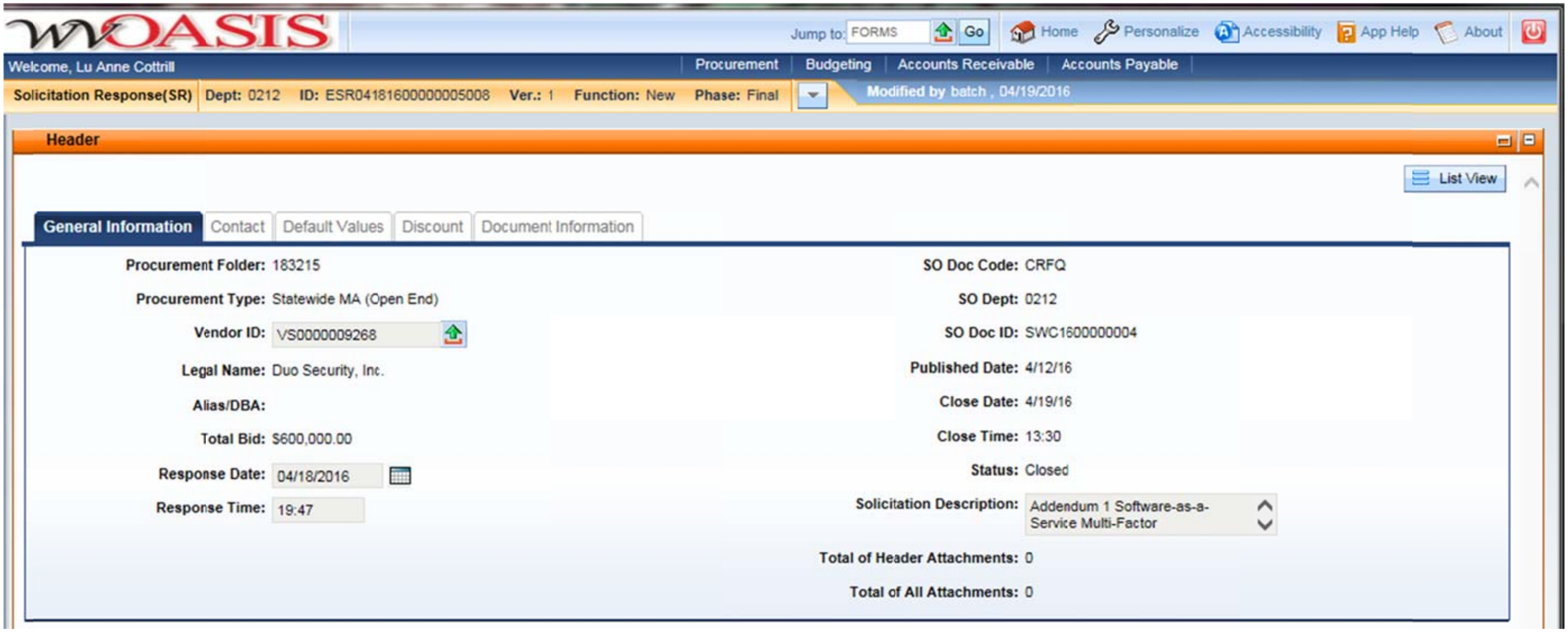
West Virginia
Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.



Welcome, Lu Anne Cottrill

Solicitation Response(SR) Dept: 0212 ID: ESR04181600000005008 Ver.: 1 Function: New Phase: Final

Modified by batch , 04/19/2016

Header

Procurement Folder:	183215
Procurement Type:	Statewide MA (Open End)
Vendor ID:	VS0000009268
Legal Name:	Duo Security, Inc.
Alias/DBA:	
Total Bid:	$600,000.00
Response Date:	04/18/2016
Response Time:	19:47

SO Doc Code:	CRFQ
SO Dept:	0212
SO Doc ID:	SWC1600000004
Published Date:	4/12/16
Close Date:	4/19/16
Close Time:	13:30
Status:	Closed
Solicitation Description:	Addendum 1 Software-as-a-Service Multi-Factor
Total of Header Attachments:	0
Total of All Attachments:	0

Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder : 183215

Solicitation Description : Addendum 1 Software-as-a-Service Multi-Factor Authentication

Proc Type : Statewide MA (Open End)

Date issued	Solicitation Closes	Solicitation No	Version
	2016-04-19 13:30:00	SR 0212 ESR04181600000005008	1

VENDOR

VS0000009268

Duo Security, Inc.

FOR INFORMATION CONTACT THE BUYER

Stephanie L Gale

(304) 558-8801
stephanie.l.gale@wv.gov

Signature X **FEIN #** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	3.1.1 Software as a Service Capabilities (SaaS) Account	5000.00000	EA	$48.000000	$240,000.00

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :	
	Pricing shall be per "account" for a two (2) year initial period.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	3.1.2.1 Optional Renewal of SaaS (One Year) Year "3"	5000.00000	EA	$24.000000	$120,000.00

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :	
	Pricing shall be per "account" for a one (1) year period.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	3.1.2.2 Optional Renewal of SaaS (One Year) Year "4"	5000.00000	EA	$24.000000	$120,000.00

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :	
	Pricing shall be per "account" for a one (1) year period.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	3.1.2.3 Optional Renewal of SaaS (One Year) Year "5"	5000.00000	EA	$24.000000	$120,000.00

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :	
	Pricing shall be per "account" for a one (1) year period.

