How do I login to MIT services that leverage Duo two-factor authentication?

Q: How do I login to MIT services that leverage Duo two-factor authentication?

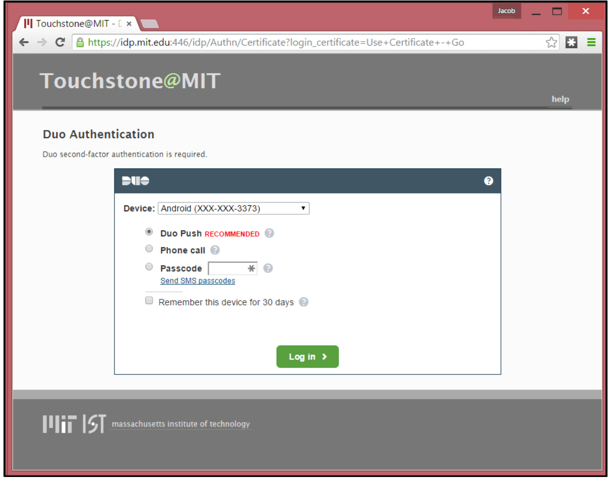
> **Touchstone and Duo updates March 22**
> Touchstone and Duo authentication has been updated with some visual changes and an improved two-factor authentication experience as Information Systems and Technology (IS&T) implemented updates to the Institute's single sign-on web authentication service on Friday, March 22.
>
> - IS&T News: Touchstone and Duo updates coming March 22
> - Duo Universal Prompt Guide

On this page:

- Authenticating via Touchstone with the Duo authentication requirement enabled
  - Duo Push
  - Phone Call
  - Passcode
- Connect to a Duo-protected Microsoft Windows machine with Remote Desktop Connection (RDP)
- Acquire Kerberos tickets for a Duo-protected principal using `kinit`

Authenticating via Touchstone with the Duo authentication requirement enabled

1. Launch a webpage (Chrome, Firefox, Safari and Internet Explorer), that requires Touchstone authentication and begin to authenticate as normal
2. Once you have completed the Touchstone authentication steps (via Certificates, kerberos tickets or kerberos username and password), you will be prompted for Duo Authentication
3. Select your Device and choose a Method


Touchstone@MIT - [
Jacob
https://idp.mit.edu:446/idp/Authn/Certificate?login_certificate=Use+Certificate+-+Go
Touchstone@MIT
help
DUO
Log in ›
MIT IST massachusetts institute of technology

Duo Authentication

Duo second-factor authentication is required.

Device: Android (XXX-XXX-3373)

● **Duo Push** RECOMMENDED
○ **Phone call**
○ **Passcode**
Send SMS passcodes
☐ Remember this device for 30 days

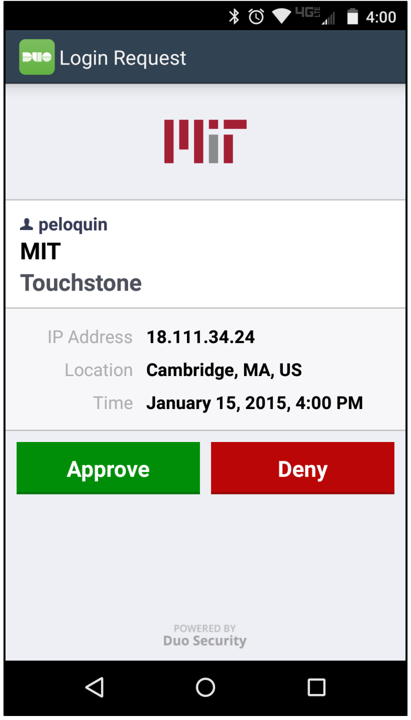
Method

- Duo Push (smartphones with Duo app installed)
- Phone Call (default for landline)
- Passcode request via SMS

- (Optional) **Remember this device for 30 days**: If you choose this, Duo will treat your device as "trusted".

