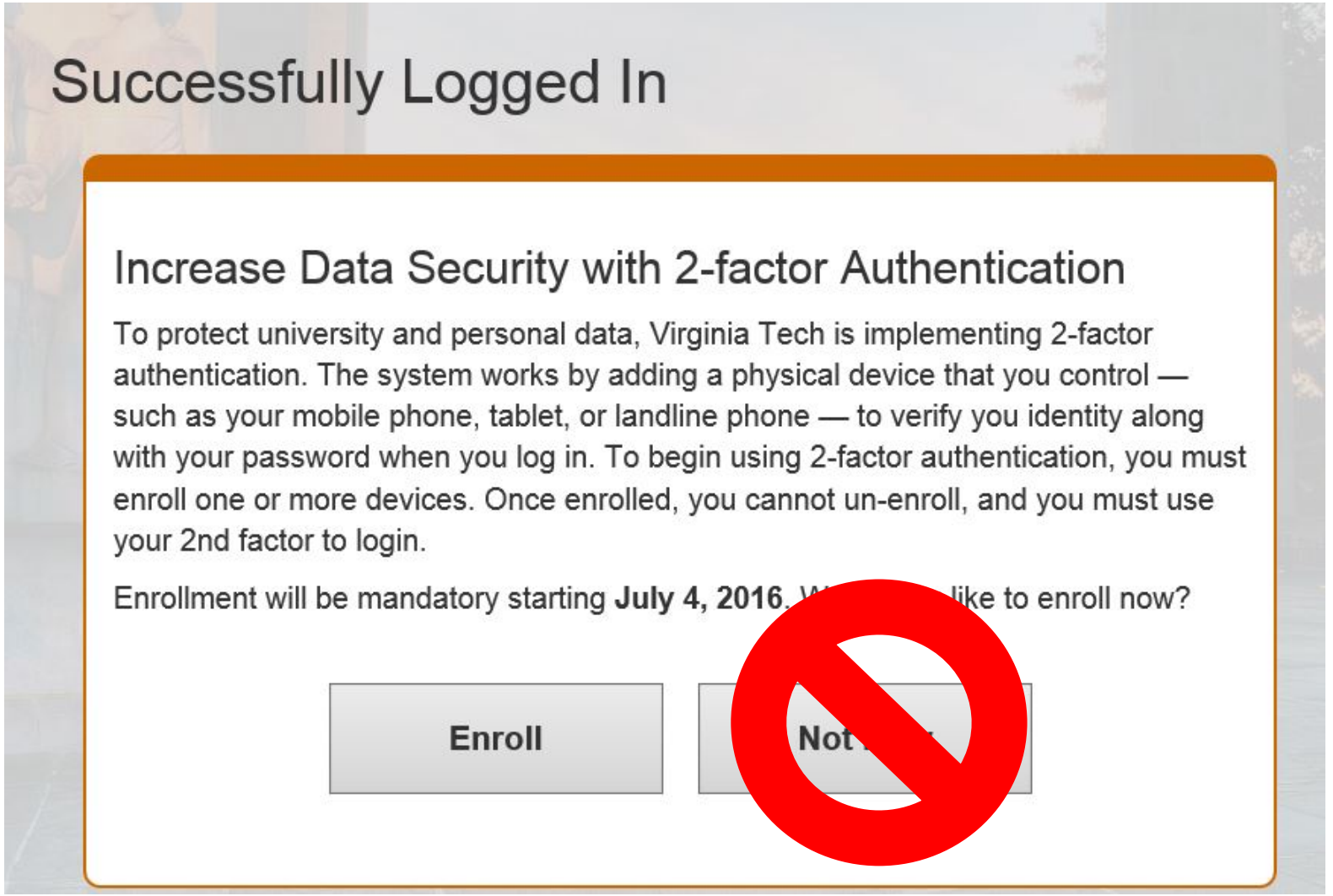
2-Factor Authentication Update

DCSS April 19, 2016

June 1, 2016


VirginiaTech
Central Authentication Service
Help
Terms of Use
About CAS
Shutdown Notice
The Central Authentication Service
will be shut down on June 1, 2016.
Services are moving to the
les use of 2-factor
authentication. Services
Canvas and Scholar
have already moved.
For more informa
te list of affected
www.it.vt.edu/2
PID or Gu
Us
Pas
username or password
re logging
Switch to high security PDC login.
Security Notice
For security reasons, please close your web browser when you have finished accessing services

July 4, 2016


Successfully Logged In
Increase Data Security with 2-factor Authentication
To protect university and personal data, Virginia Tech is implementing 2-factor authentication. The system works by adding a physical device that you control — such as your mobile phone, tablet, or landline phone — to verify you identity along with your password when you log in. To begin using 2-factor authentication, you must enroll one or more devices. Once enrolled, you cannot un-enroll, and you must use your 2nd factor to login.
Enrollment will be mandatory starting July 4, 2016.
like to enroll now?
Enroll

Don’t Wait. Enroll Now.