Duo Security Proposal

State of West Virginia Authentication Project

Duo Security Contacts

Jeremy Gentry – Account Executive

jgentry@duosecurity.com | 404.889.3787

Jeff Smith – Enterprise Solutions Engineer

jsmith@duosecurity.com | 734.217.4637

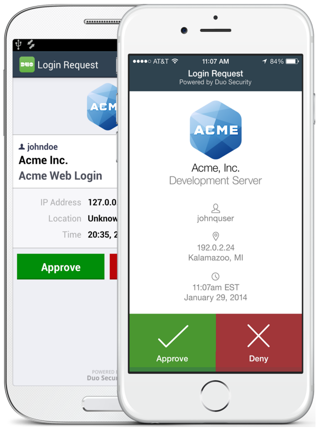
Duo Security Overview

With today’s complex IT environments, protecting access to critical systems without compromising the productivity of business users is a must. The average professional uses multiple devices to access dozens of applications from any number of locations and networks. For IT teams, this means more to manage when you’re trying to keep valuable business data secure.

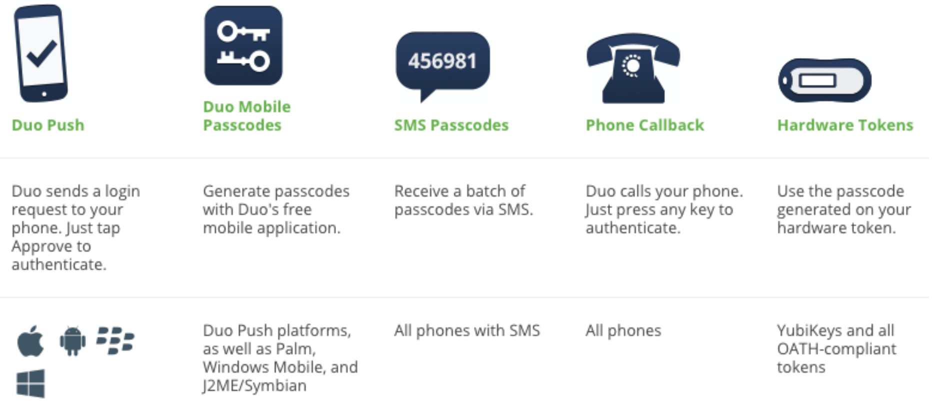
Duo Security puts organizations back in control of how their applications and data are being accessed. Duo Security provides the world's easiest two-factor authentication service with policy and control over which users, devices, and networks are permitted to access organization applications. Duo analyzes user behavior, location, and device parameters and gives you the power to set more precise authentication policies. This lets you better secure your users without inconveniencing them.

Easy to Use

Duo Security’s two-factor authentication service provides the best user experience available for two-factor authentication. With Duo Mobile a user completes a login with a single tap approval. The Duo Mobile application is available on all major smartphone platforms including iPhone, Android, BlackBerry, and Windows Phone.



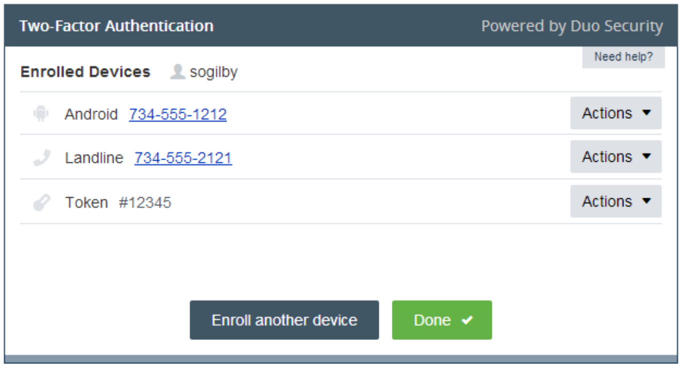
Duo Security allows the user to chose their preferred authentication method during login allowing them the flexibility to use a Smartphone, Tablet, Cell phone, Landline, Landline w/ extension or hardware token at any time.



Duo Push	Duo Mobile Passcodes	SMS Passcodes	Phone Callback	Hardware Tokens
Duo sends a login request to your phone. Just tap Approve to authenticate.	Generate passcodes with Duo's free mobile application.	Receive a batch of passcodes via SMS.	Duo calls your phone. Just press any key to authenticate.	Use the passcode generated on your hardware token.
	Duo Push platforms, as well as Palm, Windows Mobile, and J2ME/Symbian	All phones with SMS	All phones	YubiKeys and all OATH-compliant tokens

Easy to Manage

Empower your users with the ability to manage their authentication devices through Duo Security's self-service portal for your integrations. The self-service portal saves time for both administrators and end users by eliminating the need to contact IT staff for authentication device changes. Your users can add, edit, and remove authentication factors.