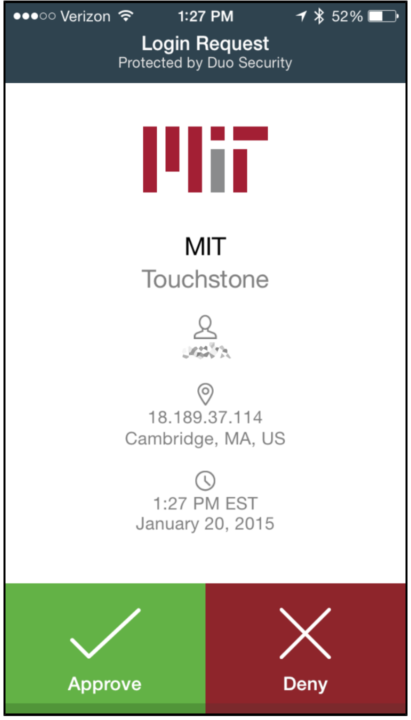
Duo Push

1. A request will be sent to your mobile device via the Duo app
   You must have an active mobile (cellular) or wifi connection to receive this request
2. Tap **Approve** on your Mobile Device's Duo app. It should look similar to one of these:



peloquin
MIT
Touchstone

IP Address **18.111.34.24**
Location **Cambridge, MA, US**
Time **January 15, 2015, 4:00 PM**



MIT
Touchstone
[redacted]
18.189.37.114
Cambridge, MA, US
1:27 PM EST
January 20, 2015

1. ***Result:*** Your web browser's Touchstone session should automatically complete authentication

> ⚠ If your mobile phone doesn't automatically show the Duo Push request, you can force a refresh of push requests by tapping and dragging the "MIT" account downwards on your phone.

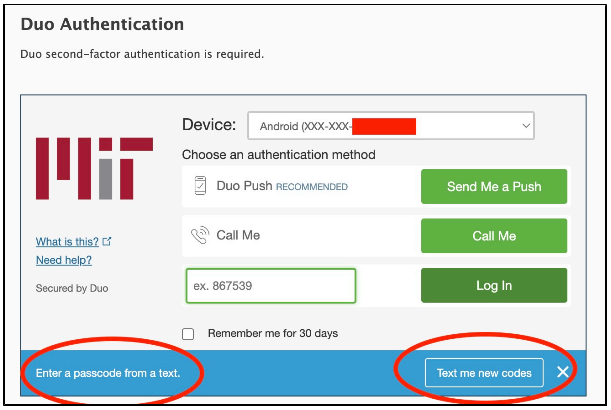
Phone Call

1. An automated attendant will call your phone
2. Answer and wait for the Duo automated message to begin playing
3. Push any valid dialpad key on your phone (0-9,# or *) and hang-up
4. ***Result:*** Your web browser's Touchstone session should automatically complete authentication

Passcode

> ⚠ Effective January 23,2024 - Touchstone will no longer accept passcodes from the Duo mobile app as a second authentication factor. Passcodes sent via SMS will be limited to one per message, with a five-minute expiration time.

1. Request a new passcode
   For a mobile phone that can accept SMS messages, you can request an SMS passcode by clicking the link underneath the passcode prompt in the Touchstone authentication window



Duo Authentication

Duo second-factor authentication is required.

Device: Android (XXX-XXX-[redacted]

Choose an authentication method

ex. 867539

☐ Remember me for 30 days

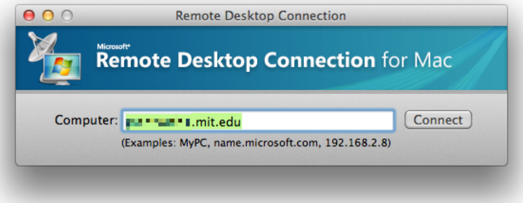
Enter a passcode from a text.

2. Enter the passcode obtained from the SMS message
3. Click **Login**
4. ***Result:*** Your web browser's Touchstone session should automatically complete authentication

> ⚠ If you type the incorrect passcode, you will be prompted to enter the correct one or you can choose another device or method

Connect to a Duo-protected Microsoft Windows machine with Remote Desktop Connection (RDP)

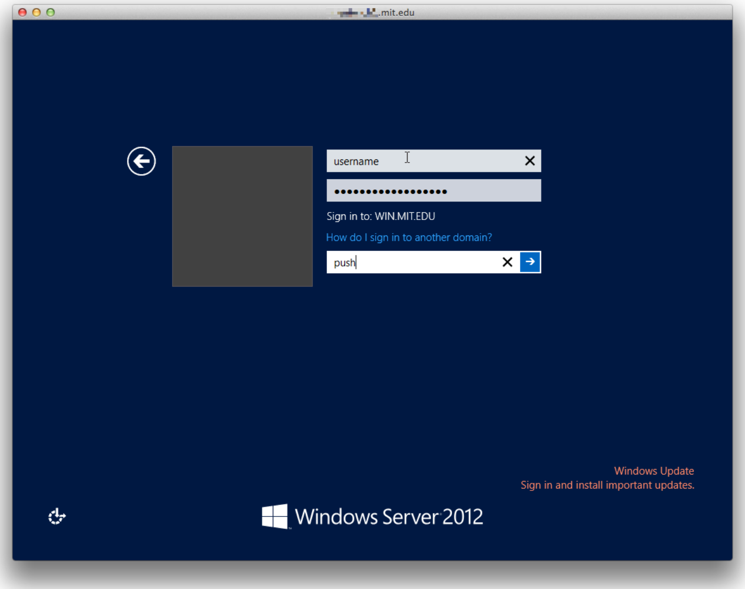
1. Launch Microsoft Remote Desktop and enter the hostname or IP address of the machine you wish to connect to (note: you may have to connect to MIT's VPN service to use RDP).