Token update

- Duo D-100 tokens at SW Distribution
- YubiKeys from Hokie Centric pre-load keys
- SNS and SW Distribution for additional help
- Token Management in Account Manager My.vt.edu/accounts

Yubico

Enrolled Phones

In order to add or remove devices other than tokens, use login.vt.edu/2fa/manage.

Phone ID	Phone Number	Type	Capabilities
DPK92TSVD8JV9XH8HUHB	+1 (540) [redacted]	Mobile	Duo Push Text Message Voice Call
DPTMM9PJDS144HVMC9W1	+1 (540) 231-9327	Landline	Voice Call
DPWXKIDGHET3RUYAEPWF	+1 (540) [redacted]	Landline	Voice Call
DP6EGTI8EPWXJC77GRF2		Mobile	Duo Push

Enrolled Tokens

Most users will be best served by using the Duo smart phone app, which is automatically configured as a token and functions even when you do not have voice or data connectivity. Hardware tokens are appropriate when a phone is not available. If you are unfamiliar with tokens and token technologies, please consult with your department's IT staff to help evaluate your situation.

Token ID	Serial Number	Type	Options
DHGPLUHN97PO28AW78BA	DSEC[redacted]	HOTP	Resync | Remove Token
DH5YNU9YCSDQJU83JAEE	yk-[redacted]	YubiKey (AES Mode)	Remove Token

U2F tokens do not display in Accounts.

Enroll Token

Note: To add your token for U2F (Chrome), please use "Add a new device" in the Login interface. Learn more.

Learn more about 2 factor at www.it.vt.edu/2factor or review the KnowledgeBase article.

Enroll Token

Logged in as **dunker**. Logout

Enroll YubiKey Token

Enroll Hardware OATH Token

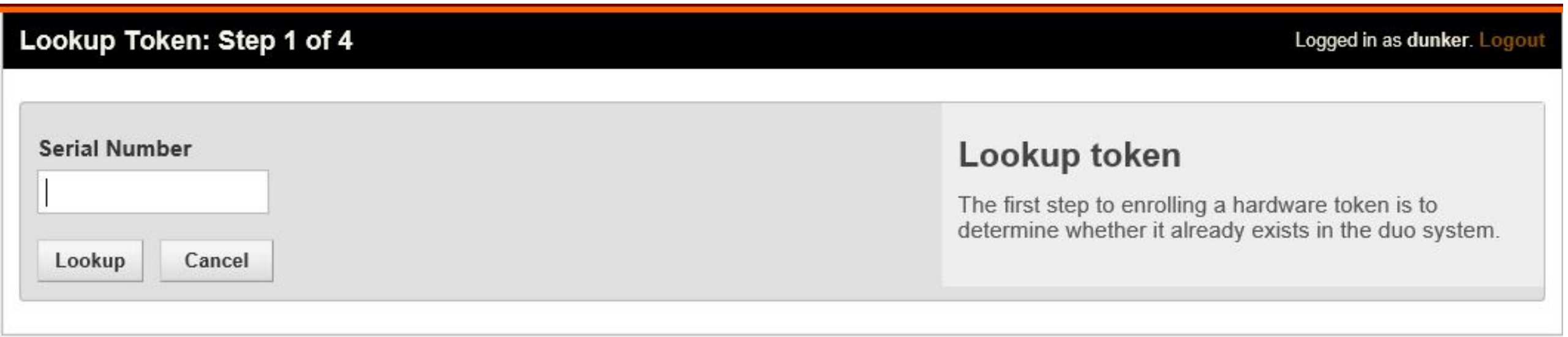
Enroll Software OATH Token

Select token type to enroll

- YubiKey (OTP mode)
- Hardware OATH token (e.g. Duo D-100, Gemalto, other HOTP)
- Software OATH token (e.g. Google Authenticator)

To enroll a token using U2F, see the KnowledgeBase article or use add device in Duo.

