



CalNet Deputy Training

CalNet (Kerberos) Authentication Services

CAL People and Computer Training
University of California, Berkeley

For more information about the CAL PACT program, to sign up for classes, or to download course documentation, please visit our website at: <http://calpact.berkeley.edu/>



Use this
space for notes

Introduction

The purpose of this course is to train you as a CalNet deputy so that you can activate CalNet accounts for faculty and staff in your department. As a departmental deputy, it is your duty to verify and activate a user's CalNet ID for members of your department or unit.

Requirements for this class

- Text editing
- How to use the mouse
- Basic computer skills, including experience with the Internet
- Submission of appropriate paperwork
- Necessary approvals from your department or unit and User & Account Services

Skills and concepts you will learn in this class

- What are CalNet and Kerberos?
- What is the difference between a personal principal and a deputy principal?
- Your responsibilities as a CalNet Deputy
- Activating personal principal accounts
- Issuing tokens
- Changing and resetting a passphrase

Conventions used in this document

Menus and menu commands are separated by a vertical bar (|). In the document they will appear as **Menu|Command**. An example of this is: “Select **File|New...**”

What is CalNet?

CalNet is a unified directory service and authentication infrastructure at UC Berkeley. The infrastructure can be used by applications for public directory services, lookups, authorization, and authentication.

What is Kerberos?

Kerberos is an authentication system, based on a centralized “trusted third party” that uses a database of identifiers and secret cryptographic keys. It allows people and services to prove their identities to each other reliably, even when the network over which they communicate is not itself secure.

Kerberos differs from some other authentication methods in that a single identifier and passphrase may be used to gain access to multiple services or applications. This identifier used by a person or service is known as a **principal name**. At UC Berkeley, the Kerberos authentication service is a component of the CalNet system. Accordingly, the principal name is also known as the **CalNet ID**.

Authentication

Authentication refers to the process by which one party determines the identity of another. On an insecure computer network where all traffic is potentially readable (and subject to tampering) by hostile parties, cleartext passwords can no longer be relied upon to provide assurance of identity. Consequently, protocols and software systems have been developed that allow people and processes to securely prove who they are even in the presence of network attackers and eavesdroppers. Kerberos is one such system.

Authorization

Authorization refers to the process whereby individuals are granted or denied access to services and resources. Some users are allowed more access than others. Applications must make these decisions, based on the identities of users after they have been authenticated. Kerberos is not involved with authorization; applications may use the CalNet Directory Services (which uses the LDAP protocol) to help them in the authorization process.

Deputy Principal and Personal Principal

Faculty and staff members (as well as students) have their own personal CalNet principals, or “CalNet IDs.” As a deputy, you also have a **deputy principal** that you will use to issue tokens as part of the activation process for staff and faculty.

IMPORTANT NOTE: Because your deputy principal is associated with additional privileges that other staff and faculty do not have, you should treat it as a separate identity from your personal CalNet ID. In particular, be sure to choose a different passphrase for your deputy principal than for your personal principal. For extra security, make sure that your deputy passphrase is not the same as **any** other password you may be using.

Note



Your deputy principal should have a different passphrase than your personal principal!

Note

In order to issue a token, you must be an authorized deputy.

Activating a New Account

Generating a Token

The first step in creating a new account for someone is to generate a **token** (temporary password) for the user. If you do not personally know the individual, you must verify their identity. Having the individual show a valid UCB employee ID and some sort of picture ID should be sufficient. Affiliates may also show their affiliate ID (such as a Visiting Scholar or Post Doc card), with their four-digit affiliate ID number they received at the User & Account Services office.

A token can be generated by going to the CalNet Gateway web page:

<http://calnet.berkeley.edu>

and selecting **Issue CalNet Token** from the “CalNet Deputies” menu on the left.

