

EZACCESS

Table of Contents

| | |
|--|----|
| Preface | 3 |
| Introduction | 4 |
| Access Paths | 5 |
| Matrix of Alternatives | 5 |
| Path Properties | 6 |
| SecureNet | 6 |
| Internet | 7 |
| Open Terminal Server (OTS) | 10 |
| Access Techniques | 11 |
| Secure Shell (SSH) | 11 |
| File Transfer: FTP, NFT, or SCP | 12 |
| X Terminal Control: XHOST or XAUTH | 14 |
| Setting Up Server Authorization | 15 |
| Setting Up Client Authorization | 15 |
| Numerical Node Names at LC | 17 |
| Access Administration | 18 |
| Forms | 18 |
| Passwords | 19 |
| One-time Passwords (OCF and SCF) | 19 |
| Static Passwords (SCF) | 19 |
| Access Prerequisites | 20 |
| One-Time Password (OTP) | 21 |
| ID Verification by Stored Answers | 23 |
| Other Information Sources | 24 |
| Disclaimer | 25 |
| Keyword Index | 26 |
| Alphabetical List of Keywords | 27 |
| Date and Revisions | 28 |

Preface

- Scope:** EZACCESS provides basic information on the alternative paths by which users can reach Livermore Computing resources, the alternative techniques and tools (such as OTS, SSH, and VPN) available for using those access paths, and access administration help (such as password-policy summaries and password usage tips, pointers to authorization and identity-verification forms, and tips on finding additional basic user documentation relevant to computing at LC). A companion manual called the EZOUTPUT (URL: <https://computing.llnl.gov/LCdocs/ezoutput>) guide provides similar information about file transfers to and among LC machines. Technical instructions for dealing with LLNL's firewall and for using the more intricate access tools introduced here appear in a separate Firewall and SSH Guide. (URL: <https://computing.llnl.gov/LCdocs/firewall>)
- Availability:** When the programs described here are limited by machine, those limits are included in their explanation. Otherwise, they run under any LC UNIX system.
- Consultant:** For assistance, contact the LC customer service and support hotline at 925-422-4531 (open e-mail: lc-hotline@llnl.gov, SCF e-mail: lc-hotline@pop.llnl.gov).
- Printing:** The print file for this document can be found at
- OCF: <https://computing.llnl.gov/LCdocs/ezaccess/ezaccess.pdf>
SCF: https://lc.llnl.gov/LCdocs/ezaccess/ezaccess_scf.pdf

Introduction

EZACCESS is a basic user guide that describes alternative paths for reaching the Livermore Computing machines, alternative techniques and tools for taking advantage of those paths, and access administration fundamentals (such as the basic LC password policies and local usage techniques, along with authorization forms).

Several other LC user manuals address specific questions that newly arriving users often have:

- **FIREWALL.**
Technical instructions for dealing with LLNL's firewall, as well as using secure shell SSH, local variant XSSH, and Virtual Private Network VPN, appear in a separate manual called the Firewall and SSH Guide (URL: <https://computing.llnl.gov/LCdocs/firewall>).
- **STORAGE.**
Users concerned about accessing LLNL machines primarily to store project files or retrieve stored files should consult the EZSTORAGE (URL: <https://computing.llnl.gov/LCdocs/ezstorage>) basic guide.
- **LINUX.**
Users new to Linux or who want a careful comparison of Linux and AIX implementation features on LC production machines, can consult LC's Linux Differences (URL: <https://computing.llnl.gov/LCdocs/linux>) user guide.
- **ENVIRONMENT VARIABLES.**
Every UNIX computing system employs environment variables in its own peculiar way, and at LC, many additions to the standard variable set help handle resources or job-control issues unique to LC's large clusters. For a comparative analysis of environment variables on LC machines, see the Environment Variables (URL: <https://computing.llnl.gov/LCdocs/ev>) user manual.

Access Paths

This section compares the different access paths available and briefly explains the role and prerequisites for using each path.

Matrix of Alternatives

Your ability to reach LC machines depends on who you are, where you are located, and which machines (open or secure) you want to use. Consult the table below for your appropriate access method.

The table uses the following standard LLNL abbreviations:

- ASC: Advanced Simulation and Computing Program.
- LDRD: Laboratory Directed Research and Development.
- M&IC: Multiprogrammatic and Institutional Computing.
- OTS: Open Terminal Server.

Access Choices for LC Users, by Status and Location.

| Status and Location | SecureNet | Internet | OTS |
|-------------------------------------|-----------|----------|-----|
| LLNL Researcher | | | |
| On site: | | | |
| M&IC investors | | X | X |
| M&IC ad hoc | | X | X |
| LDRD proposals | | X | X |
| ASC work | X | X | X |
| Off site: | | | |
| M&IC investors | | X | X |
| ASC (at a DOE site) | X | X | X |
| Los Alamos or Sandia ASC Researcher | X | X | |
| Other DOE Sites | X | X | |
| ASC Strategic Alliance Users | | X | |

Path Properties

SecureNet

ROLE:

SecureNet is a computer network designed to safely transmit classified information, including Secret Restricted Data, exclusively among DOE sites. SecureNet lets you:

- connect to DOE sites only,
- connect to secure (classified) computers only,
- use gateway computers for enhanced security,
- access the network via SSH.

