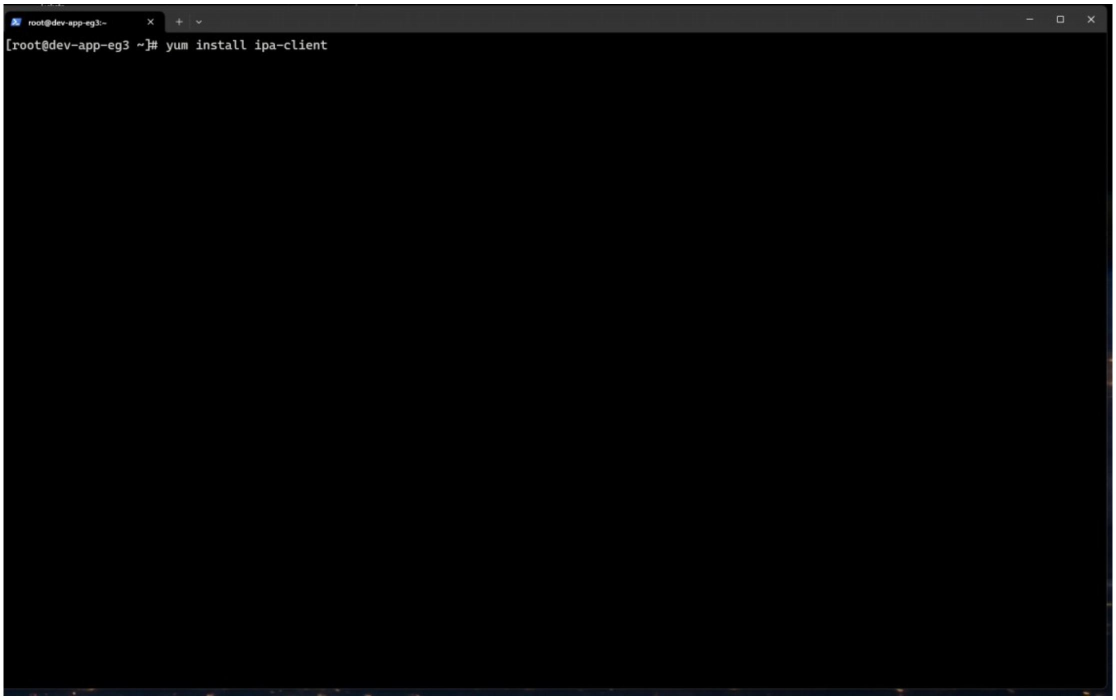
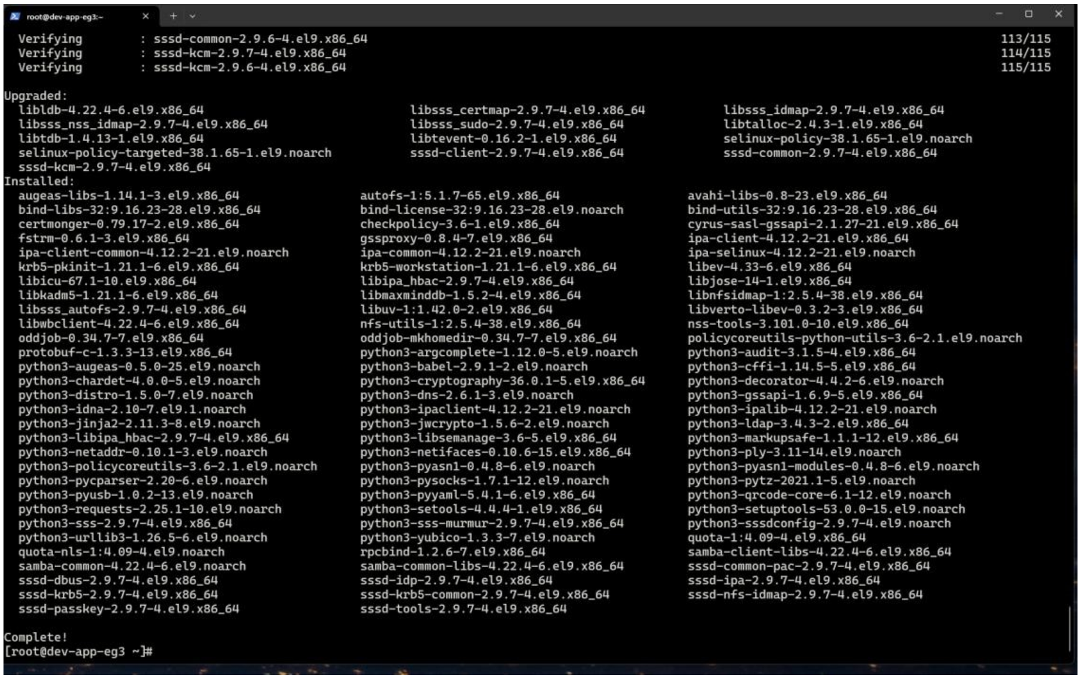
Task: Install and Configure FreeIPA client

This command installs the FreeIPA client on the system. yum install ipa-client downloads and installs the packages needed for the server to join a FreeIPA domain. After installation, the system can be configured to use centralized authentication, authorization, and identity management (users, groups, Kerberos, sudo rules, etc.) from the FreeIPA server.



```
[root@dev-app-eg3 ~]# yum install ipa-client
```

This output confirms that the FreeIPA client and its dependencies were successfully installed. Required packages such as ipa-client, sssd, Kerberos (krb5), LDAP, and SELinux utilities were installed or upgraded