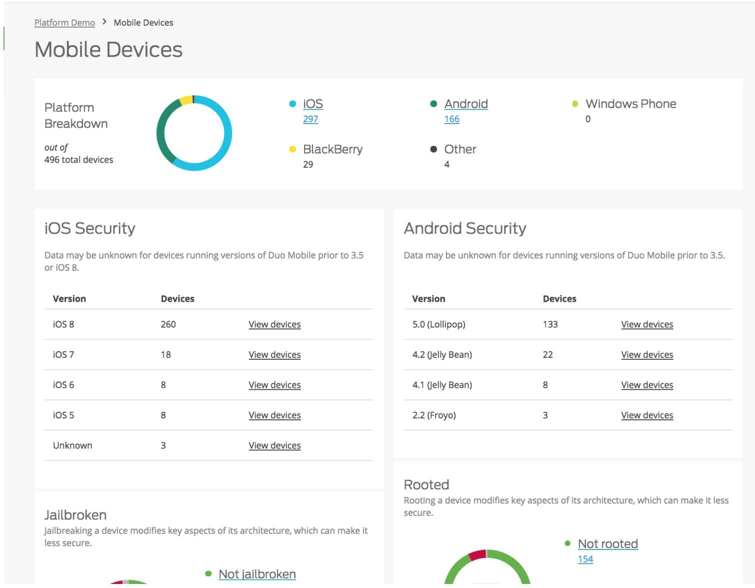
Two-Factor Authentication — Powered by Duo Security

Need help?

Enrolled Devices — sogilby

Android 734-555-1212	Actions ▾
Landline 734-555-2121	Actions ▾
Token #12345	Actions ▾

Gain greater visibility and control with Duo's Mobile Insight. Find out who's accessing what company applications, and under what conditions. Measure your organization's endpoint security health by analyzing meaningful attributes of your users' mobile and PC devices - without requiring any agents on their devices.



Platform Demo > Mobile Devices

Mobile Devices

Platform Breakdown

out of
496 total devices

● iOS 297	● Android 166	● Windows Phone 0
● BlackBerry 29	● Other 4	

iOS Security

Data may be unknown for devices running versions of Duo Mobile prior to 3.5 or iOS 8.

Version	Devices	
iOS 8	260	View devices
iOS 7	18	View devices
iOS 6	8	View devices
iOS 5	8	View devices
Unknown	3	View devices

Android Security

Data may be unknown for devices running versions of Duo Mobile prior to 3.5.

Version	Devices	
5.0 (Lollipop)	133	View devices
4.2 (Jelly Bean)	22	View devices
4.1 (Jelly Bean)	8	View devices
2.2 (Froyo)	3	View devices

Jailbroken

Jailbreaking a device modifies key aspects of its architecture, which can make it less secure.

● Not jailbroken

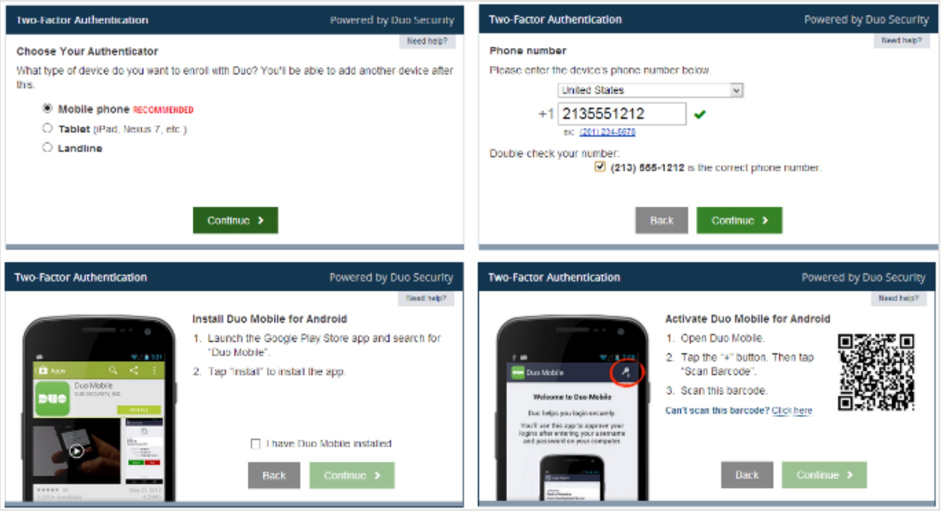
Rooted

Rooting a device modifies key aspects of its architecture, which can make it less secure.

● Not rooted
154

Easy to Deploy

Duo Security's enrollment options provide organizations with the flexibility to choose which enrollment method works best. Commonly customers choose Duo Security's self-enrollment process which makes it easy for users to register their smartphone, cellphone, landline or tablet further reducing support costs for deployment.



Choose Your Authenticator

What type of device do you want to enroll with Duo? You'll be able to add another device after this.

● **Mobile phone** RECOMMENDED
○ **Tablet** (iPad, Nexus 7, etc.)
○ **Landline**

Phone number

Please enter the device's phone number below.

United States

+1 2135551212 ✓

ex: (201) 234-5678

Double-check your number:
☑ **(213) 555-1212** is the correct phone number.

Install Duo Mobile for Android

1. Launch the Google Play Store app and search for "Duo Mobile".
2. Tap "Install" to install the app.

□ I have Duo Mobile installed

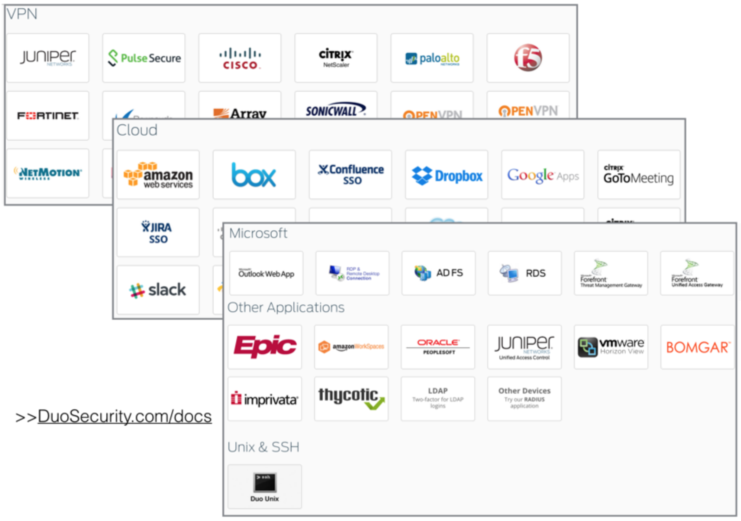
Back
Continue ›
Two-Factor Authentication
Powered by Duo Security
Need help?
Duo Mobile
Welcome to Duo Mobile
Duo helps you login securely.
You'll use this app to approve your logins after entering your username and password on your computer.