PREREQUISITES:

To use SecureNet from LLNL to connect to another DOE site, you must be authorized by your professional collaborator at that site, whether it is another laboratory (LANL or SNL) or an industrial site (e.g., Pantex). Only a host (target) site can issue you a login and password to use SecureNet to reach that site. For more information on using SecureNet from LLNL, go to this Web page:

https://computing.llnl.gov/access/content/securenet_info.php

You can use SSH (secure shell) from another SecureNet site to connect directly to a classified LLNL machine on which you have an LLNL account by supplying the full machine name, for example:

```
ssh um.llnl.gov
```

Details vary, however, depending on whether you have an account at LANL or SNL and want to "forward your credentials" to use an ASC LLNL machine, or if you want to use a non-ASC machine, which won't accept forwarded credentials, or if your user name differs at different SecureNet sites. For an explanatory matrix that shows how to handle these complex possibilities, see

<https://computing.llnl.gov/access/content/>

Internet

ROLE:

The Internet (off site) and Open LabNet (on site) are the default unclassified paths to and from all LC open machines, just as they are worldwide. (Note that in LLNL's SecureNet documentation, the Internet is always mysteriously called "the InterSite Network.") Thus ASC Strategic Alliance partners at non-DOE sites (such as universities and institutes) will routinely use the Internet to reach unclassified ASC machines located at LLNL. The Internet lets you:

- connect nonDOE sites with DOE sites,
- connect open (unclassified) computers only,
- support SSH (secure shell) as access software,
- TELNET into and between LC machines is disabled.

PREREQUISITES:

You can become authorized to use LC's unclassified computers (via the Internet) if you are either:

- an employee of a program that has invested in LC's hardware under the M&IC framework,
- an LLNL scientist who has an approved ad hoc research proposal,
- an LDRD researcher,
- officially collaborating with someone in the previous three categories, such as an ASC Strategic Alliance partner.

INSTRUCTIONS:

If you are eligible and want instructions on how to become an authorized user (i.e., on what forms to file), consult LC's Accounts page at

<https://computing.llnl.gov/accounts/content/>

or consult the Forms (page 18) section later in this document. If you are already authorized and want instructions on how to reach various LC unclassified machines using SSH, look for the specific login tables mixed with the classified instructions at the URL listed above.

INTERACTIVE USE:

Using the Internet to reach LC machines and services from offsite usually involves using a combination of VPN and SSH.

- SSH.
 - (1) The secure shell (SSH) is the only Internet *login* service that is allowed through the LLNL firewall and allows outside-the-firewall sites to access LC machines. Inward TELNET is not allowed. See also the Login section (page 11) below.
 - (2) All offsite users (except for LANL and SNL users who start from their own restricted ("yellow") network) must first run a VPN client to borrow an llnl.gov IP address before they can login to any LC machine. Timeouts apply; see details below.
 - (3) All offsite users (except LANL and SNL) must invoke SSH with port 922 to successfully connect to LC machines (use the -p 922 option, or set the port with the EDIT | PREFERENCES | CONNECTION chain of menus).
 - (4) LC machines only accept connections using the SSH version-2 protocol (which is the default protocol for all LC-provided SSH clients).
- VPN.
 - (1) A Virtual Private Network (VPN) allows outside-the-firewall machines, as well as any applications (i.e. Web browsers and FTP clients), to perform with the same privileges as a computer that is located inside the LLNL firewall.
 - (2) VPN use requires that you download and install a VPN client on your machine and then execute it during every VPN authenticated session. Your VPN client interacts with one of two LLNL VPN servers (vpna.llnl.gov or vpnb.llnl.gov) while it runs. VPN clients for Macintosh, Windows, and UNIX (Solaris and Linux) platforms are available to authorized LC users for free download from https://access.llnl.gov/vpn_access/ (URL: https://access.llnl.gov/vpn_access/), as noted in the table below.
 - (3) Only LLNL employee, contractors, and certain other ASC collaborators can establish an authorized VPN account, and a login ID and password (your token-generated one-time password) are required to run the VPN client. Paperwork and approvals are required, so contact the LC Hotline for more information.
 - (4) For more details on getting, installing, and configuring a VPN client, see LC's Firewall and SSH Guide (URL: <https://computing.llnl.gov/LCdocs/firewall>).
 - (5) VPN access requires Cisco's (VPN 3000) client (available from the URL cited in (2) above). VPN 3000 instructions, including troubleshooting tips, are at https://access.llnl.gov/vpn_access/vpn3000-moreinfo.html (URL: https://access.llnl.gov/vpn_access/vpn3000-moreinfo.html).

TIMEOUTS:

LLNL automatically disconnects a VPN session if either:

- (1) it remains *inactive* for 30 minutes, where "activity" includes incoming and outgoing traffic, e-mail checks, or Web page accesses (note that running jobs with reporting timesteps longer than 30 minutes could trigger this timeout), or
- (2) 12 hours elapse since you last *authenticated* the session. Reconnecting with VPN renews your 12-hour limit.

The table below summarizes the matrix of goals, personal status, and appropriate tools to help you make (and perhaps reevaluate later) the best access choices:

| Goal or Task | Personal Status | Access Tool(s) Needed |
|---|---|--|
| Reach public LLNL Web sites. | anyone | any web browser on any machine |
| Reach password-protected Web sites. | authorized VPN user | any web browser on any machine |
| Reach LLNL-only Web sites or sites without one-time passwords. | authorized VPN user | start VPN client locally, then login to an LC machine with SSH, then run browser there |
| Login to LC machines from outside llnl.gov | (1) SNL or LANL user (2) authorized VPN user | (1) Authenticate locally, then SSH (2) Start VPN, then run SSH port 922 |
| Transfer files to LC machines. locally, (including to storage.llnl.gov) | authorized VPN user | Start VPN client then use local FTP to PUT files to LC |

See LC's [Firewall and SSH Guide](https://computing.llnl.gov/LCdocs/firewall) (URL: <https://computing.llnl.gov/LCdocs/firewall>) for local implementation, installation, configuration, and usage details on the specialized tools introduced here.

Open Terminal Server (OTS)

The OTS service is a dial-up networking solution for LLNL employees that allows remote access to LLNL and may be used if high-speed connectivity is unavailable while at home or on travel. Non-UC/LLNL employees (e.g., SLOs and remote collaborators) may use this service, but they must obtain LLNL CSP approval. Please contact your OISSO for more information.