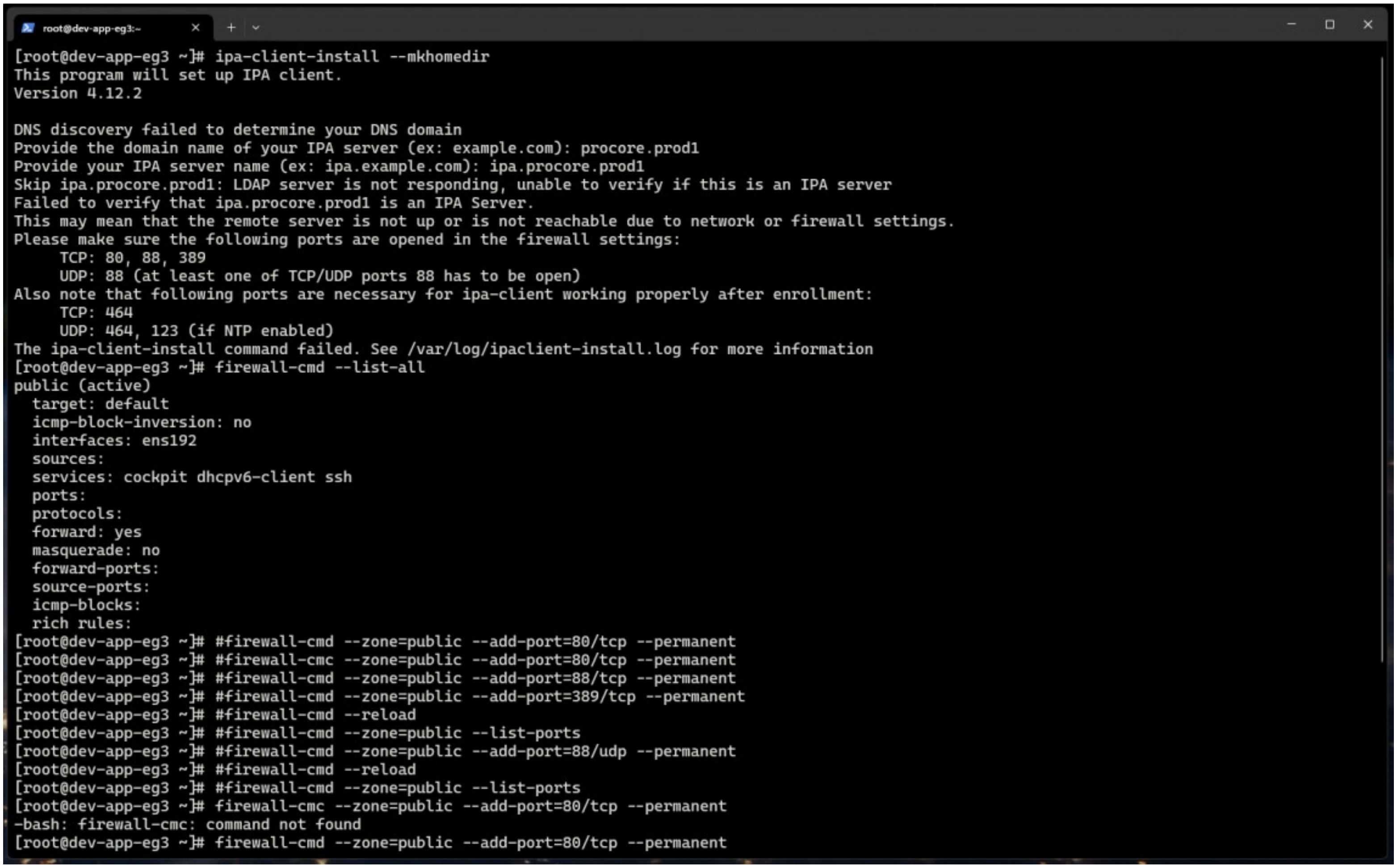
```
  Verifying        : sssd-common-2.9.6-4.el9.x86_64                                                                  113/115
  Verifying        : sssd-kcm-2.9.7-4.el9.x86_64                                                                     114/115
  Verifying        : sssd-kcm-2.9.6-4.el9.x86_64                                                                     115/115

Upgraded:
  libldb-4.22.4-6.el9.x86_64                             libsss_certmap-2.9.7-4.el9.x86_64            libsss_idmap-2.9.7-4.el9.x86_64
  libsss_nss_idmap-2.9.7-4.el9.x86_64                    libsss_sudo-2.9.7-4.el9.x86_64               libtalloc-2.4.3-1.el9.x86_64
  libtdb-1.4.13-1.el9.x86_64                             libtevent-0.16.2-1.el9.x86_64                selinux-policy-38.1.65-1.el9.noarch
  selinux-policy-targeted-38.1.65-1.el9.noarch           sssd-client-2.9.7-4.el9.x86_64               sssd-common-2.9.7-4.el9.x86_64
  sssd-kcm-2.9.7-4.el9.x86_64
Installed:
  augeas-libs-1.14.1-3.el9.x86_64                 autofs-1:5.1.7-65.el9.x86_64                 avahi-libs-0.8-23.el9.x86_64
  bind-libs-32:9.16.23-28.el9.x86_64              bind-license-32:9.16.23-28.el9.noarch        bind-utils-32:9.16.23-28.el9.x86_64
  certmonger-0.79.17-2.el9.x86_64                 checkpolicy-3.6-1.el9.x86_64                 cyrus-sasl-gssapi-2.1.27-21.el9.x86_64
  fstrm-0.6.1-3.el9.x86_64                        gssproxy-0.8.4-7.el9.x86_64                  ipa-client-4.12.2-21.el9.x86_64
  ipa-client-common-4.12.2-21.el9.noarch          ipa-common-4.12.2-21.el9.noarch              ipa-selinux-4.12.2-21.el9.noarch
  krb5-pkinit-1.21.1-6.el9.x86_64                 krb5-workstation-1.21.1-6.el9.x86_64         libev-4.33-6.el9.x86_64
  libicu-67.1-10.el9.x86_64                       libipa_hbac-2.9.7-4.el9.x86_64               libjose-14-1.el9.x86_64
  libkadm5-1.21.1-6.el9.x86_64                    libmaxminddb-1.5.2-4.el9.x86_64              libnfsidmap-1:2.5.4-38.el9.x86_64
  libsss_autofs-2.9.7-4.el9.x86_64                libuv-1:1.42.0-2.el9.x86_64                  libverto-libev-0.3.2-3.el9.x86_64
  libwbclient-4.22.4-6.el9.x86_64                 nfs-utils-1:2.5.4-38.el9.x86_64              nss-tools-3.101.0-10.el9.x86_64
  oddjob-0.34.7-7.el9.x86_64                      oddjob-mkhomedir-0.34.7-7.el9.x86_64         policycoreutils-python-utils-3.6-2.1.el9.noarch
  protobuf-c-1.3.3-13.el9.x86_64                  python3-argcomplete-1.12.0-5.el9.noarch      python3-audit-3.1.5-4.el9.x86_64
  python3-augeas-0.5.0-25.el9.noarch              python3-babel-2.9.1-2.el9.noarch             python3-cffi-1.14.5-5.el9.x86_64
  python3-chardet-4.0.0-5.el9.noarch              python3-cryptography-36.0.1-5.el9.x86_64     python3-decorator-4.4.2-6.el9.noarch
  python3-distro-1.5.0-7.el9.noarch               python3-dns-2.6.1-3.el9.noarch               python3-gssapi-1.6.9-5.el9.x86_64
  python3-idna-2.10-7.el9.1.noarch                python3-ipaclient-4.12.2-21.el9.noarch       python3-ipalib-4.12.2-21.el9.noarch
  python3-jinja2-2.11.3-8.el9.noarch              python3-jwcrypto-1.5.6-2.el9.noarch          python3-ldap-3.4.3-2.el9.x86_64
  python3-libipa_hbac-2.9.7-4.el9.x86_64          python3-libsemanage-3.6-5.el9.x86_64         python3-markupsafe-1.1.1-12.el9.x86_64
  python3-netaddr-0.10.1-3.el9.noarch             python3-netifaces-0.10.6-15.el9.x86_64       python3-ply-3.11-14.el9.noarch
  python3-policycoreutils-3.6-2.1.el9.noarch      python3-pyasn1-0.4.8-6.el9.noarch            python3-pyasn1-modules-0.4.8-6.el9.noarch
  python3-pycparser-2.20-6.el9.noarch             python3-pysocks-1.7.1-12.el9.noarch          python3-pytz-2021.1-5.el9.noarch
  python3-pyusb-1.0.2-13.el9.noarch               python3-pyyaml-5.4.1-6.el9.x86_64            python3-qrcode-core-6.1-12.el9.noarch
  python3-requests-2.25.1-10.el9.noarch           python3-setools-4.4.4-1.el9.x86_64           python3-setuptools-53.0.0-15.el9.noarch
  python3-sss-2.9.7-4.el9.x86_64                  python3-sss-murmur-2.9.7-4.el9.x86_64        python3-sssdconfig-2.9.7-4.el9.noarch
  python3-urllib3-1.26.5-6.el9.noarch             python3-yubico-1.3.3-7.el9.noarch            quota-1:4.09-4.el9.x86_64
  quota-nls-1:4.09-4.el9.noarch                   rpcbind-1.2.6-7.el9.x86_64                   samba-client-libs-4.22.4-6.el9.x86_64
  samba-common-4.22.4-6.el9.noarch                samba-common-libs-4.22.4-6.el9.x86_64        sssd-common-pac-2.9.7-4.el9.x86_64
  sssd-dbus-2.9.7-4.el9.x86_64                    sssd-idp-2.9.7-4.el9.x86_64                  sssd-ipa-2.9.7-4.el9.x86_64
  sssd-krb5-2.9.7-4.el9.x86_64                    sssd-krb5-common-2.9.7-4.el9.x86_64          sssd-nfs-idmap-2.9.7-4.el9.x86_64
  sssd-passkey-2.9.7-4.el9.x86_64                 sssd-tools-2.9.7-4.el9.x86_64

Complete!
[root@dev-app-eg3 ~]#
```

I ran ipa-client-install --mkhomedir to configure the system as a FreeIPA client and enable automatic home directory creation for IPA users. Because DNS discovery did not automatically detect the IPA domain, I manually specified the IPA domain (procore.prod1) and IPA server (ipa.procore.prod1).

