New Hire IT Orientation
April 29, 2024
Today’s Agenda

01 Account Usage and Access
Gain further understanding on account usage and access, which includes device login, DUO, and SLAC Training.

02 Device configuration
Logging in and accessing essential tools, including bookmarks, Outlook, Slack or Teams, and Crashplan.

03 Seeking IT Support
IT Assistance and Resources: Service Desk, IT Tools and Marketplace, Software Management, and Cybersecurity Alerts.

04 Enabling Remote Work
Enabling Remote Work: Using VPN, Citrix, and DUO for Accessing the SLAC Network.
Account Usage and Access

Please login to your device using your SLAC credentials

If you do not have your credentials, please raise your hand for assistance from our computer support analyst (CSA).
## Account Usage and Access

<table>
<thead>
<tr>
<th>Stanford Accounts</th>
<th>SLAC Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Axess</td>
<td>● SLAC managed PC</td>
</tr>
<tr>
<td>● Zoom</td>
<td>● Microsoft 365 Applications</td>
</tr>
<tr>
<td>● Crashplan</td>
<td>● Cisco AnyConnect</td>
</tr>
<tr>
<td>● Google Suite</td>
<td>● Citrix</td>
</tr>
<tr>
<td>● Slack</td>
<td>● SLAC Today -</td>
</tr>
</tbody>
</table>
<pre><code>                            | intranet.slac.stanford.edu      |
</code></pre>
Sign in with your SLAC Windows credentials

Username
Password

Sign in

This is a Federal computer system and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at
After logging in, you'll be prompted to enable Two-Factor Authentication (2FA) for added security. You have two options for 2FA:

1. **Mobile Device:** You can use your mobile phone for 2FA through one of the following methods:
   - **Call:** You will receive a phone call with a verification code.
   - **Text Message:** You will receive a text message containing verification codes.
   - **DUO App Notification:** If you have the DUO mobile app installed, you can receive a push notification to approve the login.

1. **Yubikey:** If you or your manager have requested it, you can use a Yubikey as your 2FA method.
   - Enter your personal passcode when prompted.
   - Insert Yubikey into your computer's USB port and tap it to confirm your identity.
New Employee Setup

Please Open Browser

- Bookmarks these sites:
  - ✓ Select SLAC Today
  - ✓ Select SLAC Training
  - ✓ Select Outlook.com
  - ✓ Select iAT Timecard
  - ✓ Select Stanford Axess
Accounts | SLAC Account
SLAC Training

Welcome to the SLAC Training Portal. From here, you can access the various training options and tools available to you.

Where Do You Want To Go?

- THE SLAC WEB TRAINING PORTAL
  Web training →

- THE SLAC TRAINING COURSE CATALOG
  Course catalog 🗝
  Requires SLAC Windows Authentication

- INTERNAL SLAC TRAINING CLASSES
  SLAC training registration system →
Accounts | Outlook Webmail

Sign in with SLAC email address

username@slac.stanford.edu
Sign in with SLAC credentials

For help with Timecards contact timekeeping@slac.stanford.edu
Device Configuration
What is Cardinal Key?

Cardinal Key password-less authentication service. This feature allows you to access websites without entering your username and password.

How does it work?

The enrollment process places a certificate on your machine that is unique to the combination of you and your machine. When you access a Cardinal Key-aware service, the login process will look for the Cardinal Key certificate on your machine. If it finds one, it will initiate a Duo multi-factor prompt and let you into the services.

Cybersecurity Compliance

- Must be SLAC owned machine
- Must be managed by SLAC IT
- Have correct property control custodian
- Crowdstrike must be installed and active
- Must be current version of operating system
- Disk must be encrypted
- Must have wifi
SLAC Cardinal Key Enrollment

How to Enroll?

After going to the SLAC Cardinal Key Link, enter in your PC number.

Select one of the following links for steps on how to install SLAC Cardinal Key:
Backup with CrashPlan

Log into CrashPlan with SUNet ID

Cloud storage and network drives:

- One drive
- Google drive
- Vdrive
1. Open the Zoom app
2. In the Zoom app, look for the "Sign in with SSO" option.
3. Choose Sign in with SSO: stanford.zoom.us
4. Use your Stanford University Network (SUNet) credentials to sign in.
Sign in with your SUNet ID:  
https://stanford.slack.com

Be a part of the SLAC workspace community:
→ Join the SLAC workspace!
→ Connect with your coworkers!
→ Update your name and picture!
→ Join channels!
Microsoft Teams

Sign in with your SLAC credentials:

username@slac.stanford.edu
Microsoft Outlook

Sign in with default profile or your SLAC credentials
If you need help please raise your hand for assistance from our computer support analyst (CSA).
IT Service Desk

- Visit the IT website: https://it.slac.stanford.edu/
  - Submit a ticket
  - Submit a request form
  - Phone Support: (650) 926-4357 (HELP) 7am-6pm
  - Onsite Support Desk: Building 050, First Floor Lobby 8am-5pm
IT Website

Navigate to [it.slac.stanford.edu](http://it.slac.stanford.edu)

- Submit a support ticket
- Find request forms
- Search Knowledge Base
- View Current Projects
- Upcoming Events
- Latest Updates
Service Now

- [https://it.slac.stanford.edu/support](https://it.slac.stanford.edu/support)
  - Knowledge Base
  - Submit a ticket
  - Request Something

How to approve a request
Hardware purchasing:
[itmarketplace.slac.stanford.edu](http://itmarketplace.slac.stanford.edu)

Available:
- Laptops
- Desktops
- Accessories
  - Monitors
  - Docking Station
  - Cables
  - Adapters
  - Webcam
  - Mouse/Keyboards
  - Headset

Will need a charge code (Project-Activity number)
Cyber Security Support

Cyber Security can assist with various security concerns. SLAC Cybersecurity’s mission is to:

- Protect the laboratory’s information resources
- Enable the laboratory to use the best technologies that empower science

**Common Areas of Support:**

1. **Phishing Activity:**
   a. Including spam emails, spoofed emails, and more.

2. **Account or Information Compromise:**
   a. For any breaches or unauthorized access.

3. **Lost or Stolen Devices:**
   a. Covers laptops, tablets, smartphones, storage devices, and other media.
Cyber Security Support

Additional Resources:
Explore further information and resources at Cybersecurity Website:
https://it.slac.stanford.edu/cybersecurity

Training Requirements:
Cyber training must be completed annually. Access it here:
https://it.slac.stanford.edu/cybersecurity/training

Contact Information:
For assistance, contact:
Cyber Security: cyber@slac.stanford.edu
IT Service Desk: Phone - xHELP (650-926-4357)

Reporting Suspicious Emails:
Forward suspicious emails to spam@slac.stanford.edu.
Enabling Remote Work

If you need help please raise your hand for assistance from our computer support analyst (CSA).
Connecting to SLAC Network Remotely

Cisco VPN: Server Address: vpn.slac.stanford.edu

Citrix: citrix.slac.stanford.edu
Administrator Privileges

For Mac Users:
- Access System Preferences.
- Navigate to Users & Groups.
- Request Administrator Privileges by raising your hand, and we'll assist you.

Windows
- Submit an Administrator Account Request.
- Note: This may not be necessary if you won't be installing many applications.
We value your feedback. Please share your thoughts with us at [SLAC IT Feedback Portal](http://slacit.stanford.edu/voc).
Thank You