« Back to 2-factor account


Lookup Token: Step 1 of 4
Logged in as dunker. Logout
Serial Number
Lookup
Cancel
Lookup token
The first step to enrolling a hardware token is to determine whether it already exists in the duo system.

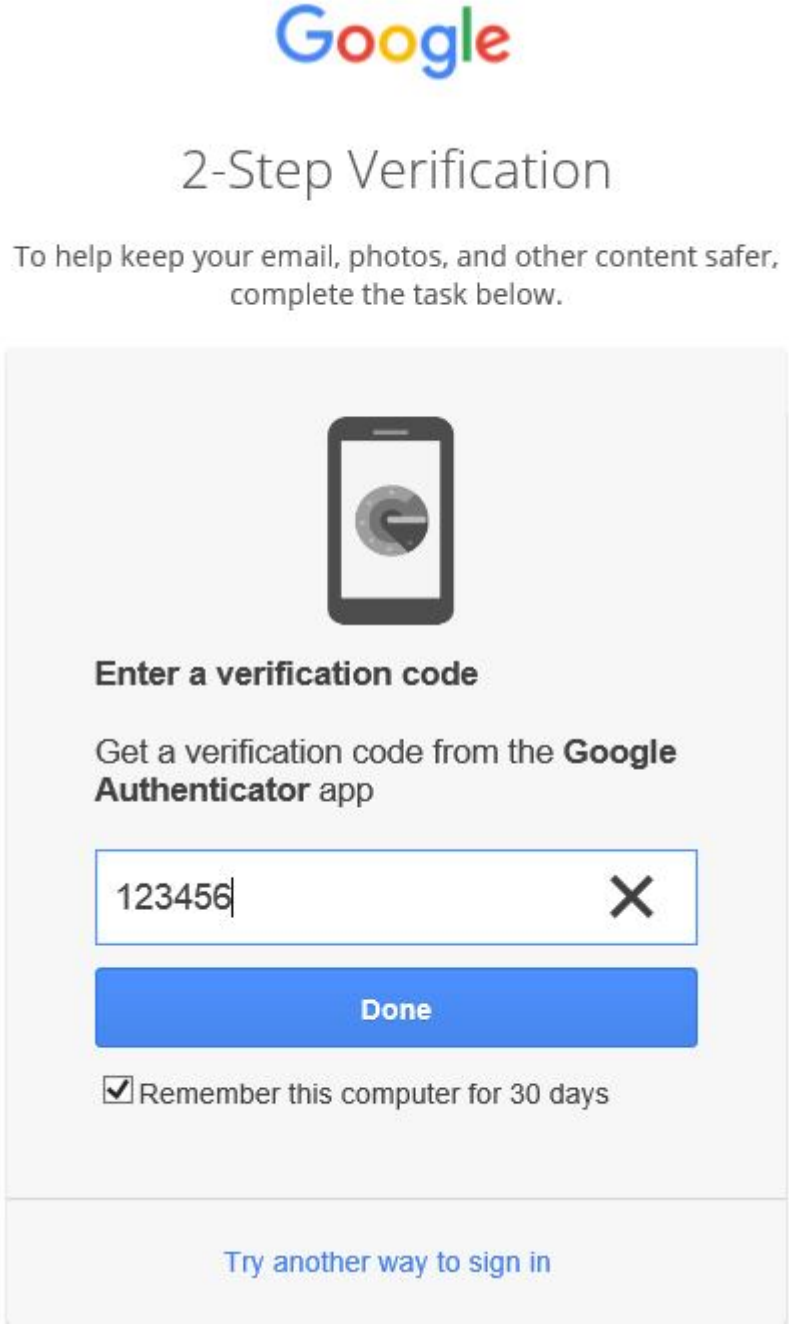
What's Next

- Passcodes retrieved from web site, alternative to SMS
- Incorporating 2FA enrollment into PID generation process by November 30, 2016
- Distributed Duo - pending resolution to an issue we discovered

http://4.bp.blogspot.com

Non-CAS and Non-Windows Recommendations

- Enforcing Google two-step
- LDAP - investigating how/whether we can implement selectively or all-or-nothing
- Investigating VPN for high risk systems that cannot directly use Duo integration



www.it.vt.edu/2factor