After the installer reported required firewall ports were not open, I verified the active firewall configuration and opened the necessary ports using firewall-cmd (80, 88, 389 TCP and 88 UDP), then reloaded the firewall to apply the changes. This prepared the system for a successful FreeIPA client enrollment.

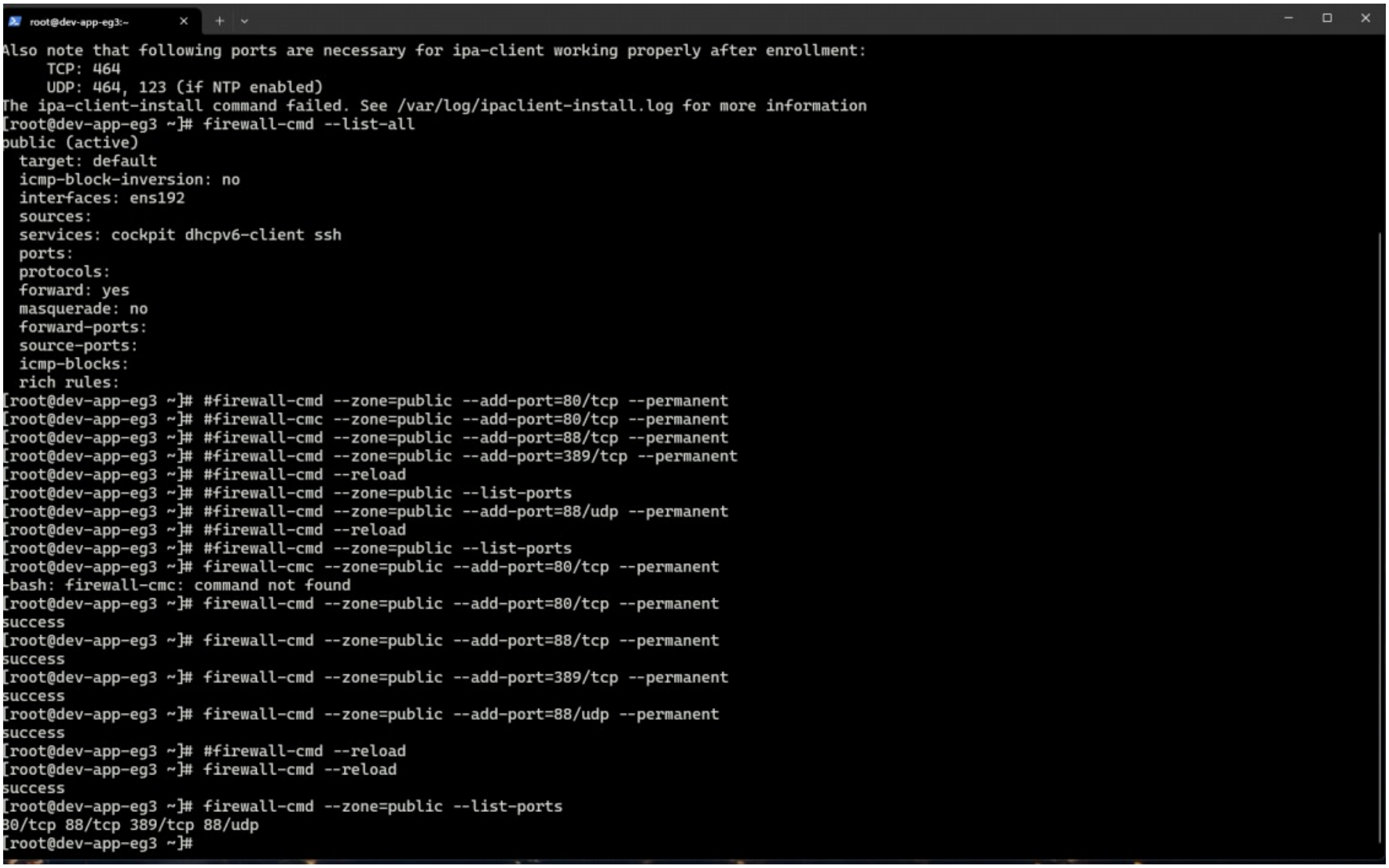


```
[root@dev-app-eg3 ~]# ipa-client-install --mkhomedir
This program will set up IPA client.
Version 4.12.2

DNS discovery failed to determine your DNS domain
Provide the domain name of your IPA server (ex: example.com): procore.prod1
Provide your IPA server name (ex: ipa.example.com): ipa.procore.prod1
Skip ipa.procore.prod1: LDAP server is not responding, unable to verify if this is an IPA server
Failed to verify that ipa.procore.prod1 is an IPA Server.
This may mean that the remote server is not up or is not reachable due to network or firewall settings.
Please make sure the following ports are opened in the firewall settings:
     TCP: 80, 88, 389
     UDP: 88 (at least one of TCP/UDP ports 88 has to be open)
Also note that following ports are necessary for ipa-client working properly after enrollment:
     TCP: 464
     UDP: 464, 123 (if NTP enabled)
The ipa-client-install command failed. See /var/log/ipaclient-install.log for more information
[root@dev-app-eg3 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --add-port=80/tcp --permanent
[root@dev-app-eg3 ~]# #firewall-cmc --zone=public --add-port=80/tcp --permanent
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --add-port=88/tcp --permanent
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --add-port=389/tcp --permanent
[root@dev-app-eg3 ~]# #firewall-cmd --reload
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --list-ports
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --add-port=88/udp --permanent
[root@dev-app-eg3 ~]# #firewall-cmd --reload
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --list-ports
[root@dev-app-eg3 ~]# firewall-cmc --zone=public --add-port=80/tcp --permanent
-bash: firewall-cmc: command not found
[root@dev-app-eg3 ~]# firewall-cmd --zone=public --add-port=80/tcp --permanent
```

After the FreeIPA client enrollment indicated required ports were missing, I verified the active firewall configuration and manually opened the necessary ports using firewall-cmd. I added TCP ports 80, 88, and 389 and UDP port 88 to the public zone, reloaded the firewall, and confirmed the changes with --list-ports.

