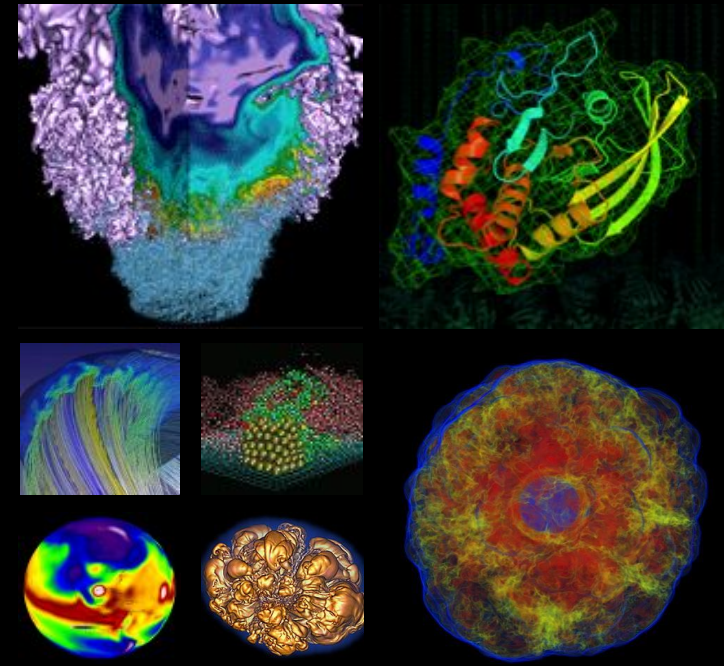


# NERSC Multi-Factor Authentication

It's easy!



Abe Singer

2018-11-01

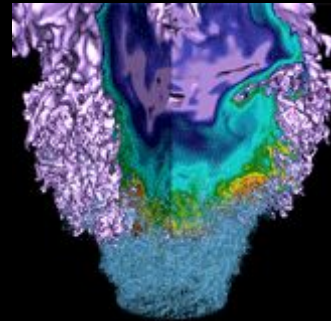
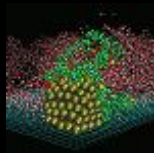
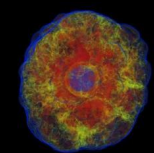
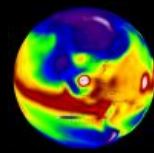
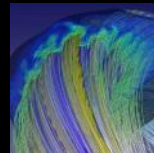


# MFA in Brief

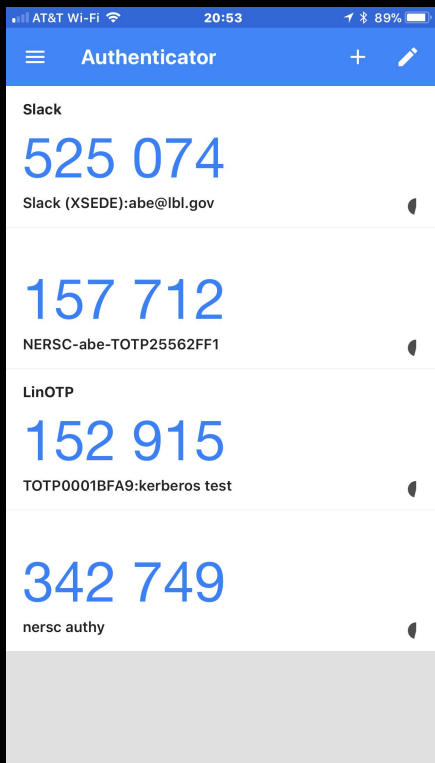


- MFA will be required starting with new allocation year
- MFA == Password + One Time Password (OTP)
  - Protects your account against password theft/guessing
- No special hardware required, uses (free) phone/tablet app
- Configure with NIM in just a few minutes
- *semi* single sign-on (SSO) across NERSC
  - sshproxy: SSO for ssh
  - Shibboleth and NEWT: SSO for websites
- Supported across virtually all of NERSC
  - Coming soon: myProxy, HPSS tokens, Jupyter, NX

# Using MFA



# Google Authenticator



OTP, changes every 30 seconds

157 712  
NERSC-abe-TOTP25562FF1

Serial Number (identifier)

Time remaining

# Using MFA: ssh



```
DOE6748468:~ abe$ ssh cori.nersc.gov
```

```
*****
```

```
* *
```

```
* NOTICE TO USERS *
```

```
* ----- *
```