PREREQUISITES:

- A valid LLNL cost (recharge) account number.
- A valid LLNL e-mail name and address.
- An LLNL-issued one-time password (OTP) token (page 21).

<https://access.llnl.gov/ots>

For more the most up-to-date information on the using the Open Terminal Server, including account information and setup, please see https://access.llnl.gov/ots_access/brief.html (URL: https://access.llnl.gov/ots_access/brief.html).

Access Techniques

Secure Shell (SSH)

LC supports one primary software tool—SSH or the "secure shell"—for network access to LC production machines. SSH provides strong authentication and protected communication, even over unsecure networks, but it demands considerable customization to use.

SSH TIPS.

Most users will need detailed localized instructions to start using SSH effectively. Furthermore, these instructions vary depending on your LC target host (e.g., common home directories make a difference) and whether you work in the open (OCF) or secure (SCF) environments. A concise but thorough SSH overview, including role, annotated setup steps, basic execute lines, and troubleshooting tips, is available in the second half of LC's Firewall and SSH Guide (URL: <https://computing.llnl.gov/LCdocs/firewall>). This manual is posted on both the open and secure LC documentation Web servers. One section explains how to enable local display of output from X-Windows programs that run remotely on LC machines (called SSH X11 forwarding). There is also a MAN page for SSH and SCP on each LC machine that supports these programs (see also the summary in the Internet section (page 7) above).

USAGE RESTRICTIONS.

Note that (1) all Internet remote-access sessions connecting from external machines to LLNL machines now have a 2-hour timeout (page 7), and (2) only the SSH version-2 protocol is supported on LC machines.

File Transfer: FTP, NFT, or SCP

Transferring files between machines is a common need and LC's EZOUTPUT (URL: <https://computing.llnl.gov/LCdocs/ezoutput>) guide addresses this need in thorough, systematic, but basic terms, complete with instructions and annotated examples. This section does not attempt to summarize everything in EZOUTPUT but alerts you to the primary file-transfer issues and tools important for practical success in LC's computing environment.

FTP: General File Transfers.

FTP is the most well-known and generally supported file-transfer utility, and FTP clients and (server) daemons are available on all LC production and special-purpose machines in both the open and secure environments. With two exceptions, personal passwords are required when you use FTP (see the Passwords (page 19) section for which ones):

(1) STORAGE. FTP is also the standard interface to the LC archival file-storage system (both open and secure). But when you run FTP (on an OTP-passworded LC machine) with STORAGE as the target host, access is "preauthenticated" and you are NOT prompted for your password.

Firewall alert: LC uses its firewall to block direct FTP connections from machines outside the llnl.gov domain to LC machines within llnl.gov. Offsite users must FTP outward after logging on to an LC machine, or LLNL badgeholders can arrange to use inward FTP after first initiating a VPN connection from their outside machine. See the Firewall and SSH Guide (URL: <https://computing.llnl.gov/LCdocs/firewall>) for detailed instructions on installing and using VPN to enable inward FTP for authorized users.

NFT: Locally Enhanced Transfers.

Available on all LC production machines, NFT is a locally developed file transfer tool. Although NFT uses standard FTP daemons to carry out its file transfers, it offers enhanced features, such as transfer between two remote machines without being logged in to either one, "persistent" transfer even if the receiving machine has temporary problems, and preauthenticated (passwordless) file transfer. NFT's default settings also facilitate reliably transferring files to or from archival storage. Basic NFT instructions appear in EZOUTPUT (URL: <https://computing.llnl.gov/LCdocs/ezoutput>), while the NFT Reference Manual (URL: <https://computing.llnl.gov/LCdocs/nft>) gives complete details.

SCP: Encrypted File Transfers.

Available on machines where the secure shell (SSH) has been installed and enabled is a secure (encrypted) version of the remote copy (RCP) utility called SCP. SCP is not limited to just LC's own "secure network," and it improves file-transfer safety most when transferring files on the open Internet. SCP is sessionless, so there's no overt log-in to the remote machine, but it does require your one-time password

for authentication. Unlike FTP, you cannot use SCP to store files or to contact the "file interchange service" (FIS, below), in either the open or secure environments at LC. For comparative execution details with FTP and NFT, see EZOUTPUT (URL: <https://computing.llnl.gov/LCdocs/ezoutput>).

FIS: Open/Secure Transfers.

FIS is LC's "file interchange service" between its open and secure networks. LC's open and secure networks are physically isolated from each other, but you can transfer files between them by using FTP and two specially designated transfer nodes. For example, to transfer from the OCF to SCF, FTP the file(s) to the outbound directory of the OCF transfer node. Next, an LC operator moves the file(s) on tape between networks, and then you retrieve the file(s) (via FTP) from the inbound directory of the SCF's transfer node. Authorized Derivative Classifier review of all secure-to-open file transfers is required (as is use of your open and secure one-time passwords), and you cannot use NFT or SCP. For the necessary administrative as well as technical instructions, see EZOUTPUT (URL: <https://computing.llnl.gov/LCdocs/ezoutput>) or consult the FIS Reference Manual (URL: <https://computing.llnl.gov/LCdocs/fis>).

Common Home Directory "Transfers."

On most LC machines, your UNIX home directory is a shared or "common home" directory. Placing a file in the common home directory eliminates the need to overtly transfer it between machines using FTP or NFT because it automatically appears to reside on all the machines that share that directory. Disk-space quotas and Network File Systems (NFS) side effects apply. Basic advice on using common home directories appears in the EZFILES (URL: <https://computing.llnl.gov/LCdocs/ezfiles>) guide, while the full analysis of their benefits and limits is in the Common Home Reference Manual (URL: <https://computing.llnl.gov/LCdocs/chome>). Never perform massively parallel I/O to your common home directory (it slows traffic for users on *all* machines.)