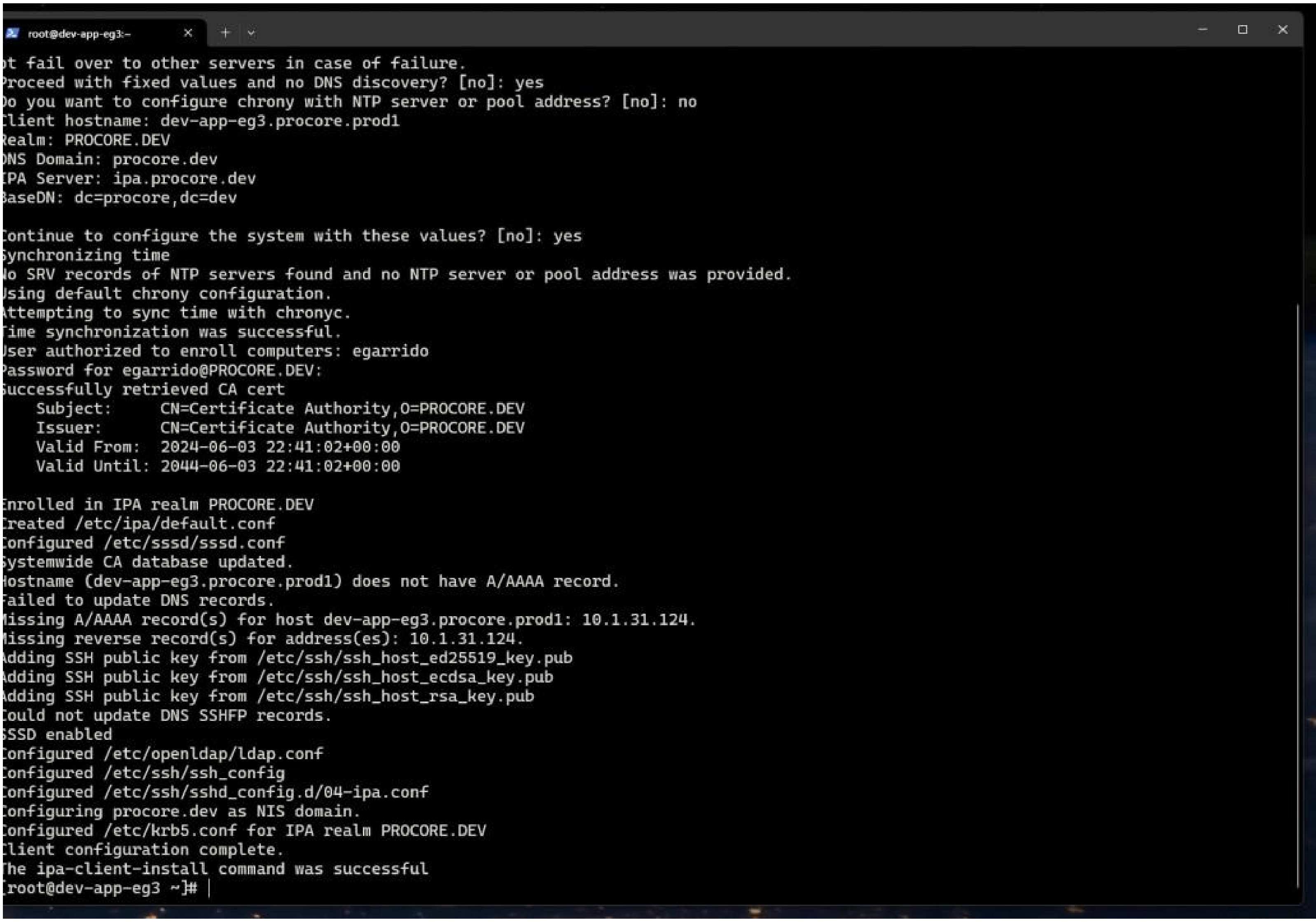
In short: the firewall is now correctly configured to allow FreeIPA communication, preparing the system for successful IPA client enrollment.



```
Also note that following ports are necessary for ipa-client working properly after enrollment:
     TCP: 464
     UDP: 464, 123 (if NTP enabled)
The ipa-client-install command failed. See /var/log/ipaclient-install.log for more information
[root@dev-app-eg3 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --add-port=80/tcp --permanent
[root@dev-app-eg3 ~]# #firewall-cmc --zone=public --add-port=80/tcp --permanent
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --add-port=88/tcp --permanent
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --add-port=389/tcp --permanent
[root@dev-app-eg3 ~]# #firewall-cmd --reload
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --list-ports
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --add-port=88/udp --permanent
[root@dev-app-eg3 ~]# #firewall-cmd --reload
[root@dev-app-eg3 ~]# #firewall-cmd --zone=public --list-ports
[root@dev-app-eg3 ~]# firewall-cmc --zone=public --add-port=80/tcp --permanent
-bash: firewall-cmc: command not found
[root@dev-app-eg3 ~]# firewall-cmd --zone=public --add-port=80/tcp --permanent
success
[root@dev-app-eg3 ~]# firewall-cmd --zone=public --add-port=88/tcp --permanent
success
[root@dev-app-eg3 ~]# firewall-cmd --zone=public --add-port=389/tcp --permanent
success
[root@dev-app-eg3 ~]# firewall-cmd --zone=public --add-port=88/udp --permanent
success
[root@dev-app-eg3 ~]# #firewall-cmd --reload
[root@dev-app-eg3 ~]# firewall-cmd --reload
success
[root@dev-app-eg3 ~]# firewall-cmd --zone=public --list-ports
80/tcp 88/tcp 389/tcp 88/udp
[root@dev-app-eg3 ~]#
```

I successfully completed the FreeIPA client enrollment by providing the required domain and server details and confirming the configuration. The system synchronized time, authenticated with the IPA server, retrieved the certificate authority, and joined the IPA realm (PROCORE.DEV).

During enrollment, the client configured SSSD, Kerberos, LDAP, and SSH, enabled centralized authentication, and installed host SSH keys. DNS forward and reverse records were reported as missing, but this did not prevent successful enrollment.

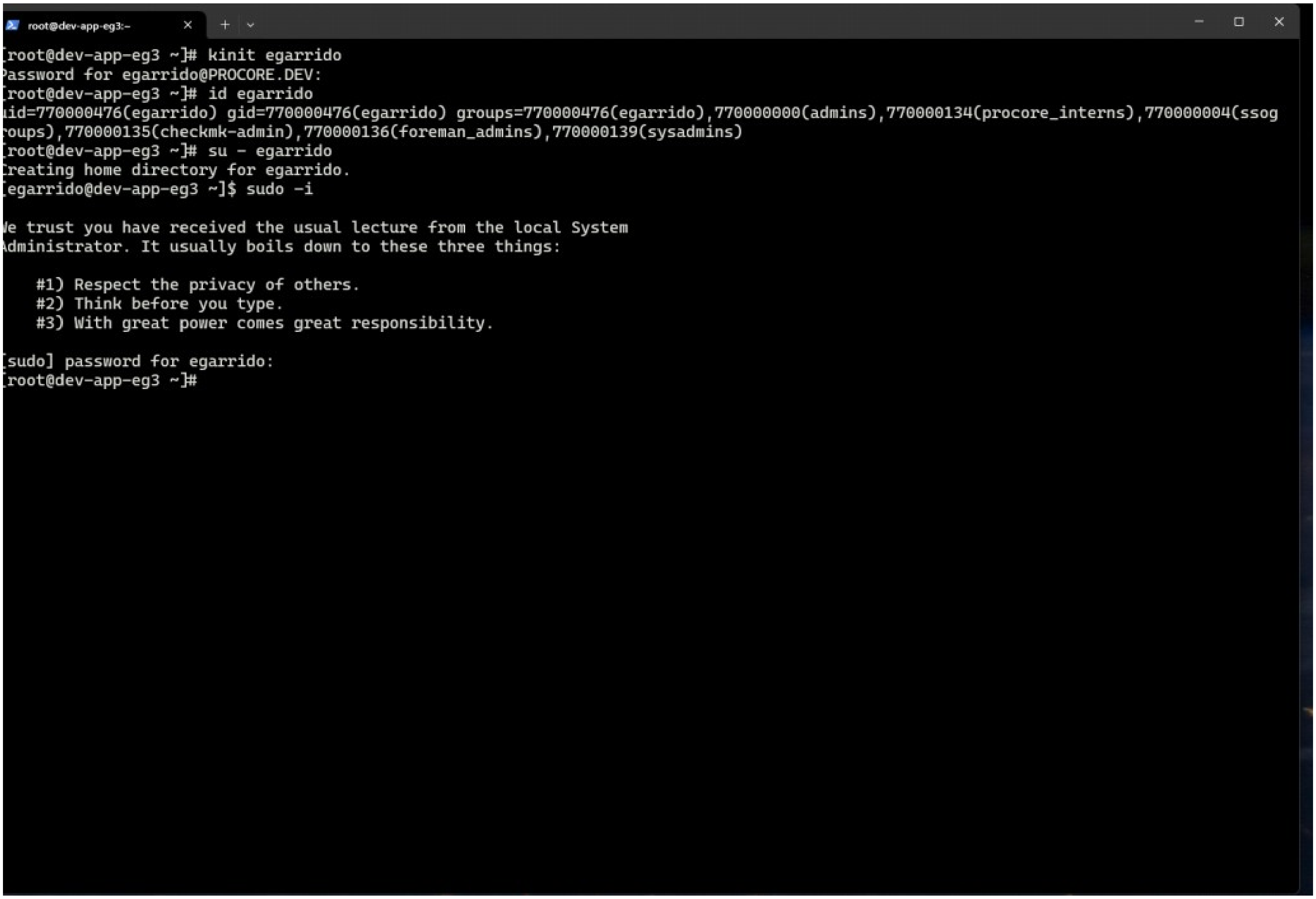


```
ot fail over to other servers in case of failure.
roceed with fixed values and no DNS discovery? [no]: yes
o you want to configure chrony with NTP server or pool address? [no]: no
lient hostname: dev-app-eg3.procore.prod1
ealm: PROCORE.DEV
NS Domain: procore.dev
IPA Server: ipa.procore.dev
aseDN: dc=procore,dc=dev

ontinue to configure the system with these values? [no]: yes
ynchronizing time
o SRV records of NTP servers found and no NTP server or pool address was provided.
sing default chrony configuration.
ttempting to sync time with chronyc.
ime synchronization was successful.
ser authorized to enroll computers: egarrido
assword for egarrido@PROCORE.DEV:
uccessfully retrieved CA cert
    Subject:     CN=Certificate Authority,O=PROCORE.DEV
    Issuer:      CN=Certificate Authority,O=PROCORE.DEV
    Valid From:  2024-06-03 22:41:02+00:00
    Valid Until: 2044-06-03 22:41:02+00:00

nrolled in IPA realm PROCORE.DEV
reated /etc/ipa/default.conf
onfigured /etc/sssd/sssd.conf
ystemwide CA database updated.
ostname (dev-app-eg3.procore.prod1) does not have A/AAAA record.
ailed to update DNS records.
issing A/AAAA record(s) for host dev-app-eg3.procore.prod1: 10.1.31.124.
issing reverse record(s) for address(es): 10.1.31.124.
dding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
dding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
dding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
ould not update DNS SSHFP records.
SSD enabled
onfigured /etc/openldap/ldap.conf
onfigured /etc/ssh/ssh_config
onfigured /etc/ssh/sshd_config.d/04-ipa.conf
onfiguring procore.dev as NIS domain.
onfigured /etc/krb5.conf for IPA realm PROCORE.DEV
lient configuration complete.
he ipa-client-install command was successful
root@dev-app-eg3 ~]# |
```