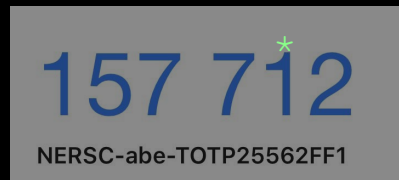
**Password + OTP:** *NIM.password157712*

```
Last login: Wed Oct 31 21:02:26 2018 from 71.143.193.229
```

```
----- Contact Information -----
```



```
abe@cori07:~>
```



- Entering OTP every time isn't very friendly with scripts/workflows
- sshproxy
  - Service developed by NERSC
  - You use MFA to obtain an ssh key that expires after 24 hours
    - MFA once, run everywhere (at NERSC)
    - Use sshproxy again when key expires
  - Leverages ssh *certificates*
  - NERSC-supplied bash client script does all the work

# Using MFA: sshproxy

```
abe$ sshproxy.sh
```

```
Enter your password+OTP: NIM.password157712
```

```
Successfully obtained ssh key /Users/abe/.ssh/nersc
```

```
Key is valid: from 2018-11-01T04:36:00 to 2018-11-02T04:37:51
```

```
abe$ ls ~/.ssh
```

```
config      id_rsa.pub  nersc      nersc.pub
```

```
id_rsa      known_hosts nersc-cert.pub
```

```
abe$ ssh -i ~/.ssh/nersc cori.nersc.gov
```

```
*****
```

```
*
```

```
*
```



```
*
```

```
NOTICE TO USERS
```

```
*
```

```
abe@cori07:~>
```

# Using MFA: ssh config (less typing)

~/.ssh/config

```
Host cori cori.nersc.gov
      Hostname cori.nersc.gov
      IdentityFile ~/.ssh/nersc
```

# Using MFA: Shibboleth

**NERSC**



National Energy Research  
Scientific Computing Center

abe

\*\*\*\*\*

Log in

[Forgot your password?](#)



National Energy Research  
Scientific Computing Center

Hello, Abraham

Your account has MFA enabled; please enter your one-time password.

157712

Log in

[Information on MFA at NERSC](#)

## Please sign in

NERSC Username

NIM Password:

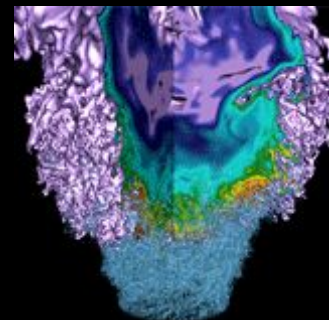
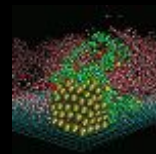
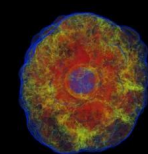
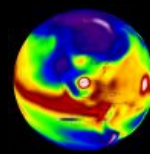
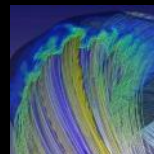
MFA (if applicable),

[Reset your NIM password.](#) | [Forgot your username?](#) | [Lost your tokens?](#) | [Sign in as Staff](#)