On the following page, enter the requested information and click on the **Generate token** button. This verifies that you are a deputy and that this principal (the faculty or staff ID) is currently in the CalNet system but inactive. The system will then produce a token, which is displayed on a web page in the browser window. Give the token to the faculty or staff member. One good way to do this is to print the page for the individual, *but do not write the CalNet ID on this page!*

Remind the individual that this is a sensitive passphrase and therefore should not be shared with anyone.



Issue Token

This page allows a departmental deputy to issue CalNet registration tokens to faculty, staff and affiliates. They will enter their tokens on another web page to activate their CalNet IDs.

In order to issue a token, you must be an authorized deputy. In the form below, you are asked to enter your Kerberos deputy principal (but without the **deputy** portion of the name, which is shown and will be included automatically), as well as the passphrase for that principal. Only if you are on the list of authorized deputies and you are authenticated successfully by Kerberos may you generate a token.

Before generating a token for an employee or affiliate, it is your responsibility as a deputy to identify the individual; in particular, to ascertain that the CalNet ID (employee or affiliate ID) for which you are generating a token actually belongs to the person to whom you will be giving the token.

Deputy Kerberos Principal: /deputy

Deputy Passphrase:

CalNet ID (employee or affiliate ID):

Using a Token to Activate an Account

The faculty or staff person in turn uses the token on the following web page:

<https://net-auth.berkeley.edu/cgi-bin/krbreg>

Once at the page, the user will type in their CalNet ID and their token. The individual will need to select a passphrase at this time.

The passphrase must meet the following criteria:

- A minimum length of 9 characters (maximum 255). It may also include blanks (which is why we call it a passphrase).
- It must contain AT LEAST three *different* character classes. The defined character classes are uppercase, lowercase, numbers, punctuation, and all other characters.
- It may not be the same as your CalNet ID name.
- If this is a passphrase reset, you will not be able to select a passphrase that is the same as the last one you had, or the one before that.

* If you don't have a CalNet registration token and are a faculty or staff member at UC Berkeley who wants to activate your CalNet ID, you should contact [User & Account Services](#) for further information.

Required Passphrase Characteristics:

- A minimum length of **9** characters (maximum 255). It may also include blanks (which is why we call it a *passphrase*).
- It must contain at least three *different character classes*. (The defined character classes are **uppercase, lowercase, numbers, punctuation, all other characters**).
- It must not be the same as your ID.
- (If this is a passphrase reset, you will not be able to select a passphrase that is the same as the last one you had, or the one before that).

CalNet ID (employee ID)

Token /

Choose your passphrase

Enter passphrase again

Don't forget your passphrase; you're the only one who knows it! If you do forget it, you must go to a [CalNet deputy](#), or to [User & Account Services](#), and present identification (including your employee ID), so that you can be issued a new token.

To activate your CalNet ID, click here

To clear all fields, click here

A new account user will have up to **three days** to complete this phase of the authentication process. After three days, the token expires and the entire account activation process must be repeated.

Here are two sample scenarios for activating a CalNet ID account:

1. You as the deputy print out the web page containing the token and give it to the faculty or staff member, who then has three days to visit the *Activate CalNet ID* web page (<http://net-auth.berkeley.edu/cgi-bin/krbreg/>) and supply the requested information there to create their passphrase. (If you don't have a printer attached to your computer, you may copy the token, expiration date and "Activate CalNet ID" page URL by hand and give it to the user. Do not write down their ID number on the same piece of paper. This helps prevent someone else from activating the account).
2. If you and the user so choose, the activation process can be done at your computer immediately after the token has been generated. In this case, it is advisable for you to open two browser windows, so that you can copy and paste the token from the page where it is first displayed into the appropriate locations on the Activate CalNet ID web page. After submitting the token, the user will choose a new passphrase as described above. *If you choose this method, be sure that you copy only numbers from the token, and not any of the leading or following spaces surrounding the token.*

Which of the above approaches you choose depends on the needs and desires of both yourself (the deputy) and the user. Because it may take several tries for some users to choose a valid passphrase, it may be preferable for the user to do this in the comfort and privacy of their own work environment.