I verified FreeIPA authentication and authorization by obtaining a Kerberos ticket with kinit, confirming user and group information with id, and logging in as the IPA user. The system automatically created the user’s home directory, demonstrating successful --mkhomedir configuration. I then confirmed sudo access using sudo -i, showing that IPA group-based privileges are correctly applied.



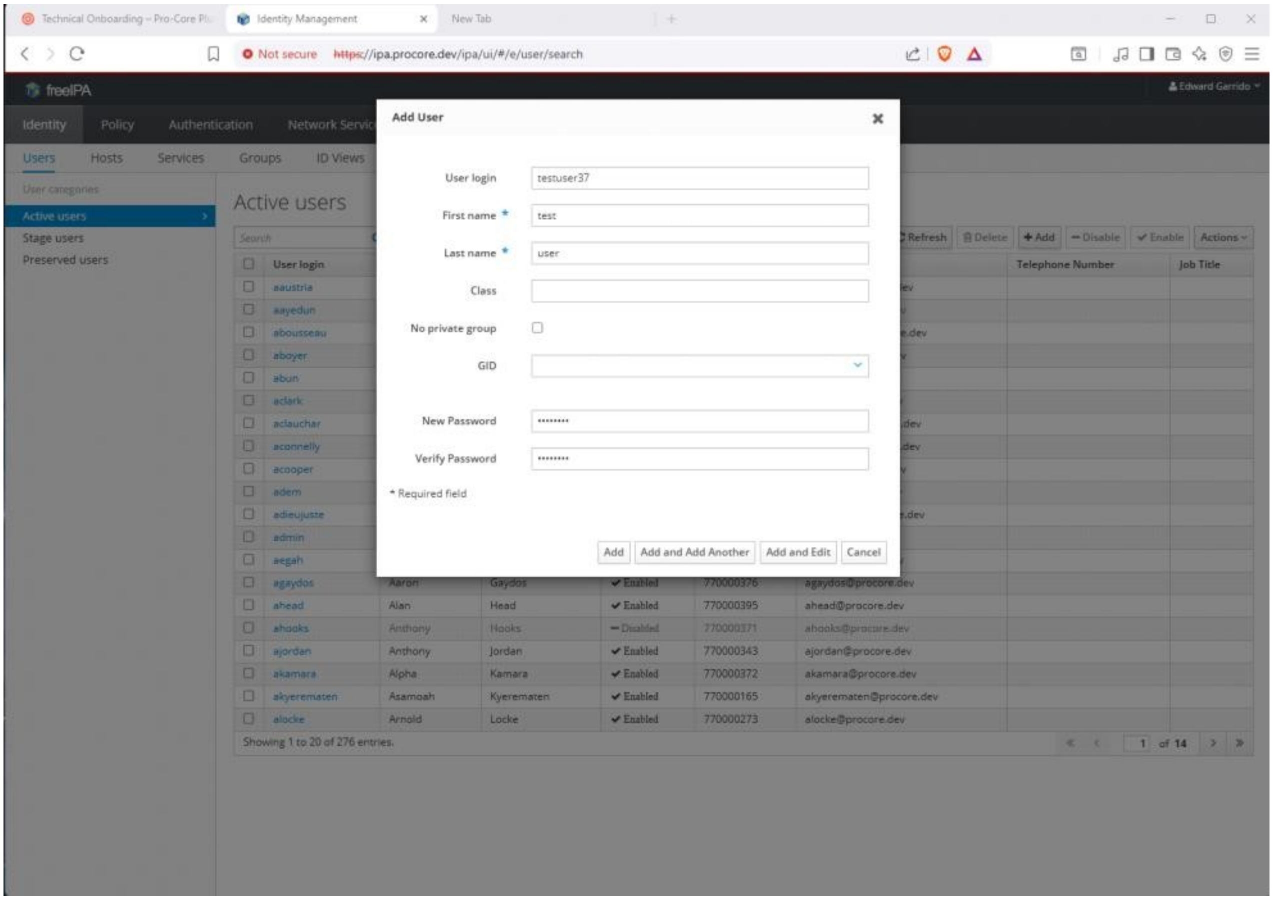
```
[root@dev-app-eg3 ~]# kinit egarrido
Password for egarrido@PROCORE.DEV:
[root@dev-app-eg3 ~]# id egarrido
uid=770000476(egarrido) gid=770000476(egarrido) groups=770000476(egarrido),770000000(admins),770000134(procore_interns),770000004(ssog
roups),770000135(checkmk-admin),770000136(foreman_admins),770000139(sysadmins)
[root@dev-app-eg3 ~]# su - egarrido
Creating home directory for egarrido.
[egarrido@dev-app-eg3 ~]$ sudo -i

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for egarrido:
[root@dev-app-eg3 ~]#
```

I created a new user in the FreeIPA web interface, adding them to centralized identity management for domain-wide authentication.