Activate Duo Mobile for Android

1. Open Duo Mobile.
2. Tap the "+" button. Then tap "Scan Barcode".
3. Scan this barcode.

Can't scan this barcode? Click here

Easily protect any service with Duo’s drop-in Integrations and support for any application. Full Documentation is publicly available at duosecurity.com/docs.

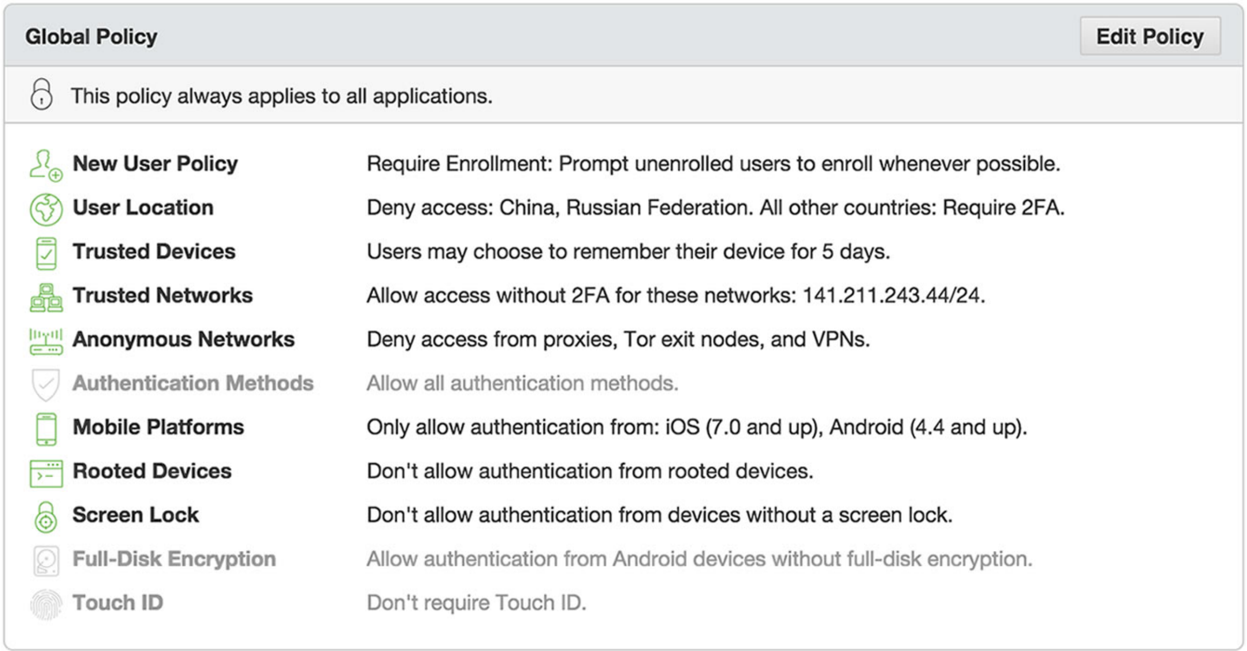


>>DuoSecurity.com/docs

Easy to Secure

Duo lets you easily define access policies appropriate for your organization’s users and applications. Allow, deny or require two-factor authentication for every authentication attempt, depending on certain conditions and how they are configured per application and user group.

Specify expected user locations, Allow or Deny specific networks and enforce device policy without agents. All easily controllable and enforceable with Duo’s policy and controls.



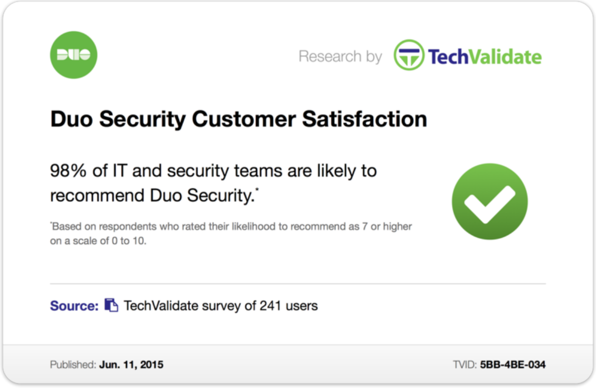
Global Policy

This policy always applies to all applications.

New User Policy	Require Enrollment: Prompt unenrolled users to enroll whenever possible.
User Location	Deny access: China, Russian Federation. All other countries: Require 2FA.
Trusted Devices	Users may choose to remember their device for 5 days.
Trusted Networks	Allow access without 2FA for these networks: 141.211.243.44/24.
Anonymous Networks	Deny access from proxies, Tor exit nodes, and VPNs.
Authentication Methods	Allow all authentication methods.
Mobile Platforms	Only allow authentication from: iOS (7.0 and up), Android (4.4 and up).
Rooted Devices	Don't allow authentication from rooted devices.
Screen Lock	Don't allow authentication from devices without a screen lock.
Full-Disk Encryption	Allow authentication from Android devices without full-disk encryption.
Touch ID	Don't require Touch ID.