Computer: [redacted].mit.edu

(Examples: MyPC, name.microsoft.com, 192.168.2.8)

2. When presented with the Windows login screen, enter your MIT username and password.
3. In the field labeled "Duo Password" you can enter one of the following options:
   a. **push** - *Duo will send a push notification to your registered cell phone with the Duo Security mobile app installed*
   b. **sms** - *Duo will send an SMS to your registered cell phone*
   c. **phone** - *Duo will call your registered cell phone*
   d. *The one time code generated by your hardware token or the Duo Security mobile app (the code changes ever 60 seconds)*



[redacted].mit.edu

username

Sign in to: WIN.MIT.EDU

How do I sign in to another domain?

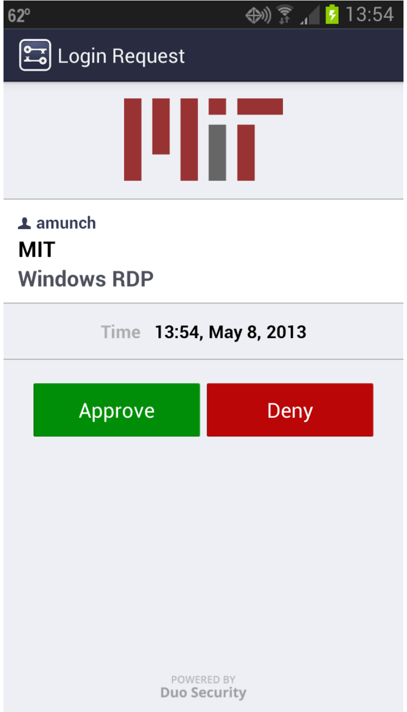
push

Windows Update
Sign in and install important updates.

In this example, we've entered "push" in the "Duo Password" field.

> ⚠ **'How to call different devices'**
> If you have multiple devices that can use the same method, for instance two mobile phones or two phones that can receive phone calls, you can reference them by different numbers. For instance, to call the top device on your managed devices page (http://duo.mit.edu), you can use 'phone' (for the default) or 'phone1' to call the second phone, you can use 'phone2'.

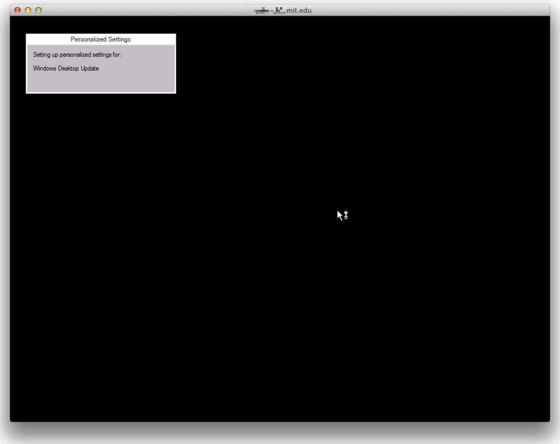
4. In this example, you will receive a push notification on your cell phone. Click **Approve**.



amunch
MIT
Windows RDP

Time 13:54, May 8, 2013

5. The remote Windows system should now complete authentication and the Remote Desktop Connection will complete.



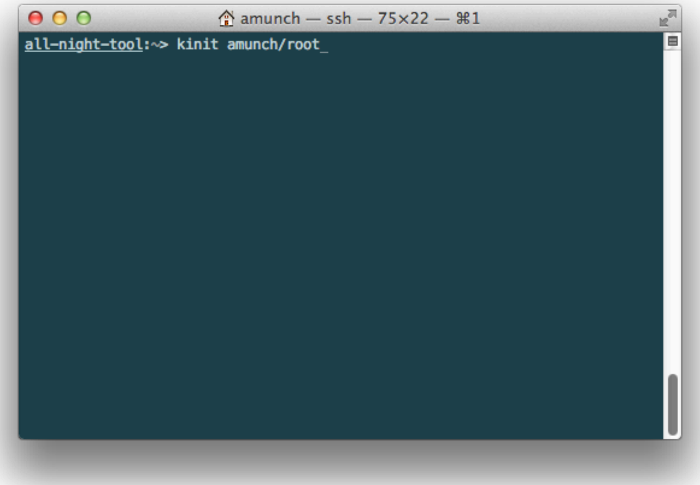
Personalized Settings

Setting up personalized settings for:

Windows Desktop Update

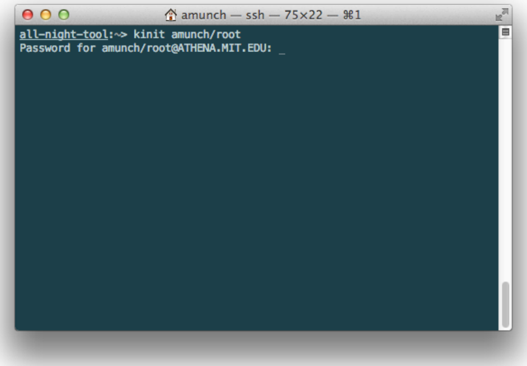
Acquire Kerberos tickets for a Duo-protected principal using `kinit`

1. Log into an Athena machine (e.g. `ssh athena.dialup.mit.edu`).



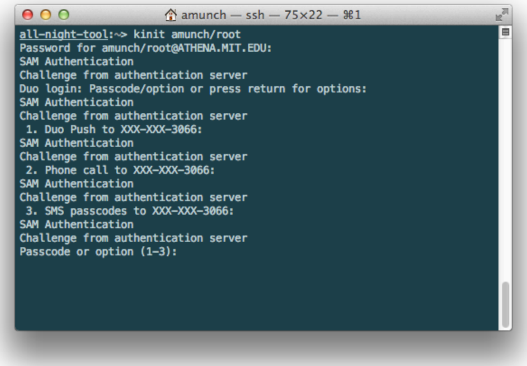
```
all-night-tool:~> kinit amunch/root_
```

2. Initiate Kerberos ticket acquisition (e.g. `kinit username/root`) and enter the appropriate Kerberos password when prompted. **Note:** not all Kerberos accounts will be protected with Duo. Typically, only root accounts or users with escalated privileges (e.g. username/root or username/extra) will be protected with Duo.



```
all-night-tool:~> kinit amunch/root
Password for amunch/root@ATHENA.MIT.EDU: _
```

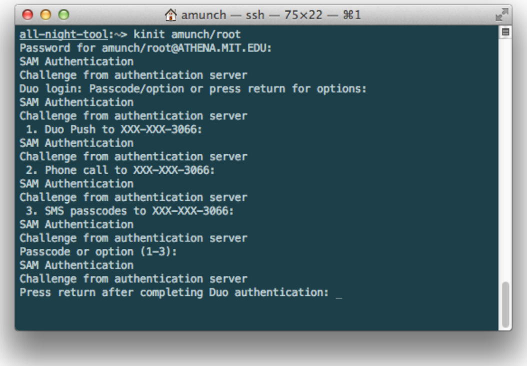
3. The Duo two-factor system will now challenge your login asking for a method to contact you. You can hit the "Enter" key to see all the options available to you. By default, option "1" will send a push notification to the Duo mobile app.



```
all-night-tool:~> kinit amunch/root
Password for amunch/root@ATHENA.MIT.EDU:
SAM Authentication
Challenge from authentication server
Duo login: Passcode/option or press return for options:
SAM Authentication
Challenge from authentication server
 1. Duo Push to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
 2. Phone call to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
 3. SMS passcodes to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
Passcode or option (1-3):
```