HTAR: Transferring TAR Files Efficiently.

HTAR is a locally developed, special-purpose transfer tool that efficiently moves files into or out of TAR-format archives (library files) either in the OCF or SCF storage systems or on other LC hosts, even when the files or archives are very large. See the HTAR Reference Manual (URL: <https://computing.llnl.gov/LCdocs/htar>) for a thorough discussion of HTAR's helpful but very specialized file-transfer role.

X Terminal Control: XHOST or XAUTH

For an X client (such as the TotalView debugger) to display on an X-display server (such as your X terminal or workstation), the client must be authorized to connect to the server. XHOST and XAUTH offer alternative ways to manage this authorization.

Many users run the XHOST utility on the server machine to authorize X clients running on a specified host to connect to the server. This method is called host-based access control. It poses inherent security problems: any user on the specified host can access your display, and indeed any user can capture all your keystrokes too. Running

```
xhost +yana3.llnl.gov
```

for example, authorizes several hundred users on YANA3 to connect to your server. The reverse is also true. Running

```
xhost -yana3.llnl.gov
```

prevents every user on YANA3 from connecting to your X server, including yourself.

LC recommends that you use a user-based, rather than a host-based, access control method. User-based access control avoids most of the security deficiencies present with host-based access control. The most common user-based access control method is called MIT-MAGIC-COOKIE-1. This method of user-based access control requires two steps. First, the .Xauthority file in your server's home directory must be set up and supplied with the magic cookie. Second, the .Xauthority file in the remote machine's home directory must be established and given the same cookie. Fortunately, many LC production computers share common home directories. This gives you the convenience of setting up just one .Xauthority file in your common home directory that allows you to open windows on your display from clients running on any of the remote hosts that share that directory.

XAUTH is a utility program that manipulates these .Xauthority files (examples follow). Running XAUTH with no options returns an `xauth>` prompt. You can respond with a question mark to see a list of XAUTH commands, or type

```
help command
```

to get information on a specific command.

WARNING: host-based access control (with XHOST) overrides user-based access control (with XAUTH). If you have used XHOST to declare a whole host's access to your X server, then all users on that host can access your server even if you also implement magic cookies by running XAUTH.

Setting Up Server Authorization

Launch the X-window using either XDM (X display manager) or XINIT. The program your system uses determines how much work, if any, you need to do to set up user-based authorization on your server machine.

If you are using XDM, the X server is always running, and you start your individual X session by logging in via a dialog box. User-based access control is built into the XDM control protocol. This means that the `.Xauthority` file will automatically be set up for you and the magic cookie will be communicated with your server when you log in. You can skip to the next section.

If you are using XINIT, you may have to set up authorization on the server machine yourself. Some window managers, such as OpenWindows, do this for you. If you have a `.Xauthority` file in your home directory on the server machine, then authorization was probably set up for you. If your home directory lacks a `.Xauthority` file, you can create one using XAUTH. First, you must create a pseudorandom number to be used as the magic cookie code. This should consist of an even number of hexadecimal digits. One method of generating a suitable magic cookie is with:

```
cookie='echo "(obase=16;$$^3)" | bc'      [Korn/Bourne shell]
set cookie='echo "(obase=16;$$^3)" | bc' [C shell]
```

You can add this magic cookie to the `.Xauthority` file by running XAUTH twice:

```
xauth add $(HOST)/unix:0 . $cookie
xauth add $(HOST):0 . $cookie
```

Then you must start the X server using this code, which can be done by running XINIT with a special argument:

```
xinit -auth $HOME/.Xauthority
```

Setting Up Client Authorization

After setting up server authorization (see previous section), you must set up the corresponding `.Xauthority` file on each remote machine where you will be running X clients. First, use XAUTH on your server (here `xyz.llnl.gov`) to list the contents of your `.Xauthority` server file, extract the magic cookie code, and place it in a new file (here called AUTHFILE) for exporting to remote client machines:

```
xauth list
xyz.llnl.gov:0 MIT-MAGIC-COOKIE-1
e471b4f5a9ed8674fe38bcd2b01f8ab9
xyz/unix:0 MIT-MAGIC-COOKIE-1
e471b4f5a9ed8674fe38bcd2b01f8ab9
xauth extract authfile xyz.llnl.gov:0
```

Next, move AUTHFILE to the remote machine(s) and place it in your home directory (using FTP). If a `.Xauthority` file does not already exist there, you can just rename (MV) your AUTHFILE

to .Xauthority. If .Xauthority already exists, merge the two files by running XAUTH on the remote machine:

```
xauth merge authfile
```

If for some reason you cannot FTP your extracted cookie file (here AUTHFILE) to the remote machine, you can run XAUTH on the remote machine and add the cookie by hand using an execute line of this form (cut and paste the cookie string to avoid errors):

```
xauth add xyz.llnl.gov:0 e471b4f5a9ed8674fe38bcd2b01f8ab9
```

Your X clients on the remote machine can now authorize themselves to display on your X server (here xyz.llnl.gov).

Remember too that many LC production computers share common home directories. Setting up one .Xauthority file in your common home directory allows you to open windows on your display from clients running on any of the remote hosts that share that directory, without further use of XAUTH.

Numerical Node Names at LC

Some LC machines or cluster nodes have all-character names, but often the number of names needed calls for using digits instead of just characters (e.g., YANA25). Numerically naming the nodes of a massively parallel computer (or of a many-noded cluster) poses subtle problems, however, if not handled with a consistent, foresighted policy regarding:

- The start digit (0 or 1?),
- The use of leading zeros (is a single-digit node called 3 or 03?), and
- The numerical range of available nodes (is it 0 to 31, or 1 to 32?).