Thousands Trust Duo Security

Duo makes it radically easy to deploy and manage two-factor authentication. This easy of use has allowed Duo to achieve a 98% customer satisfaction rating with TechValidate.



Research by TechValidate

Duo Security Customer Satisfaction

98% of IT and security teams are likely to recommend Duo Security.*

*Based on respondents who rated their likelihood to recommend as 7 or higher on a scale of 0 to 10.

Source: TechValidate survey of 241 users

Published: **Jun. 11, 2015** TVID: **5BB-4BE-034**

Duo has also worked with several of their satisfied customers to create case studies on why they choose Duo for their two-factor authentication solution. The full list of Duo's case studies is available online at duosecurity.com/success-stories.

Day & Zimmermann | Case Study

With hundreds of utility, nuclear power and government customers, D&Z knew they needed to find an easy and effective security solution to protect their customers. Read more…

Safelite | Case Study

Safelite chose Duo for their extensive documentation and to eliminate the expense of buying hardware tokens. Read more…

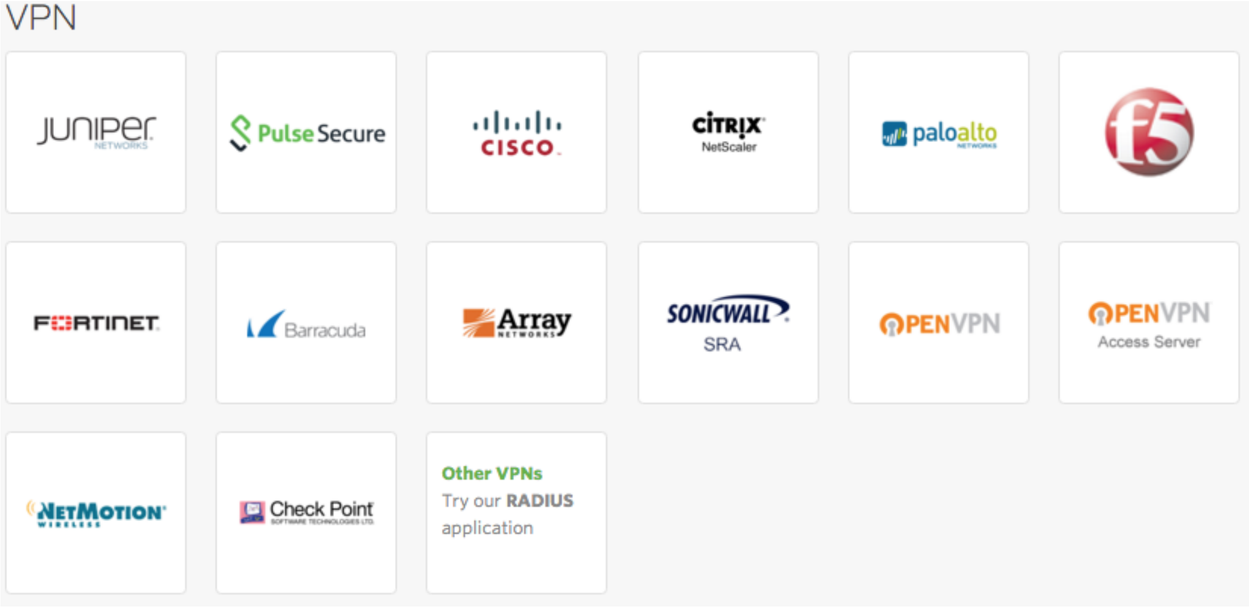
3.1 Mandatory Contract Item Requirements: Vendor shall provide Agency with the Contract Items listed below on an open-end and continuing basis. Contract Items must meet or exceed the mandatory requirements as shown below.

3.1.1 Software as a Service Capabilities (SaaS). The SaaS must include the following:

3.1.1.1 Vendor must be listed in Gartner's 2014 Magic Quadrant for User Authentication.

3.1.1.2 Must be fully integrated with the existing Remote Access: Virtual Private Network (VPN) solution utilized by the State.

Duo's solution seamlessly integrates with some of the largest VPN providers, including Juniper, Cisco, Palo Alto and more.