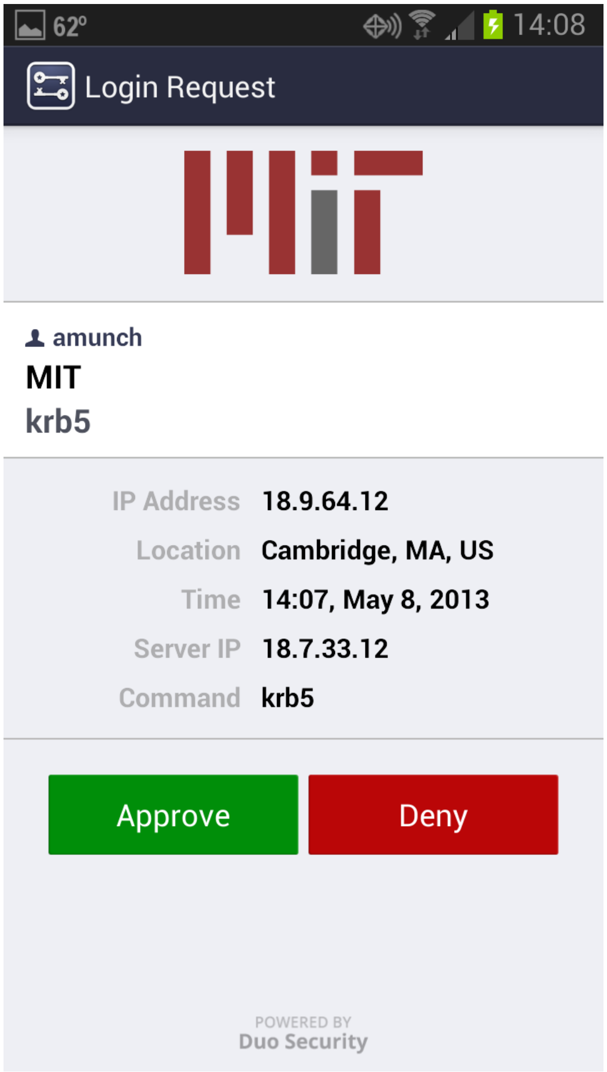
In this example, we've entered "1" as the option.
Note: You will not see any input on the screen as you type.

4. Duo will now output, "Press return after completing Duo authentication."



```
all-night-tool:~> kinit amunch/root
Password for amunch/root@ATHENA.MIT.EDU:
SAM Authentication
Challenge from authentication server
Duo login: Passcode/option or press return for options:
SAM Authentication
Challenge from authentication server
 1. Duo Push to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
 2. Phone call to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
 3. SMS passcodes to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
Passcode or option (1-3):
SAM Authentication
Challenge from authentication server
Press return after completing Duo authentication: _
```

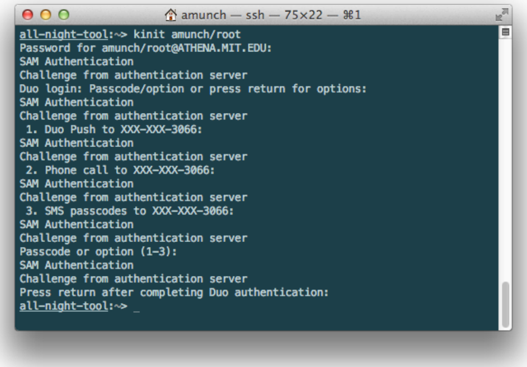
5. In this example, you will receive a push notification on your cell phone. Click **Approve**.



amunch
MIT
krb5

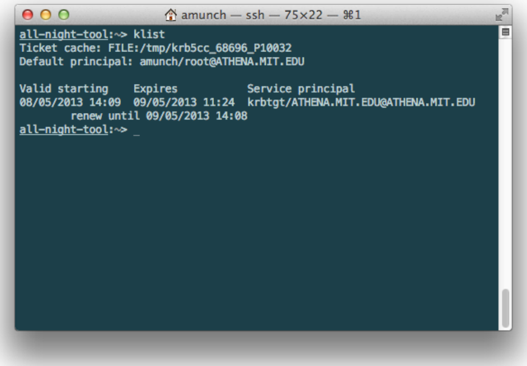
IP Address	18.9.64.12
Location	Cambridge, MA, US
Time	14:07, May 8, 2013
Server IP	18.7.33.12
Command	krb5

6. Back in your console window, click the **Enter** key.
7. If you have not received any error messages, you should be back at the > prompt and have valid Kerberos tickets.



```
all-night-tool:~> kinit amunch/root
Password for amunch/root@ATHENA.MIT.EDU:
SAM Authentication
Challenge from authentication server
Duo login: Passcode/option or press return for options:
SAM Authentication
Challenge from authentication server
 1. Duo Push to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
 2. Phone call to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
 3. SMS passcodes to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
Passcode or option (1-3):
SAM Authentication
Challenge from authentication server
Press return after completing Duo authentication:
all-night-tool:~> _
```

8. You can view your Kerberos tickets by running `klist` from within your console window.



```
all-night-tool:~> klist
Ticket cache: FILE:/tmp/krb5cc_68696_P10032
Default principal: amunch/root@ATHENA.MIT.EDU

Valid starting    Expires           Service principal
08/05/2013 14:09  09/05/2013 11:24  krbtgt/ATHENA.MIT.EDU@ATHENA.MIT.EDU
        renew until 09/05/2013 14:08
all-night-tool:~> _
```

Also See
Configuring MacPorts Kerberos for Duo Authentication