At LC, all such node-naming decisions have been ad hoc so that even machines with the same hardware or the same operating system (Linux) may have different node-naming schemes. Hence, numerical node names here vary in regard to all three features above.

For example, UM has a start digit of 001 with leading zeros and ranges from 001–128. Atlas has a start digit of 0 and Yana's is 1, but neither uses leading zeros. For more information on LC's Numerical Node Names:

OCF

https://computing.llnl.gov/resources/content/OCF_resources.php (URL: https://computing.llnl.gov/resources/content/OCF_resources.php)

SCF

https://computing.llnl.gov/resources/content/SCF_resources.php (URL: https://computing.llnl.gov/resources/content/SCF_resources.php)

For interactive log on, some LC machines with leading-zero node names use a single generic name (up, uv, um, thunder) that automatically assigns you randomly to one of the available log-on nodes (without your having to specify the leading zeros).

Access Administration

Forms

At LC, every significant administrative change (new users, new user groups, new privileges, new FIS access) requires a paper form. And these forms require appropriate, original authorizing signatures (usually division-leader level) along with the usual identifying information. Send or deliver completed forms requesting new or changed computing service to:

LC Hotline
B-453, L-63
LLNL, P. O. Box 808
Livermore, CA 94551

LC administrative forms are available in two ways:

(1) From the LC Hotline.

Since which form to use or how to correctly complete the form is sometimes less than obvious, visiting the Hotline office or calling the Hotline staff (925-422-4533) to discuss your administrative needs often proves the most practical approach to handling LC forms.

(2) From the Web.

You can use any Web browser to access the LC Forms page at:

<https://computing.llnl.gov/?page=forms>

Passwords

Open and secure passwords are never the same, even when the authentication mechanism is the same. If you use a variety of LC machines, password management requires careful attention.

One-time Passwords (OCF and SCF)

OCF and SCF users (except for LANL and Sandia) authenticate via an OTP token and PIN. The LC Hotline will send you an OTP token when you are given an account. An OTP token is a small, key fob-like device that generates random 6-digit numbers. When you receive your OTP token, you must enable it before you can log in. Instructions are provided with your account notification e-mail and can also be found at https://access.llnl.gov/otp_access/ (URL: https://access.llnl.gov/otp_access/). The same OTP token is used for both OCF and SCF; however, a different PIN is used for each network.

OTPs are also used for other services, such as access to restricted Web pages and remote (off-site) access accounts.

Under certain circumstances, an OTP server may lose track of the values it expects from a particular token. In such cases, it is necessary to enter two consecutive token codes so the server can resynchronize itself. This can be done at [OTP Token Diagnostics](https://access.llnl.gov/otp_access/cgi-bin/otpdiaq.cgi) (URL: https://access.llnl.gov/otp_access/cgi-bin/otpdiaq.cgi). If a token is locked out, you can unlock it at [Test My OTP Token](https://access.llnl.gov/otp_access/cgi-bin/test_otp.cgi) (URL: https://access.llnl.gov/otp_access/cgi-bin/test_otp.cgi).

Static Passwords (SCF)

Currently, SCF users may authenticate via a static password (8-character machine-generated) instead of an OTP. These passwords expire every six months. SCF static passwords can be changed online on the SCF at <https://lc.llnl.gov/bin/passwd/>. Lockouts can occur when a password is entered incorrectly too many times. The lock is released after 15 minutes. If multiple lockouts occur, your account may be permanently locked. You must obtain a new password from the LC Hotline (walk-in or certified mail) if your password expires or you become permanently locked out.

NOTE.

Static SCF passwords will be discontinued in the near future, and only authentication via OTP will be allowed.

Access Prerequisites

The table below lists the different methods you can use connect to both open and secure machines.

| Going to —> Coming From | OCF Inside LLNL | OCF LANL/ Sandia | OCF Other DOE | SCF Inside LLNL | SCF LANL/ Sandia | SCF Outside LLNL |
|---|--------------------------------|---------------------------------|------------------------------|--------------------------------|---------------------------------|---------------------------------|
| Valid account on the LC machine(s) you wish to use (see the Accounts Web pages) | x | x | x | x | x | x |
| - | | | | | | |
| Network connectivity from your local machine to the LC OCF or SCF network | x | x | x | x | x | x |
| - | | | | | | |
| SSH (version 2) software installed on your local machine (see Using SSH below) | x | x | x | x | x | x |
| - | | | | | | |
| One-time Password (OTP) token and PIN* (see Passwords below) | x | | x | x | | x |
| - | | | | | | |
| Virtual Private Network (VPN) account and VPN software (see VPN Access below) | | | | | | x |
| - | | | | | | |
| Ability to authenticate locally with credential forwarding (kinit-f) | | x | | | x | |

One-Time Password (OTP)

BACKGROUND.

To comply with DOE Order 205.1, LC implemented "two-factor" authentication for its open systems (and their passworded services, such as storage and FIS). Two-factor authentication replaced the traditional password, which was reusable over long periods of time but vulnerable to outside detection, with a series of single-use passwords each comprised of:

- A long-term personal identification number (PIN) combined with
- An random string of digits, or "token string," generated by a proprietary electronic device, such as the RSA SecurID token provided by LC.

The LC Hotline provides each new user with their own OTP token and an instruction sheet for getting a PIN and activating OTP service at a designated LC web site.

For more information, see the OTP pages at http://access.llnl.gov/otp_access (URL: http://access.llnl.gov/otp_access).

USING ONE-TIME PASSWORDS (OTP).

Your OTP consists of two strings without spaces:

ppppptttttt

where

pppp is your PIN, a user-selected string between 4 and 8 digits long (like the ATM PIN at your bank)

ttttt is the 6-digit token string currently displayed on your OTP token. At LC, the token string changes every 30 seconds and can only be used once.