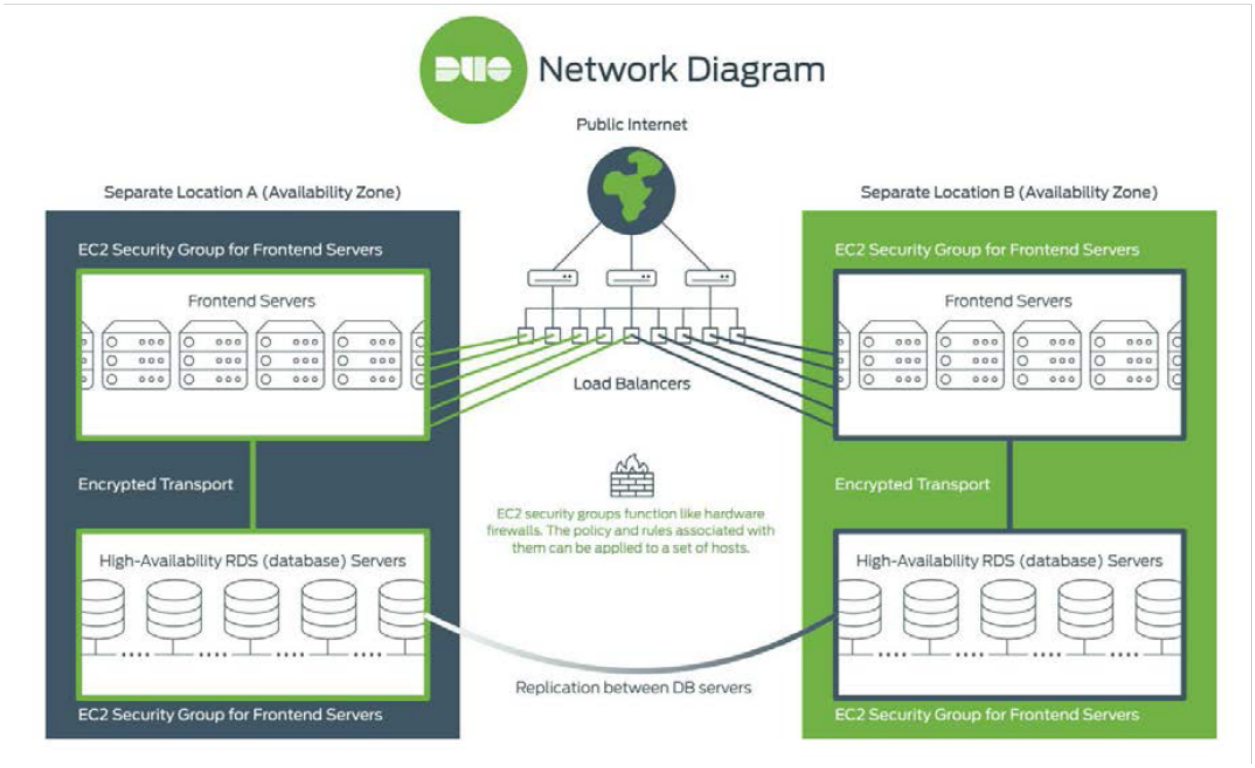


3.1.1.2.1 Solution must adhere to Level 3 specifications of NIST Special Publication 800-63-2, Electronic Authentication Guideline.

Duo Security's 2FA is an LOA 3 solution that is a significantly better fit for the business needs and threat model of many organizations.

3.1.1.3 Must be configured for high-availability (HA).

Duo's high availability service is architected to offer world class availability, uptime and seamless end-user experience. Based on the flexible and scalable Amazon EC2 environment, Duo is hosted in multiple regions and multiple availability zones.


Network Diagram
Public Internet
Separate Location A (Availability Zone)
Separate Location B (Availability Zone)
EC2 Security Group for Frontend Servers
Frontend Servers
Load Balancers
Encrypted Transport
High-Availability RDS (database) Servers
Replication between DB servers
EC2 Security Group for Frontend Servers
EC2 Security Group for Frontend Servers
Frontend Servers
Encrypted Transport
High-Availability RDS (database) Servers
EC2 Security Group for Frontend Servers

EC2 security groups function like hardware firewalls. The policy and rules associated with them can be applied to a set of hosts.

3.1.1.4 Must provide customer data protection through data-at rest and data-in-transit encryption.

All Duo integrations are mutually-authenticated and speak over SSL-encrypted channels to Duo's hosted service. Duo provides 2-factor authentication and does not handle any PII. Encryption at rest is also available.

3.1.1.5 The vendor must provide the State, at minimum annually, third party information security audit(s) and be willing to share results of those audits(s).

Duo has completed multiple security audits by external third parties. Bi-annual external security audits are performed by firms such as Matasano and iSEC partners.

Audits of Duo security can be provided under NDA.

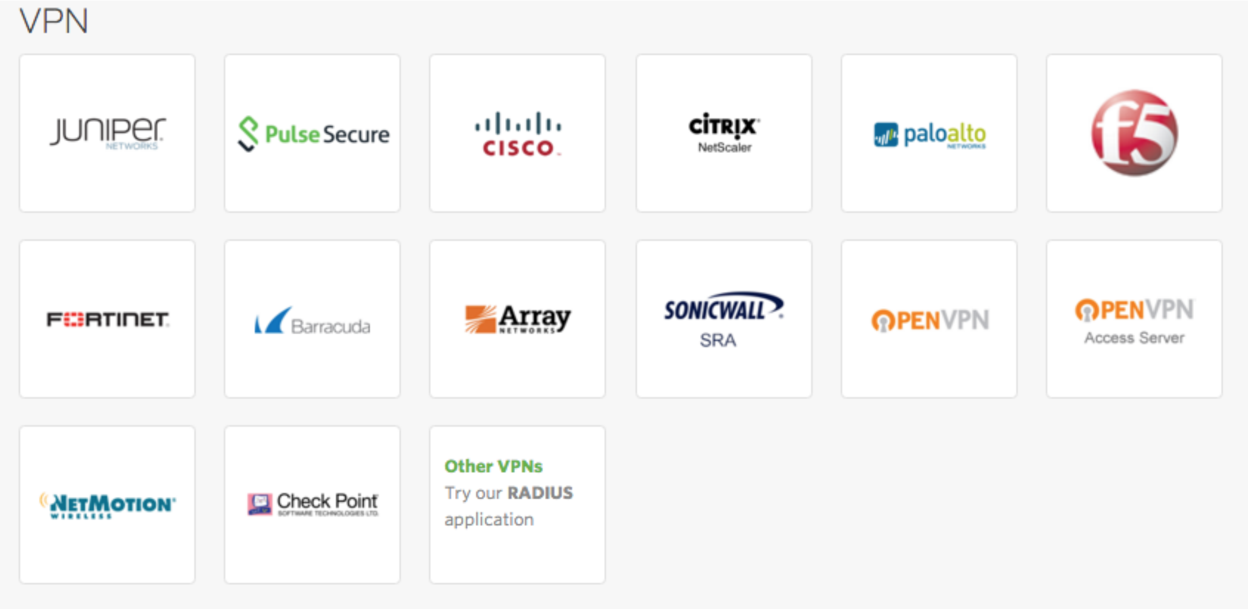
3.1.1.6 The vendor must provide documentation outlining the use of any third party cloud services used by the vendor for the State.

