MFA: Login via CAS, VPN Browser & Cisco AnyConnect

Summary

Instructions for Logging into CAS, YaleConnect, and VPN (via web browser) with Multifactor Authentication (MFA)

**NOTE:** MFA is only required when logging into Yale resources from off campus. Off Campus is defined as anything other than YaleSecure Wireless, Yale Wireless, or Yale hard-wired networks. There are a few physically/geographically remote offices (medical) which are connected via Aruba Networks however they are considered on Campus and they will see no change. “Yale Guest” is an Off Campus network.

Information

Multi-factor Authentication (MFA) is an additional security measure to protect your intellectual property, personal information, and Yale’s data. MFA adds a step to the log-in process used to access some of Yale’s resources by requiring an individual, after entering their NetID and password, to prove their identity by responding to a prompt on a mobile device, landline, tablet or token. Use this article to find a Word Document with instructions for logging into VPN with Multi-factor Authentication.

To learn more about Multi-factor Authentication open and read the Logging into VPN with Multi-factor Authentication document.

Step-by-step guide

**Step 1: Follow the instructions below for your specific login situation**

- **Logging into CAS with Multi-Factor Authentication**
  1. Log in as usual with your netID and password. This will launch the Duo Multifactor Authentication Screen
  2. Proceed to Step 2

- **Logging into VPN from a browser with Multi-Factor Authentication**
  1. Navigate to access.yale.edu into your web browser. This will launch the log in screen.
  2. Log in with your netID and password. This will launch the Duo Multifactor Authentication Screen
  3. Proceed to Step 2

- **Logging into VPN from Cisco Anyconnect with Multi-Factor Authentication**
  1. Launch the Cisco AnyConnect Client
  2. Type access.yale.edu or choose it from your drop down if it is not pre-populated and click connect. This will launch a new log in screen.

  3. Enter your NetID and password in the corresponding fields. In the “Second password” field, type “push”, “SMS”, or “phone” to tell Duo how you want to authenticate or enter a Duo generated passcode. Click OK.
Step 2: Log in with your second factor device by choosing 1 of 3 methods to authenticate:

- **Method 1: Duo Push**
  - Push a login request to your phone if you have the Duo Mobile app.
  - Click to select "Automatically send a push to XXX-XXX-1234 from now on." to always automatically receive a Duo Push. *This is the recommended and simplest way to authenticate.*
  - Tap “Approve” on your mobile device to be logged into your desired application. See image below for screenshots.

- **Method 2: Phone call**
  - Generate a phone call to the landline or mobile phone enrolled on your DuoMobile account.
  - Follow the prompts when you are called to be logged into your desired application. See image below for screenshots.

- **Method 3: Passcode**
  - Login by typing a Passcode received via SMS, a hardware token, or your administrator.
You can also generate a new passcode sent via SMS from this screen. See image below for screenshots.

### What Multifactor Authentication device(s) do you have?
(WE RECOMMEND REGISTERING AT LEAST TWO DEVICES)

<table>
<thead>
<tr>
<th>Device Type</th>
<th>How Can I Authenticate?</th>
<th>Where Can I Use It?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartphone</td>
<td>Duo Push* (Recommended), Phone Call, Passcode, Text Message</td>
<td>Locally (in the US) and globally (outside the US) even without a wireless or cellular connection (on Airplane Mode, at no charge to you)</td>
</tr>
<tr>
<td>Tablet</td>
<td>Duo Push* (Recommended), Phone Call, Passcode</td>
<td>Locally (in the US) and globally (outside the US) even without a wireless connection (on Airplane Mode, at no charge to you)</td>
</tr>
<tr>
<td>Cellphone</td>
<td>Phone Call, Text Message</td>
<td>Locally (in the US) and globally (outside the US) but you may incur a charge for a phone call or text message</td>
</tr>
<tr>
<td>Landline</td>
<td>Phone Call</td>
<td>Anywhere you can access your landline while authenticating</td>
</tr>
</tbody>
</table>

* Duo Push, a notification sent to your smartphone or tablet, is the simplest method to authenticate.

**What is a token? Do I need one?**

A token is a small device that generates a secure passcode to authorize access to Yale resources from off-campus. If you have a smartphone or a tablet the Duo Mobile App will act as a token, even if you are in an area with no cellular data or wifi connectivity, both in the US and outside the US.

**I don’t have any of these devices.**

Call the Help Desk at 203-432-9000 for a set of one-time use codes for authentication.

---

For more information, visit its.yale.edu/mfa or contact the Help Desk.
Help us improve

Your Rating:  
Results: 17 rates

Related articles

• Capital IQ requires VPN to access when off campus
• Access Network Shared Drives from off-campus using VPN (Windows 10)
• DUO: MFA FAQs
• MFA Quick Guide: Enrolling a Device
• Cisco AnyConnect Troubleshooting