Use your OTP just exactly as you would use a standard password string; there is no extra step(s), no special gateway to visit, and no keying anything on the token itself. When you get your token, the LC Hotline provides a current list of LC systems and services that accept OTP (for example, open FIS and OTS do exclusively, and offsite access using VPN does also).

COUNTDOWN FEATURES.

To help you manage the constantly changing 6-digit token strings (*ttttt*) the OTP token's screen also displays several countdown features:



At the lower right is a blinking dot that flashes once each second. Along the left edge is a stack of short horizontal bars. When 5 bars are displayed, that means the token number will change in approximately 30 seconds. With 25 seconds left, the token shows 2 bars, 15 seconds with 1 bar, and 5 seconds with zero bars.

RECOVERY FROM PROBLEMS.

You can give yourself more flexibility in recovering from OTP login problems during remote access if you "enroll" in LC's optional identity-verification service in advance, as described in a later section. (page 23)

ID Verification by Stored Answers

Open LabNet and Livermore Computing jointly offer an option to store answers to preselected questions (sometimes called "questions on file" or "answers on file") so that users can verify their identity independently of their passwords. Users who have already stored such answers and who later need to

- reset their OPT PIN when they forget it, or
- unlock their OTP token when it locks because of too many failed login attempts (especially during remote access)

can perform these functions for themselves at a special Web site after they successfully verify their identity by matching their current answers with their previous answers to five questions on an interactive form.

The URL for this (open network) emergency identity-verification service is (note the 's' in https and the uppercase A):

<https://access.llnl.gov/cgi-bin/newAnswer.cgi>

To use this service:

(1) Open the URL above with your Web browser. After authenticating, you will be offered a list of 30 possible questions, from which you must select five (5). The questions ask about the names of various relatives (youngest aunt on your mother's side, etc.) or places from your past (school locations, etc.).

(2) Click on the check box for each of the 5 questions that you want to use for ID verification.

(3) Click on the SUBMIT button.

(4) On the next page:

(A) Insert your answer text string for each question into its corresponding text-input box. Note that you can insert *any* string you choose; some cautious users intentionally insert a "secret string" for every answer to decrease the likelihood that an attacker could guess any answer from background knowledge about them.

(B) Click on the SUBMIT button.

The Web site will tell you that your response has been saved and confirm the storage of your answers. In the future, if you can repeat these answers to these questions when prompted after an OTP access problem, you can then perform the OTP management or recovery tasks noted above. If you still have problems logging in, you can also call the LC Hotline as usual.

Other Information Sources

SHORT TERM.

Short-term announcements are generally shared either through the "message of the day" (MOTD), which appears on your terminal just after you log in to a specific LC machine, or through NEWS items. A list of unread NEWS items (that is, the file names for unread NEWS postings) appears when you log in. To read a particular item (or, optionally, save it to a local file), use the execute line

```
news newsfile[>myfile]
```

An archive of old NEWS items is available to Web browsers on the open network at <https://lc.llnl.gov/computing/news> (URL: <https://lc.llnl.gov/computing/news>) (but your open OTP is required for access to this secure server).

LONG TERM.

LC provides a variety of user documentation online, including software manuals and user guides that are locally developed to meet LLNL needs, locally adapted documents from other sites, or locally relevant standard publications from vendors. Most LC documentation is now delivered on the Web either directly as Web pages or indirectly as PostScript or PDF files. Among the most useful URLs for finding or surveying LC-relevant documentation are these:

- Livermore Computing Documentation—includes (or links directly to) a subject list of local manuals, an alphabetical list of local manuals, a (reverse) chronological list of LC documentation announcements, and an archive of LC Technical Bulletins.
OPEN: <https://computing.llnl.gov/> (URL: <https://computing.llnl.gov/>) [fine-grained topics]
OPEN: <https://computing.llnl.gov/LCdocs/> (URL: <https://computing.llnl.gov/LCdocs/>) [whole manuals]
SCF: <https://computing.llnl.gov/LCdocs/> (URL: <https://computing.llnl.gov/LCdocs/>)
- Supported Software and Computing Tools—a tabular guide to the software maintained by LC's Development Environment Group and to the documentation that supports that software.
OPEN: https://computing.llnl.gov/code/content/software_tools (URL: https://computing.llnl.gov/code/content/software_tools)
SCF: https://computing.llnl.gov/code/content/software_tools (URL: https://computing.llnl.gov/code/content/software_tools)

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government thereof, and shall not be used for advertising or product endorsement purposes.

(C) Copyright 2007 The Regents of the University of California. All rights reserved.

Keyword Index

To see an alphabetical list of keywords for this document, consult the next section (page 27).

| Keyword | Description |
|-------------------------------|--|
| <u>entire</u> | This entire document. |
| <u>title</u> | The name of this document. |
| <u>scope</u> | Topics covered in EZACCESS. |
| <u>availability</u> | Where these programs run. |
| <u>who</u> | Who to contact for assistance. |
| <u>introduction</u> | Role and goals of EZACCESS. |
| <u>access-paths</u> | Three alternative paths compared. |
| <u>path-chart</u> | Paths listed by user status, location. |
| <u>path-properties</u> | Characteristics of each access path. |
| <u>securenet</u> | Classified network access. |
| <u>internet</u> | Open network access (SSH, IPA, VPN). |
| <u>ots</u> | Terminal-server (dial-up) access. |
| <u>access-techniques</u> | Access-supporting software compared. |
| <u>login</u> | How to log in with SSH. |
| <u>ssh</u> | How to log in with SSH. |
| <u>x-terminals</u> | Two X-terminal access approaches. |
| <u>x-server-authorization</u> | XAUTH server set up tips. |
| <u>x-client-authorization</u> | XAUTH client set up tips. |
| <u>node-names</u> | Numerical node names at LC. |
| <u>access-administration</u> | Administrative access issues. |
| <u>forms</u> | Fifteen access-support forms. |
| <u>passwords</u> | Local LC password rules. |
| <u>password-map</u> | Which system uses which passwords. |
| <u>access-prerequisites</u> | Requirements for logging into servers. |
| <u>otp</u> | Usage tips for one-time passwords. |
| <u>one-time-passwords</u> | Usage tips for one-time passwords. |
| <u>id-verification</u> | "Answers on file" to confirm identity. |
| <u>info</u> | Other LC documentation sources. |
| <u>index</u> | The structural index of keywords. |
| <u>a</u> | The alphabetical index of keywords. |
| <u>date</u> | The latest changes to EZACCESS. |
| <u>revisions</u> | The complete revision history. |