3.1.1.7 The Vendor shall notify the State concerning the discovery of critical vulnerability and security incidents that potentially jeopardize the confidentiality, integrity and availability of the SaaS. Notification shall be implemented and confirmed within twenty-four (24) hours following confirmation of the event.

3.1.1.8 Multi-factor Authentication Support. Must support multi-factor authentication integration with the following applications & services at no additional charge:

3.1.1.8.1 Remote Access/Virtual Private Network (VPN)

Duo's solution seamlessly integrates with some of the largest VPN providers, including Juniper, Cisco, Palo Alto Networks and more.
Documentation: https://duo.com/docs



Other VPNs
Try our RADIUS application

3.1.1.8.2 Microsoft Outlook, Forefront, Remote Desktop Protocol, Active Directory Federation Services (ADFS) and Office 365.

Microsoft Outlook
Duo offers a variety of methods for adding two-factor authentication and flexible security policies to Microsoft Office Suite logins.
Documentation: https://duo.com/docs/o365#office-clients

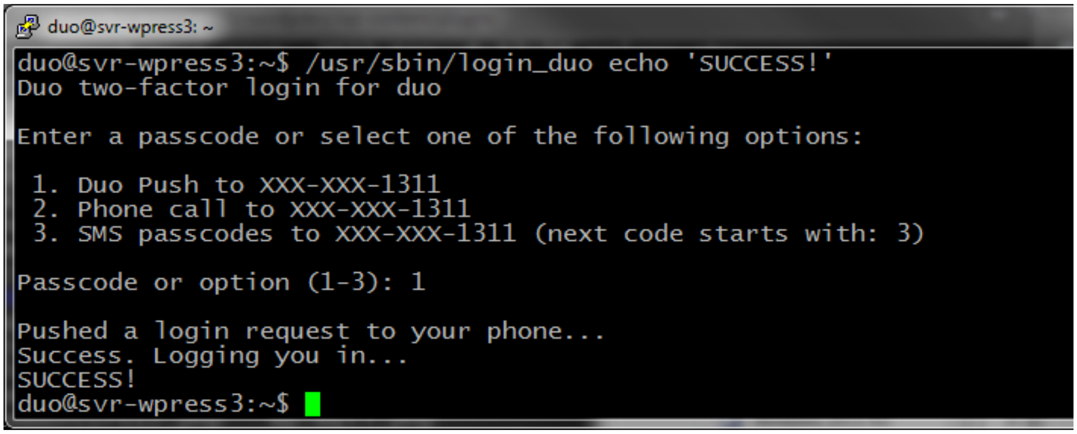
Remote Desktop Protocol
Duo integrates with Microsoft Windows client and server operating systems to add two-factor authentication to Remote Desktop and local logons.
Documentation: https://duo.com/docs/rdp

ADFS
Duo integrates with Microsoft ADFS to add two-factor authentication to services using browser-based federated logins, complete with inline self-service enrollment and authentication prompt.
Documentation: https://duo.com/docs/adfs

Office 365
Duo offers a variety of methods for adding two-factor authentication and flexible security policies to Office 365 SSO logins.
Documentation: https://duo.com/docs/o365

3.1.1.8.3 Unix – Secure Socket Shell (SSH)

Duo can be enabled on any Unix system with the addition of a simple pam_duo PAM module to add two-factor authentication.

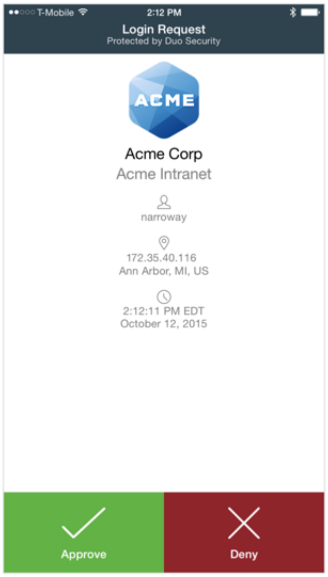


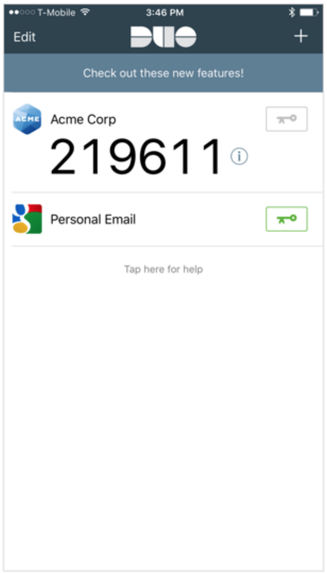
```
duo@svr-wpress3:~$ /usr/sbin/login_duo echo 'SUCCESS!'
Duo two-factor login for duo

Enter a passcode or select one of the following options:

 1. Duo Push to XXX-XXX-1311
 2. Phone call to XXX-XXX-1311
 3. SMS passcodes to XXX-XXX-1311 (next code starts with: 3)

Passcode or option (1-3): 1

Pushed a login request to your phone...
Success. Logging you in...
SUCCESS!
duo@svr-wpress3:~$
```