Add User

User login	testuser37
First name *	test
Last name *	user
Class	
No private group	□
GID	
New Password	••••••••
Verify Password	••••••••

* Required field

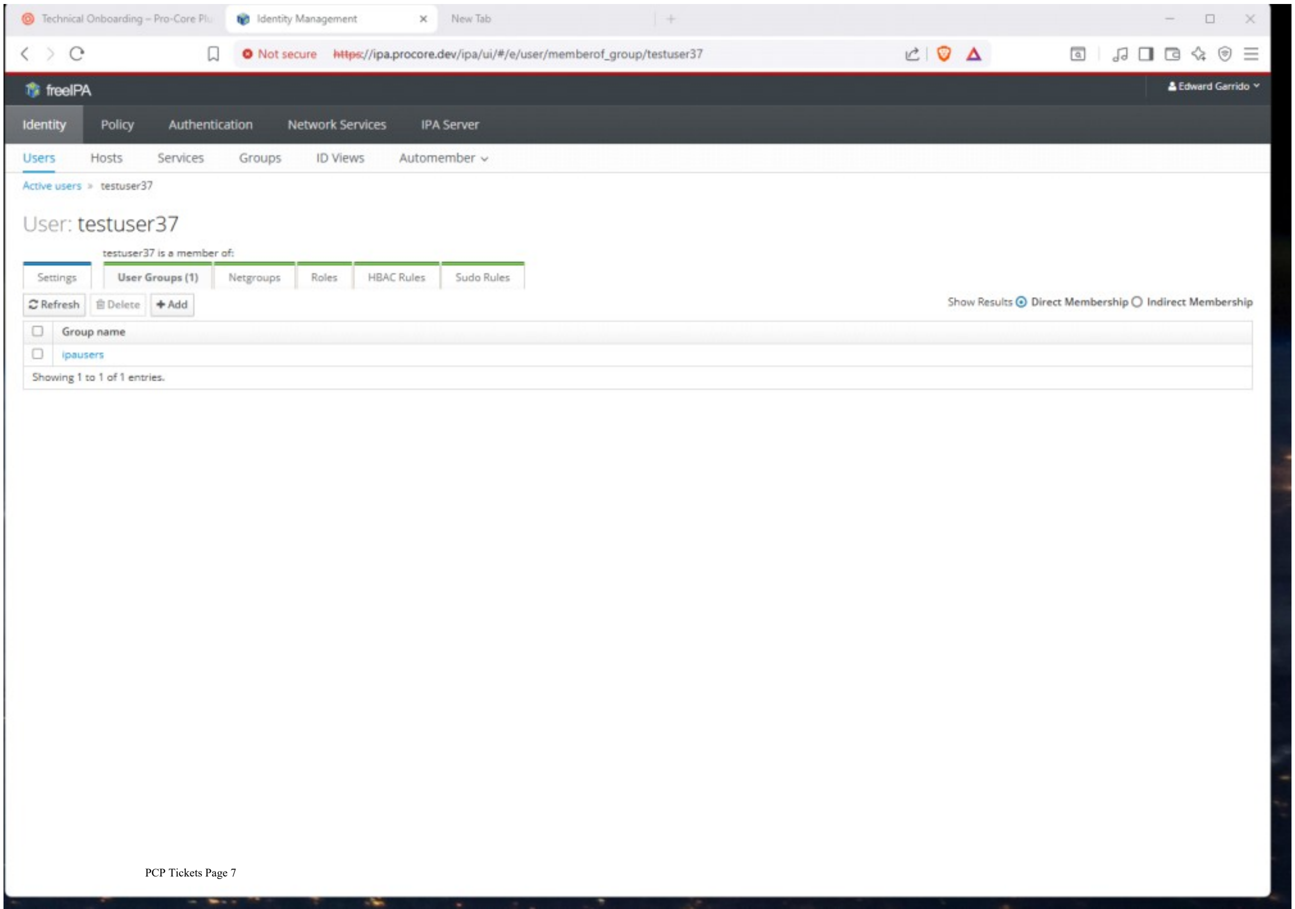
Add | Add and Add Another | Add and Edit | Cancel

User login						Telephone Number	Job Title
aaustria					ev		
aayedun							
abousseau					e.dev		
aboyer							
abun							
aclark							
aclauchar					dev		
aconnelly					dev		
acooper							
adem							
adieujuste					e.dev		
admin							
aegah							
agaydos	Aaron	Gaydos	✓ Enabled	770000376	agaydos@procore.dev		
ahead	Alan	Head	✓ Enabled	770000395	ahead@procore.dev		
ahooks	Anthony	Hooks	− Disabled	770000371	ahooks@procore.dev		
ajordan	Anthony	Jordan	✓ Enabled	770000343	ajordan@procore.dev		
akamara	Alpha	Kamara	✓ Enabled	770000372	akamara@procore.dev		
akyerematen	Asamoah	Kyerematen	✓ Enabled	770000165	akyerematen@procore.dev		
alocke	Arnold	Locke	✓ Enabled	770000273	alocke@procore.dev		

Showing 1 to 20 of 276 entries.

1 of 14

I added the user to the ipausers group in FreeIPA, granting standard domain access.



User: testuser37

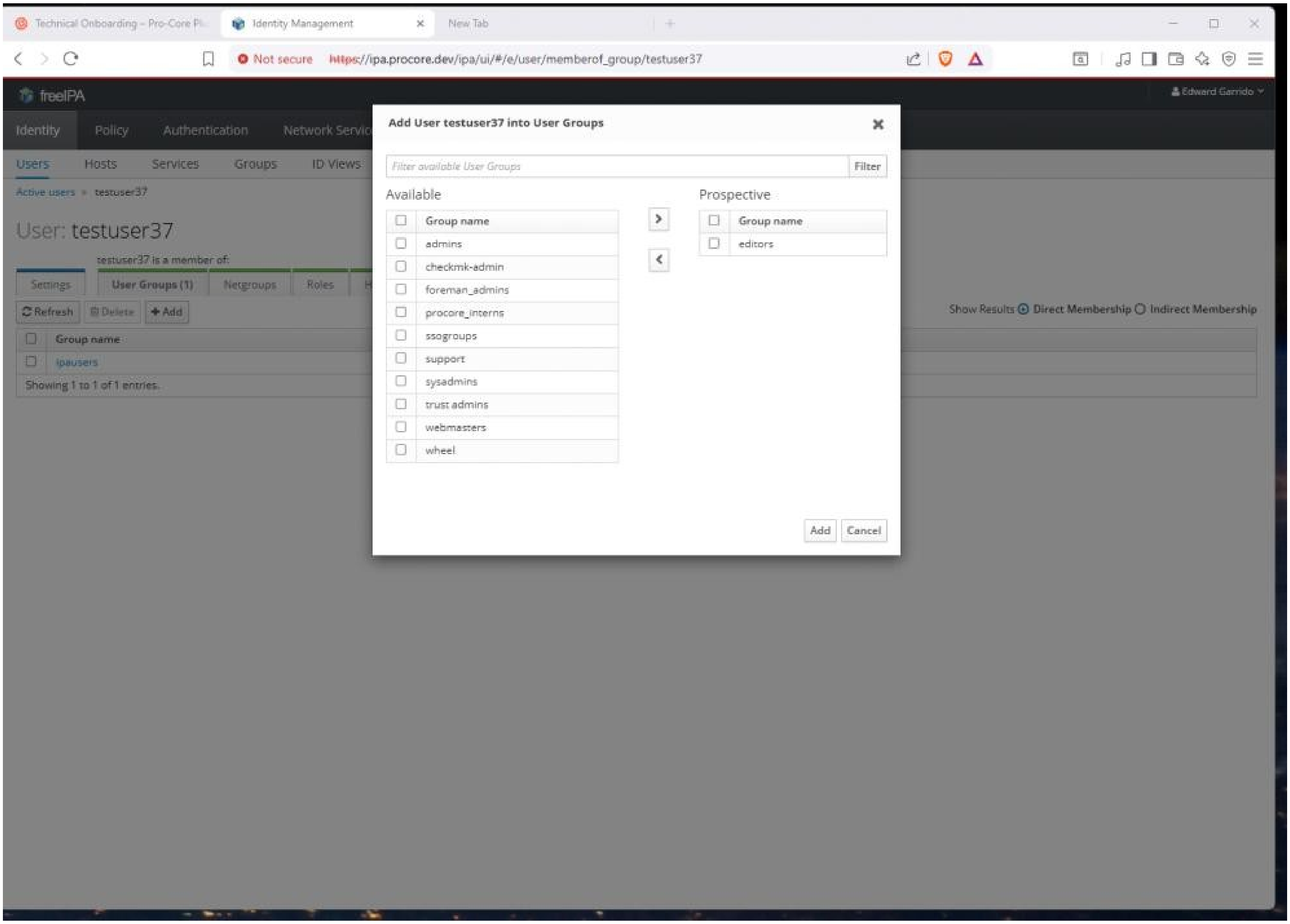
testuser37 is a member of:

Show Results ● Direct Membership ○ Indirect Membership

□	Group name
□	ipausers

Showing 1 to 1 of 1 entries.