Alphabetical List of Keywords

| Keyword ----- | Description ----- |
|-------------------------------|--|
| <u>a</u> | The alphabetical index of keywords. |
| <u>access-administration</u> | Administrative access issues. |
| <u>access-paths</u> | Three alternative paths compared. |
| <u>access-prerequisites</u> | Requirements for logging into servers. |
| <u>access-techniques</u> | Access-supporting software compared. |
| <u>availability</u> | Where these programs run. |
| <u>date</u> | The latest changes to EZACCESS. |
| <u>entire</u> | This entire document. |
| <u>file-transfer</u> | Three file-transfer tools. |
| <u>forms</u> | Fifteen access-support forms. |
| <u>id-verification</u> | "Answers on file" to confirm identity. |
| <u>index</u> | The structural index of keywords. |
| <u>info</u> | Other LC documentation sources. |
| <u>internet</u> | Open network access (SSH, IPA, VPN). |
| <u>introduction</u> | Role and goals of EZACCESS. |
| <u>login</u> | How to log in with SSH (TELNET blocked). |
| <u>node-names</u> | Numerical node names at LC. |
| <u>one-time-passwords</u> | Usage tips for one-time passwords. |
| <u>otp</u> | Usage tips for one-time passwords. |
| <u>ots</u> | Terminal-server (dial-up) access. |
| <u>password-map</u> | Which system uses which passwords. |
| <u>passwords</u> | Local LC password rules. |
| <u>path-chart</u> | Paths listed by user status, location. |
| <u>path-properties</u> | Characteristics of each access path. |
| <u>revisions</u> | The complete revision history. |
| <u>scope</u> | Topics covered in EZACCESS. |
| <u>securenet</u> | Classified network access. |
| <u>ssh</u> | How to log in with SSH. |
| <u>title</u> | The name of this document. |
| <u>uinfo</u> | Reporting LC personal profiles. |
| <u>who</u> | Who to contact for assistance. |
| <u>x-client-authorization</u> | XAUTH client set up tips. |
| <u>x-server-authorization</u> | XAUTH server set up tips. |
| <u>x-terminals</u> | Two X-terminal access approaches. |

Date and Revisions

| Revision Date ----- | Keyword Affected ----- | Description of Change ----- |
|---------------------------|---|--|
| 12Aug08 | <u>internet</u> <u>x-terminals</u> <u>ots</u> <u>passwords</u> <u>uinfo</u> | Old IPA information deleted. Old MacX information deleted. OTS section condensed and revised. Kerberos sections deleted. Personal Profile information deleted. |
| 13Sep07 | <u>login</u> <u>internet</u> <u>index</u> | Old TELNET comparisons deleted. Old TELNET information deleted. Separate SSH keyword added. |
| 05Jun07 | <u>node-names</u> <u>password-map</u> <u>kerberos</u> <u>index</u> | ATLAS added to chart. Kerberos replaces DCE throughout. Kerberos replaces DFS/DCE credentials. Kerberos, DCE sections combined. |
| 26Feb07 | <u>login</u> <u>x-terminals</u> <u>node-names</u> <u>passwords</u> | SC references deleted. YANA replaces MCR examples. SC, ILX, MCR, GPS deleted. All Compaq references deleted. |
| 13Nov06 | <u>uinfo</u> <u>otp</u> | How LDAPSEARCH supplements UINFO. Details updated. |
| 05Sep06 | <u>internet</u> | VPN, IPA inactivity timeout now 30 min. |
| 02Aug06 | <u>internet</u> <u>file-transfer</u> <u>node-names</u> <u>info</u> | White references replaced. Home dir parallel I/O warning added. White references replaced. URLs for SCF updated. |
| 10May06 | <u>login</u> <u>x-terminals</u> | Cross ref on X11 forwarding added. Cross ref on X11 forwarding added. |
| 18Apr06 | <u>introduction</u> <u>node-names</u> | Cross refs reorganized, expanded. Details updated, BG/L added. |
| 18Oct05 | <u>securenet</u> <u>internet</u> | Support URLs updated. Support URLs updated. IPA very rarely allowed now. VPN 3000 replaces VPN 5000 client. |
| 13Sep05 | <u>internet</u> <u>login</u> | Only SSH version-2 protocol now. Only SSH version-2 protocol now. |
| 16Jun05 | <u>internet</u> <u>node-names</u> <u>passwords</u> | IPA scope, time limits restricted. Adelie, Emperor no longer GA. B-453 replaces B-113. |
| 18May05 | <u>ots</u> <u>node-names</u> | New URL for new OTS manual. Thunder added. |

