.lab.local,O=LAB.LOCAL	ipa	VALID
13	CN=idm2.lab.local,O=LAB.LOCAL	ipa	VALID
14	CN=idm2.lab.local,O=LAB.LOCAL	ipa	VALID

14 certificates matched

Wenn du auf «Actions» klickst und dann auf «Download» dann solltest du in deinem Download Ordner ein File mit dem Namen «cert.pem» haben.

Certificate: 1

Refresh Actions

Certificate

Serial Number	1
Serial Number (hex)	0x1
Issuing CA	ipa
Subject	CN=Certificate Authority,O=LAB.LOCAL
Issuer	CN=Certificate Authority,O=LAB.LOCAL
Issued On	Wed Jul 10 07:43:19 2024 UTC
Expires On	Sun Jul 10 07:43:19 2044 UTC
SHA1 Fingerprint	1d:95:8d:e5:6d:9b:23:2d:ab:71:44:49:72:ec:a6:13:bd:e0:44:88
SHA256 Fingerprint	95:fe:6b:c2:5fa9:6e:5b:83:30:85:bf:4f:3f:26:cb:93:7c:cf:da:8c:76:70:c3:13:a2:bd:0d:e8:6a:df:dd

Certificate: 1

Refresh Actions

Revoke certificate
Remove hold
Download

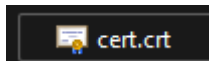
Downloads

Name

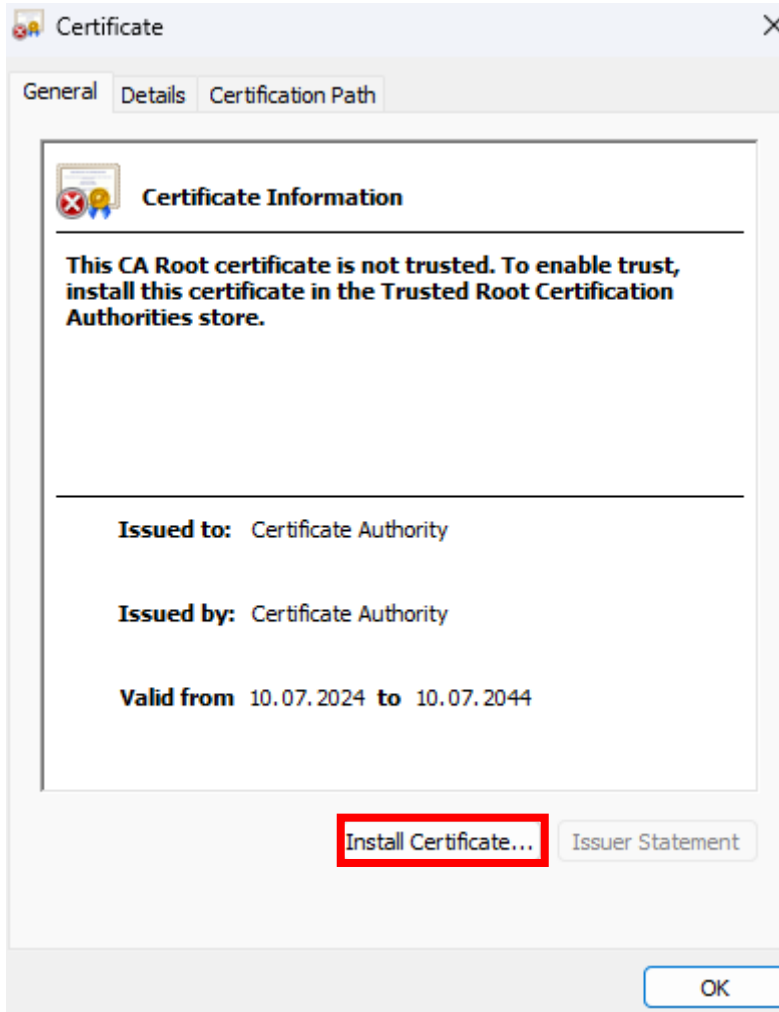
Today

cert.pem

Um die Certificate Authority zu installieren, musst du das File von «cert.pem» auf «cert.crt» umbenennen. Danach sollte es wie folgt aussehen.



Wenn du das dann mit einem Doppelklick öffnest, sollte Folgendes erscheinen. Hier musst du auf «Install Certificate...» klicken.



Folge jetzt den Bildern, um das Zertifikat am richtigen Ort zu installieren.



← Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

☐ Current User

☒ Local Machine

To continue, click Next.

Next

Cancel



← Certificate Import Wizard

Certificate Store

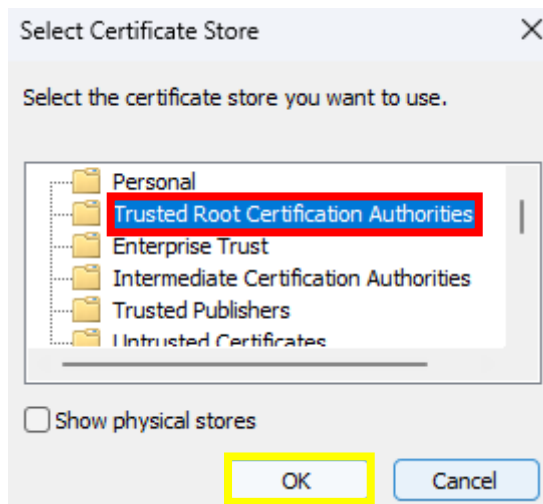
Certificate stores are system areas where certificates are kept.


Windows can automatically select a certificate store, or you can specify a location for the certificate.

- ☐ Automatically select the certificate store based on the type of certificate
- ☒ Place all certificates in the following store

Certificate store:

Browse...



←  Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

- ☐ Automatically select the certificate store based on the type of certificate
- ☒ Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

[Browse...](#)

Next

Cancel

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

Finish

Cancel

Wenn alles funktioniert hat sollte Folgendes zu sehen sein.

Certificate Import Wizard



The import was successful.

OK