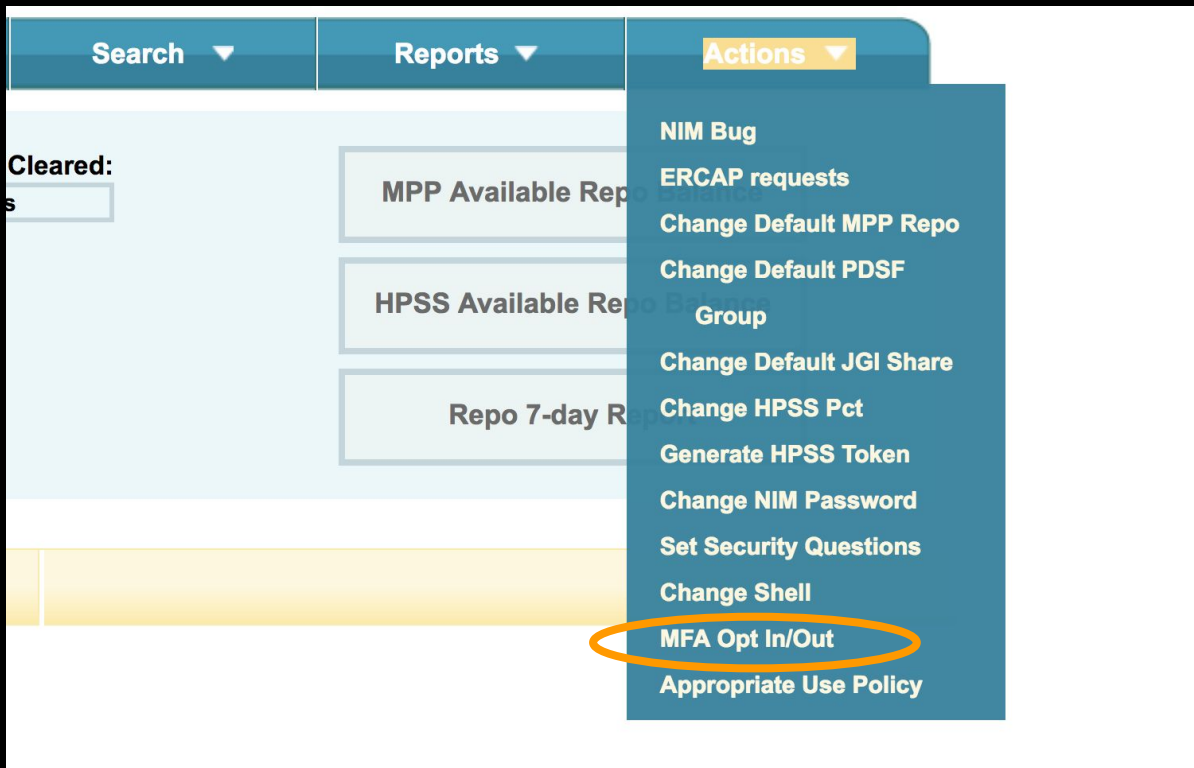
Log In



# Enabling MFA



# Enabling MFA



The screenshot displays the NERSC user interface. At the top, there are three tabs: 'Search', 'Reports', and 'Actions'. The 'Actions' tab is selected, and its dropdown menu is open, showing a list of options. The option 'MFA Opt In/Out' is circled in orange. Other options in the menu include 'NIM Bug', 'ERCAP requests', 'Change Default MPP Repo', 'Change Default PDSF Group', 'Change Default JGI Share', 'Change HPSS Pct', 'Generate HPSS Token', 'Change NIM Password', 'Set Security Questions', 'Change Shell', and 'Appropriate Use Policy'. In the background, there are sections for 'Cleared:', 'MPP Available Repo', 'HPSS Available Repo', and 'Repo 7-day R'.

# Enabling MFA (cont.)

Enabling your account for MFA will then require you to use a multi-factor authenticator when logging into NERSC systems.

More information can be found [here](#)

## MFA Opt In/Out

Default Login Name	MFA Enabled ?
--------------------	---------------

abe	Enabled ▾
-----	-----------

Save All Rows

Enter and manage MFA Tokens

# Creating a "token"

Account Usage	Logins by Host	Unix Groups	Roles	Contact Info	Grid Certificates	SSH Keys	MFA Tokens
---------------	----------------	-------------	-------	--------------	-------------------	----------	------------

Abraham Singer

User	Serial Id	Token Description	Fails
abe	TOTP3875DD4A	authy	0
abe	TOTP3880C953	foo	0
abe	TOTP25562FF1	iphone	0

Add Token

Not allowed to delete tokens

Generate backup passwords:

Generate!

MFA can be disabled by [Clicking here](#) and selecting '*disabled*', then '*Save All Rows*'.

# Creating a token (cont.)

Account Usage	Logins by Host	Unix Groups	Roles	Contact Info	Grid Certificates	SSH Keys	MFA Tokens
---------------	----------------	-------------	-------	--------------	-------------------	----------	------------

Abraham Singer

User	Serial Id	Token Description	Fails
abe	TOTP3875DD4A	authy	0
abe	TOTP3880C953	foo	0
abe	TOTP25562FF1	iphone	0

Add Token

Not allowed to delete tokens

Generate backup passwords:

Generate!

Select User

abe ▾

Enter Token Description

yet another token

Submit

MFA can be disabled by [Clicking here](#) and selecting '*disabled*', then '*Save All Rows*'.

# Creating a token (cont).

OATH Soft Token

OTP seed

QR-Code for installing the OATH compatible Soft Tokens (FreeOTP, Google Authenticator and other apps using the 'otpauth://' syntax).