| | | |
|---------|---|---|
| 02Mar05 | <u>ots</u> <u>info</u> | Post-connect authentication started. Tools table URLs updated. |
| 01Dec04 | <u>node-names</u> <u>internet</u> <u>login</u> | TC2K dropped, UM, Lilac, ALC added. 12-hour renewable timeout explained. 12-hour timeout noted. |
| 25Aug04 | <u>file-transfer</u> <u>node-names</u> <u>info</u> | HTAR role expanded. Blue retired. SCF documentation URL updated. |
| 12Jan04 | <u>node-names</u> | ACE (SCF), MCR (OCF) added. |
| 15Sep03 | <u>introduction</u> <u>internet</u> <u>login</u> | Cross ref to EZSTORAGE added. XSSH role explained. XSSH role explained. |
| 07Apr03 | <u>internet</u> <u>ots</u> <u>forms</u> | Two VPN servers now. New manual, details updated. New OCF URL, more choices. |
| 24Feb03 | <u>node-names</u> <u>ots</u> <u>otp</u> | Only GPS17-22 are interactive. One-time passwords now required. Role updated. |
| 03Feb03 | <u>node-names</u> | TC retired, GPS grows to 48 nodes. |
| 16Dec02 | <u>id-verification</u> <u>node-names</u> <u>index</u> | New section on new OTP aid. ILX cluster added. New keyword for new section. |
| 02Oct02 | <u>node-names</u> <u>securenet</u> <u>login</u> <u>passwords</u> | Log-on issues elaborated. OAK now SC39, ALDER now SC40. OAK now SC39, ALDER now SC40. Forest cluster departs. |
| 26Aug02 | <u>ots</u> <u>otp</u> <u>info</u> <u>file-transfer</u> <u>forms</u> <u>dce</u> | Many details and URLs updated. Scope of OTP use updated. Several URLs updated. SCF anon FTP site deleted. SCF forms URL updated. SCF password URL updated. |
| 15Jul02 | <u>info</u> <u>uinfo</u> <u>index</u> | UNIFO personal profile tool added. Keyword added for new tool. Keyword added for new tool. |
| 15May02 | <u>node-names</u> <u>internet</u> <u>password-map</u> <u>otp</u> | SCF Linux nodes added. OTP optional now for VPN, IPA. SCF Linux nodes added. OTS still does not use OTP. |
| 07Feb02 | <u>node-names</u> <u>path-properties</u> <u>x-terminals</u> <u>password-map</u> | More nodes, more clusters added. SCCD becomes ICC in OCF URLs (only). GPS replaces Compass cases. More OTP-only cases. |
| 03Oct01 | <u>passwords</u> | Section subdivided. |

| | | |
|---------|-----------------------|--|
| | <u>otp</u> | One-time password section added. |
| | <u>index</u> | New keyword for new section. |
| | <u>password-map</u> | Shows where OTP used. |
| | <u>file-transfer</u> | HTAR role noted. |
| 11Apr01 | <u>internet</u> | SSH, IPA, VPN comparison added. Table of access combinations added. |
| | <u>file-transfer</u> | Cross ref to VPN role added. |
| 08Feb01 | <u>internet</u> | All incoming TELNET blocked. |
| | <u>securenet</u> | SecureNet roles for TELNET, SSH clarified. |
| | <u>login</u> | All incoming TELNET blocked. |
| | <u>passwords</u> | No Kerberos passwords remain. |
| 11Dec00 | <u>node-names</u> | Linux names changed from lc to lx. |
| 21Nov00 | <u>node-names</u> | Linux Cluster names added. |
| 05Oct00 | <u>node-names</u> | New section on numerical names. |
| | <u>index</u> | New keyword for new section. |
| 17Jul00 | <u>internet</u> | Globus/Internet job submittal noted. |
| 07Jun00 | <u>file-transfer</u> | FIS, anon. FTP details revised. |
| | <u>passwords</u> | Real words choice suspended. |
| 06Apr00 | <u>introduction</u> | Firewall cross reference added. |
| | <u>internet</u> | Gateway disabled, VPN enabled. SSH role elaborated. |
| | <u>login</u> | Gateway disabled, SSH elaborated. |
| | <u>file-transfer</u> | FTP restrictions updated. |
| | <u>forms</u> | URL for open forms updated. |
| | <u>passwords</u> | CRAY J90s deleted. |
| | <u>info</u> | CRAY sources deleted. |
| 20Sep99 | <u>macx-passwords</u> | New section on MacX encryption. |
| | <u>passwords</u> | DCE publicly replaces Kerberos. entire OCF replaces FAST. |
| 02Sep99 | <u>file-transfer</u> | DCE passwords for FIS coming. |
| | <u>passwords</u> | DCE-open password-change web site. |
| | <u>info</u> | URLs revised, IBM sources added. |
| | <u>forms</u> | SCF forms URL revised again. |
| 07Jun99 | <u>login</u> | SCF TELNET restrictions added. |
| | <u>passwords</u> | TELNET restrictions on password change. Meiko (Tribble) deleted. |
| 26May99 | <u>file-transfer</u> | Firewall effect clarified. |
| | <u>internet</u> | TELNET blocking scope expanded. |
| | <u>login</u> | TELNET blocking scope expanded. |
| 29Mar99 | <u>file-transfer</u> | Firewall blocks FTP now. |
| 02Feb99 | <u>file-transfer</u> | Firewall alert added. |
| | <u>internet</u> | Firewall effects noted. |
| | <u>login</u> | Firewall effects on TELNET noted. |
| 11Jan99 | <u>file-transfer</u> | SCP added, NFT on open net. |
| | <u>passwords</u> | SCF Kerberos steps clarified. |

| | | |
|---------|---|---|
| | <u>internet</u> | Getting Started URL revised. |
| 22Sep98 | <u>forms</u> <u>passwords</u> <u>info</u> | SCF forms URL revised. Borg gone, Tera cluster added. URLs revised. |
| 04May98 | <u>securenet</u> | Web-page password restrictions added. |
| 08Apr98 | entire | First edition of LC EZACCESS manual. |

ANG (12Aug08)

Privacy and Legal Notice (URL: <http://www.llnl.gov/disclaimer.html>)
ANG (12Aug08) Contact: lc-webers@llnl.gov