I added the user to the appropriate FreeIPA groups by clicking Add in the User Groups section to assign access and permissions.



User: testuser37

testuser37 is a member of:

□	Group name
□	ipausers

Showing 1 to 1 of 1 entries.

Add User testuser37 into User Groups

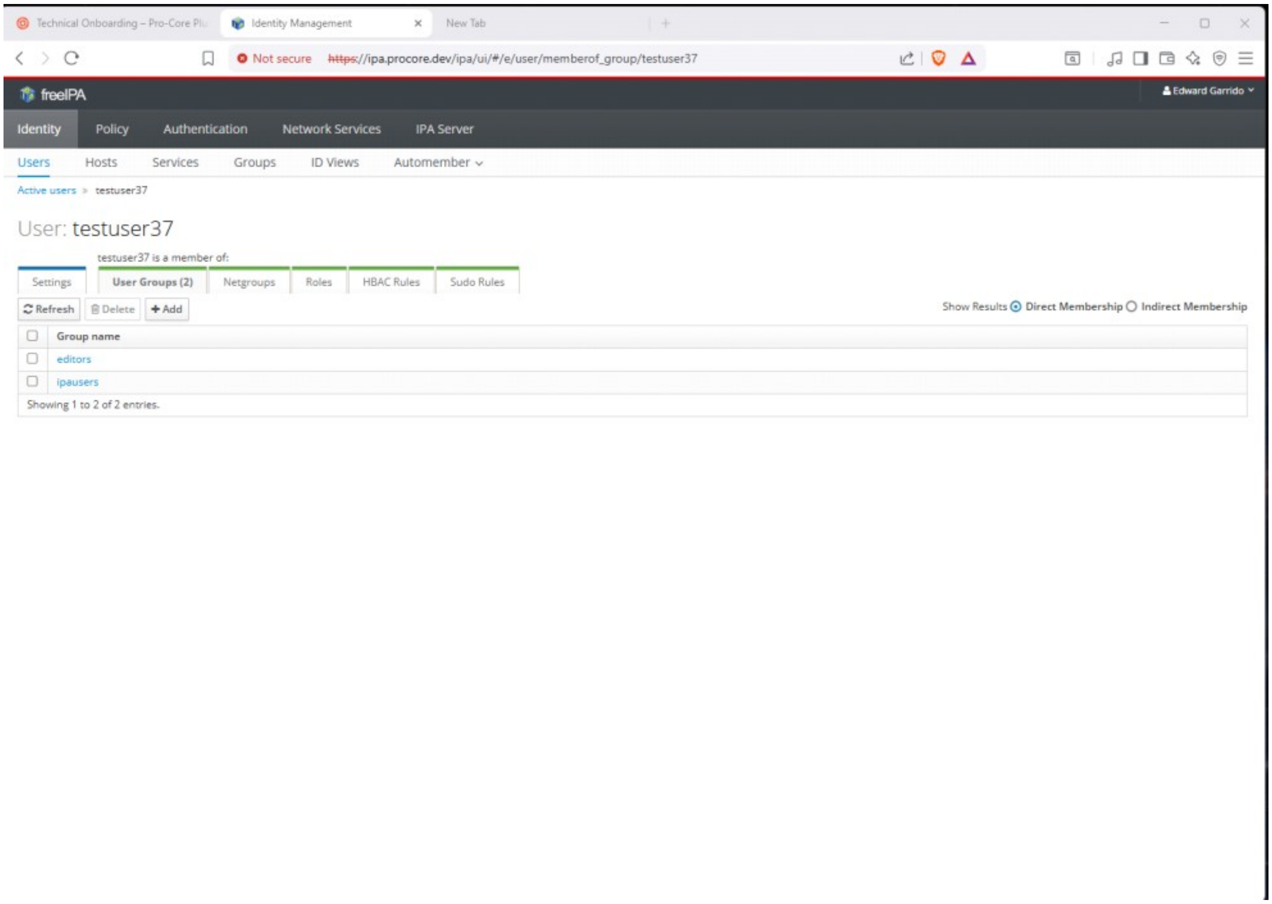
Available

□	Group name
□	admins
□	checkmk-admin
□	foreman_admins
□	procore_interns
□	ssogroups
□	support
□	sysadmins
□	trust admins
□	webmasters
□	wheel

Prospective

□	Group name
□	editors

I assigned the user to the ipausers and editors groups by clicking Add in the FreeIPA User Groups section.



https://ipa.procore.dev/ipa/ui/#/e/user/memberof_group/testuser37

Active users » testuser37

User: testuser37

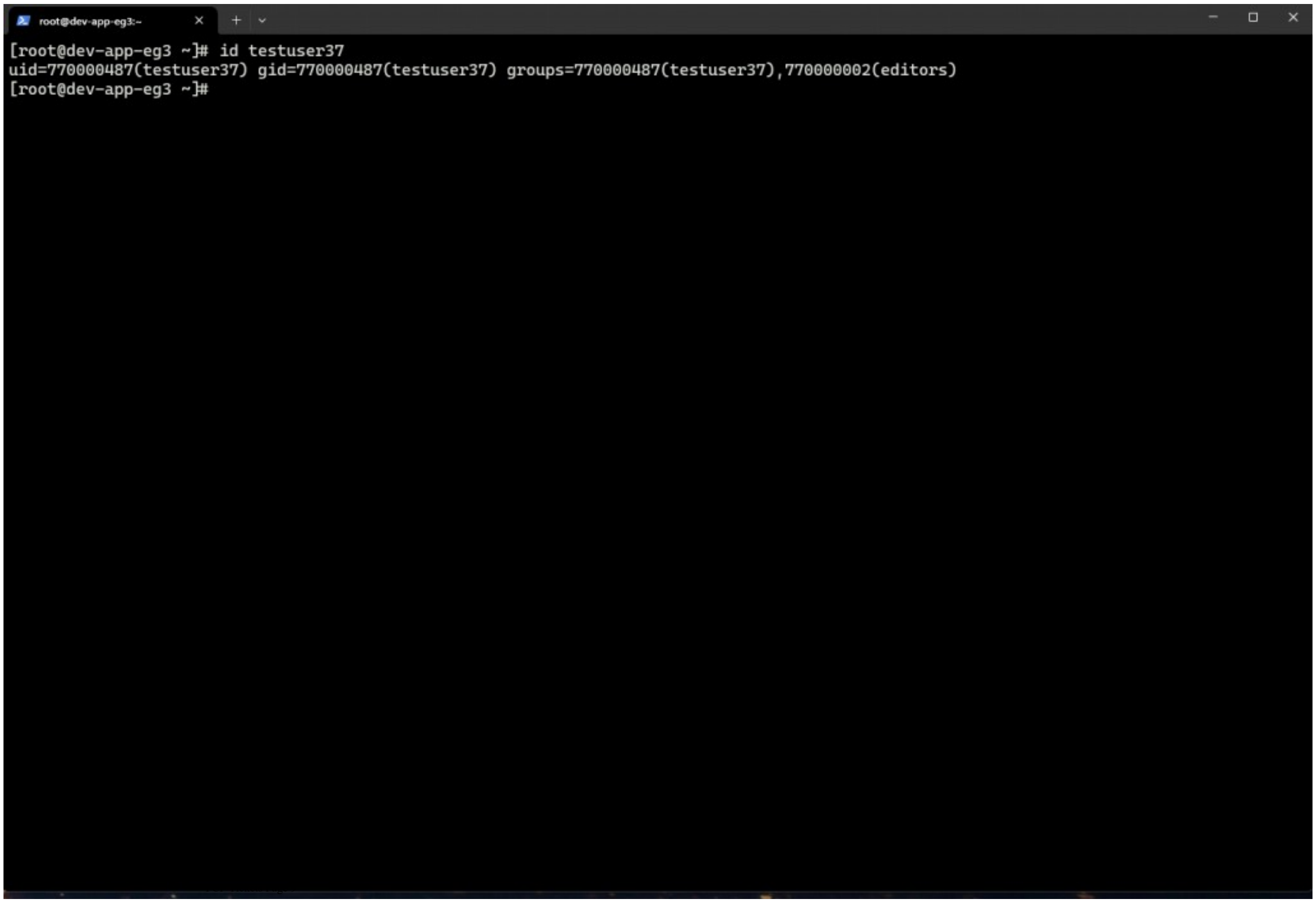
testuser37 is a member of:

Show Results ● Direct Membership ○ Indirect Membership

□	Group name
□	editors
□	ipausers

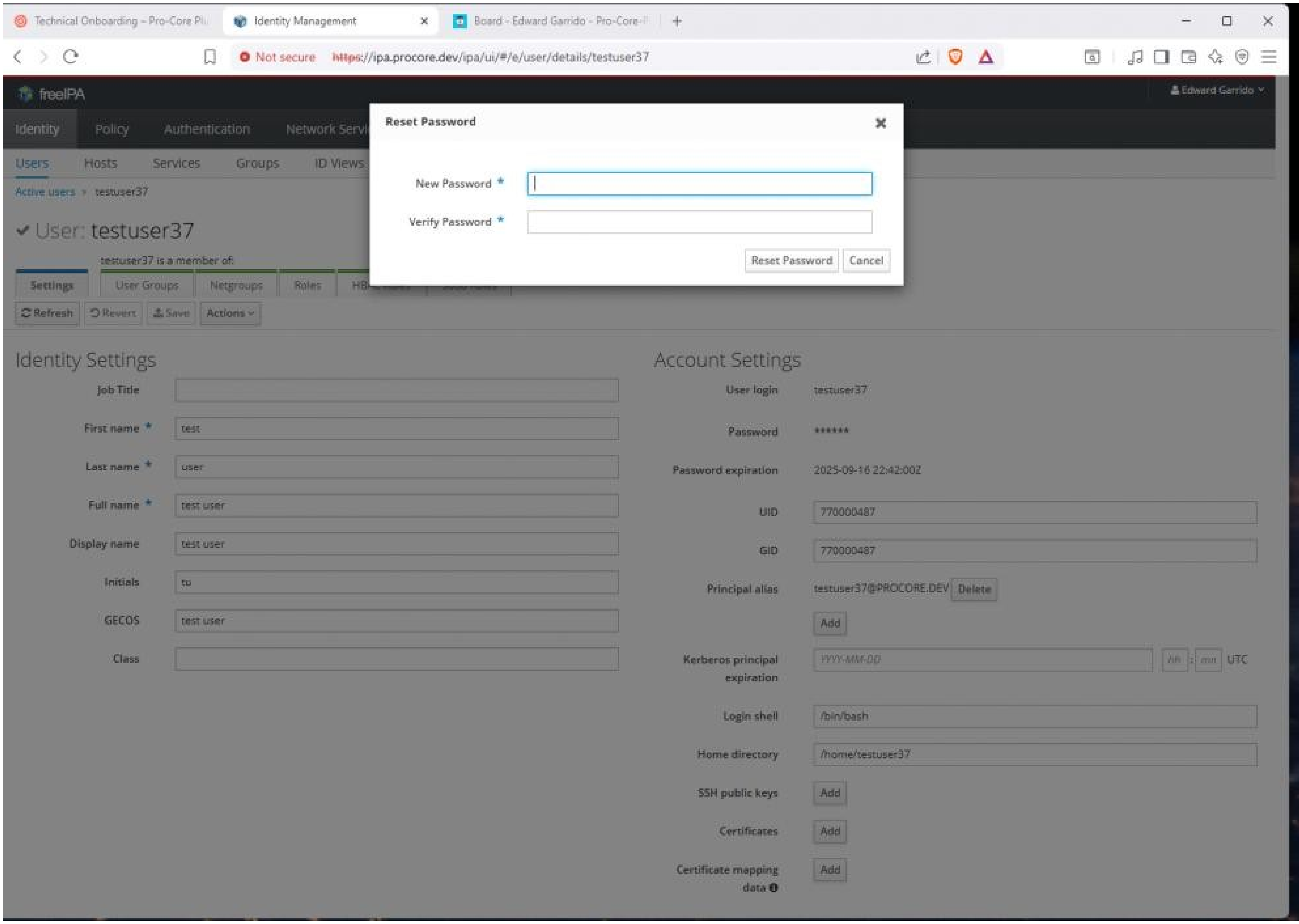
Showing 1 to 2 of 2 entries.

I verified the user’s group membership on the system using id, confirming the account is correctly associated with the editors group.



```
[root@dev-app-eg3 ~]# id testuser37
uid=770000487(testuser37) gid=770000487(testuser37) groups=770000487(testuser37),770000002(editors)
[root@dev-app-eg3 ~]#
```

I verified the user's group membership on the system using id, confirming the account is correctly associated with the editors group.



https://ipa.procore.dev/ipa/ui/#/e/user/details/testuser37

Reset Password

New Password *

Verify Password *

✔ User: testuser37

testuser37 is a member of:

Identity Settings

Job Title	
First name *	test
Last name *	user
Full name *	test user
Display name	test user
Initials	tu
GECOS	test user
Class	

Account Settings

User login	testuser37
Password	******
Password expiration	2025-09-16 22:42:00Z
UID	770000487
GID	770000487
Principal alias	testuser37@PROCORE.DEV
Kerberos principal expiration	YYYY-MM-DD hh : mm UTC
Login shell	/bin/bash
Home directory	/home/testuser37
SSH public keys	
Certificates	
Certificate mapping data	

Summary:

Installed FreeIPA Client

Installed ipa-client and required dependencies to prepare the system for centralized identity management.

Configured IPA Client Enrollment

Initiated ipa-client-install --mkhomedir and manually specified the IPA domain and server when DNS discovery was unavailable.

Firewall Configuration for IPA

Verified firewall settings and opened required TCP/UDP ports to allow FreeIPA communication.

Successful IPA Client Enrollment

Joined the system to the FreeIPA realm, configuring SSSD, Kerberos, LDAP, and SSH for centralized authentication.

Verified IPA Authentication

Confirmed Kerberos authentication with kinit, validated user/group resolution, and verified sudo access.

Created User in FreeIPA Web UI

Added a new user through the FreeIPA web interface for domain-wide identity management.

Assigned User to Default Group

Added the user to the ipausers group to grant standard domain access.

Added User to Additional Groups

Assigned the user to the editors group via the FreeIPA UI to provide elevated permissions.

Verified Group Membership on Client

Confirmed correct user and group assignment on the system using the id command.