**This will be the only time you will be able to scan this code into your Google Authenticator (or similar app), or use the URL string below.**

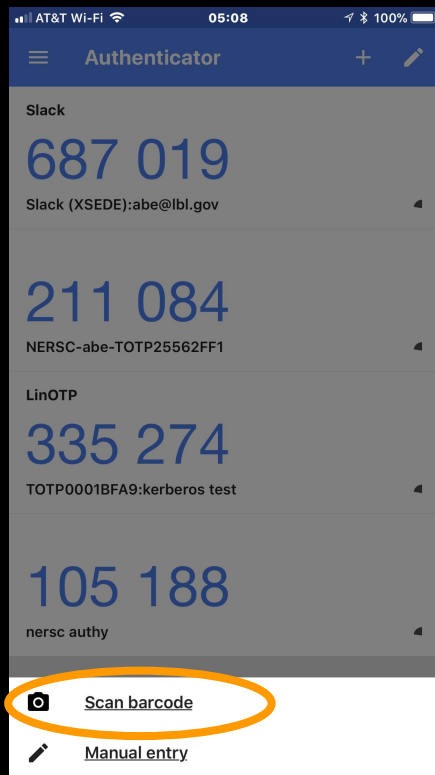
For other apps that require manual configuration, choose the "OTP seed" tab above.



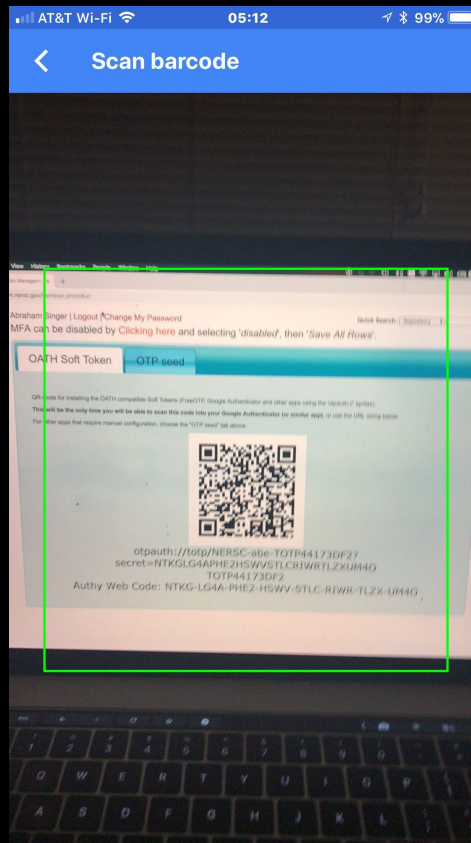
otpauth://totp/NERSC-abe-TOTP44173DF2?  
secret=NTKGLG4APHE2HSWVSTLCRIWRTLZXUM4O  
TOTP44173DF2

Authy Web Code: NTKG-LG4A-PHE2-HSWV-STLC-RIWR-TLZX-UM4O

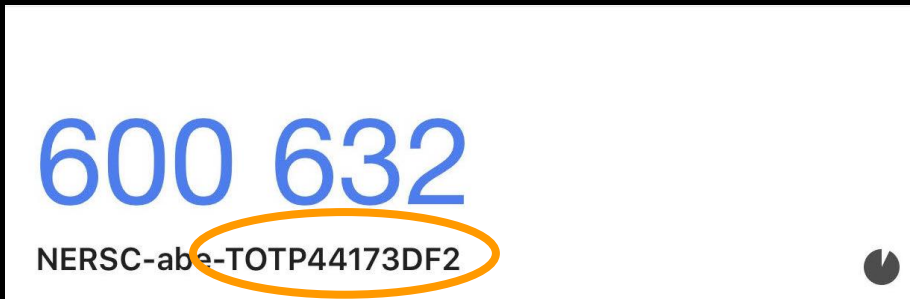
# Creating a token (cont).



# Creating a token (cont).



# Creating a token (cont).



User	Serial Id	Token Description	Fails
abe	TOTP3875DD4A	authy	0
abe	TOTP3880C953	foo	0
abe	TOTP25562FE1	iphone	0
abe	TOTP44173DF2	yet another token	0
Add Token		Not allowed to delete tokens	
Generate backup passwords:		Generate!	

# Additional details



- sshproxy keys >24 hours with justification and authorization
- Desktop app ("authy") for the smartphone-less
- "Backup" OTP passwords for when you leave your mobile at home
- Token "reset" for when you lose/replace your device(s)
- Hardware token (yubikey) supported
  - You have to purchase (~\$40) and configure
  - Requires desktop software
  - Kindle Fire is only slightly more (\$50)
    - And you can play games on it too!
- Exceptions to MFA available if necessary
  - Tell us why MFA can't work for you

# Any Questions?

---



- <https://www.nersc.gov/users/connecting-to-nersc/mfa/>
  - Or google "NERSC MFA"
- Any questions?

# NERSC

Thank You



U.S. DEPARTMENT OF  
**ENERGY**

Office of  
Science