On the other hand, if the user would prefer to do the activation right away, and the deputy is willing to take the time (for example, there is not a long line of other users waiting to be issued tokens), the second option above may be desirable.

As a deputy, it may be helpful to e-mail the passphrase requirements to individuals ahead of time so they can decide on a passphrase before coming to have their account activated.

Changing a CalNet ID

Once a user has activated their CalNet ID, they may choose to "self-select" (or "create") a more personalized CalNet ID (as opposed to their employee or affiliate ID number). This can be done by the user from the CalNet homepage by selecting *Change CalNet ID*. This can only be done once.

Changing a Passphrase

Users may change their passphrase at any time by selecting the *Change CalNet Passphrase* option from the CalNet Gateway page at:

<http://calnet.berkeley.edu/>

If a user tries to change their passphrase and receives an error message that their CalNet ID is expired, it's likely that they have self-selected a CalNet ID but have forgotten. If that's the case, and they cannot remember their self-selected CalNet ID, the user must contact a CalNet Deputy to have the deputy reset the user's passphrase.

The screenshot shows the 'Change Passphrase' web form. At the top is the CalNet logo. Below it, the title 'Change Passphrase' is centered. A paragraph explains the importance of a strong passphrase. A section titled 'Required Passphrase Characteristics:' lists four bullet points: minimum length of 9 characters, at least three different character classes, not the same as the user ID, and not the same as the current or previous passphrase. The form includes input fields for 'CalNet ID (this is your staff or student ID)', 'Current Passphrase or PIN', 'New Passphrase', and 'Enter New Passphrase Again'. At the bottom, there are two buttons: 'Change my CalNet Passphrase' and 'Clear this form'.

Resetting a Passphrase

If a person forgets their passphrase, you have the ability to reset their passphrase. This essentially deactivates their CalNet ID until you issue them a new token. You can do this by going to the *Reset CalNet Passphrase* page from the CalNet Gateway, or going directly to

<https://net-auth.berkeley.edu/cgi-bin/krbtoken?reset>

If a user has “self-selected” a new CalNet ID, you should enter *both* the user's employee ID number *and* self-selected CalNet ID to make sure that they match. If the user does not remember their self-selected CalNet ID, you may enter only the employee (or affiliate) ID and the system will look up the self-selected CalNet ID for you.

VERY IMPORTANT NOTE: Make sure you check and double-check that the ID you entered is correct before resetting the account. If you enter the wrong ID number, you will reset another individual's CalNet ID and they will be unable to use their account.

Additional Help for Users

If you will be away from the office for some reason, please refer individuals who need help with their accounts to User & Account Services (UAS) in room 206, Evans Hall. They are open from 10:00 a.m. to 4:00 p.m. weekdays. UAS will help them set up a new passphrase.

Help for CalNet Deputies

All CalNet deputies will be placed on an e-mail alias. This means that you will receive information and updates regarding the CalNet system. If you have questions about the account activation process or related issues, please contact User & Account Services. For questions regarding your role as a deputy or the CalNet system, please send an email to k5reg@berkeley.edu

CalNet Resources & Information

Main CalNet Page:

<http://calnet.berkeley.edu>

Current and Planned CalNet-enabled Applications at UC Berkeley:

Current: **https://calnet.berkeley.edu/current_apps.html**

Planned: **https://calnet.berkeley.edu/planned_apps.html**

User & Account Services:

<http://uas.berkeley.edu>

telephone: (510) 642-7355

fax: (510) 643-5385

email: accounts@socrates.berkeley.edu

location: 206 Evans Hall

hours: 10:00 a.m. - 4:00 p.m. (weekdays)

Kerberos V5 at UC Berkeley:

<http://www.net.berkeley.edu/kerberos/>