3.1.1.9 Second Factor Authentication Requirements. The "something you have" factor must support:

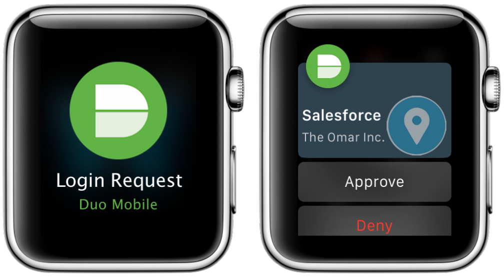
3.1.1.9.1 No-cost, vendor-provided mobile phone application compatible with the latest Apple, Android and Windows mobile phone operating systems.

Duo Push and Duo Mobile passcodes are available on all major smartphone platforms including iPhone, Android, BlackBerry, and Windows Phone at no cost.





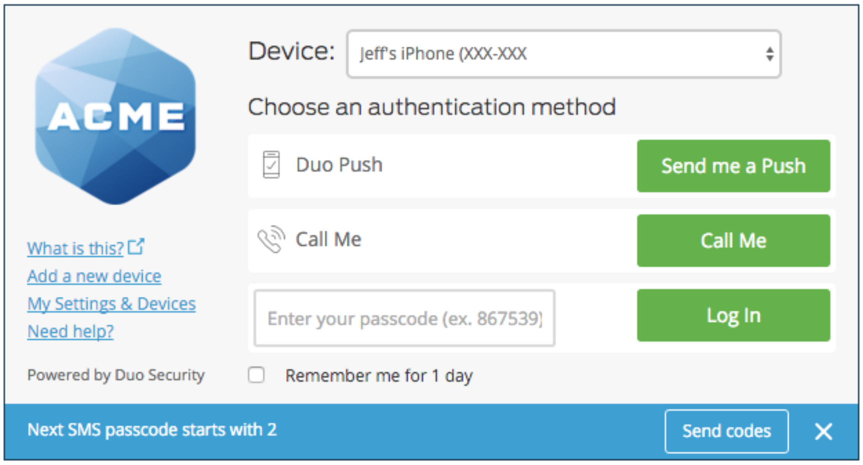
Duo also allows users to leverage wearables such as the Apple Watch as an authenticator.



3.1.1.9.2 Non-proprietary hardware tokens.
Duo Security supports standalone, one-time password hardware tokens for two-factor authentication; choose from either USB devices or tokens. These tokens are non-proprietary.

3.1.1.9.3 Short Message Service (SMS) passcode authentication.

Duo can text you passcodes via SMS. If you need a new batch of passcodes choose "Send Codes" (or type "sms" in the "second password" field).


ACME

Device: Jeff's iPhone (XXX-XXX

Choose an authentication method

Duo Push — Send me a Push

Call Me — Call Me

Enter your passcode (ex. 867539) — Log In

What is this?
Add a new device
My Settings & Devices
Need help?

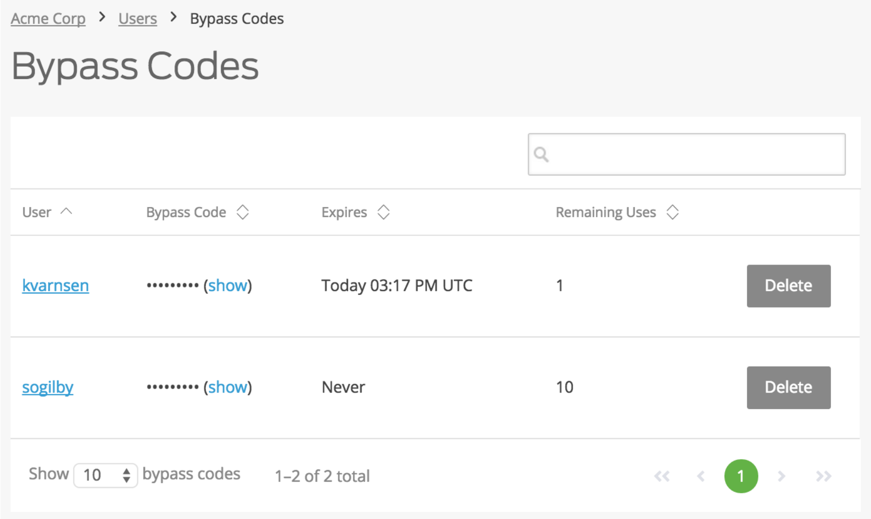
Powered by Duo Security

□ Remember me for 1 day

Next SMS passcode starts with 2 — Send codes ✕

3.1.1.9.4 System-generated backup codes.

Bypass codes, or backup codes, can be generated by administrators using Duo’s administrative interface or API. Users that are having difficulty with their mobile devices or tokens can still log into their applications.
Documentation: https://duo.com/docs/administration-users#generating-a-bypass-code



Acme Corp > Users > Bypass Codes

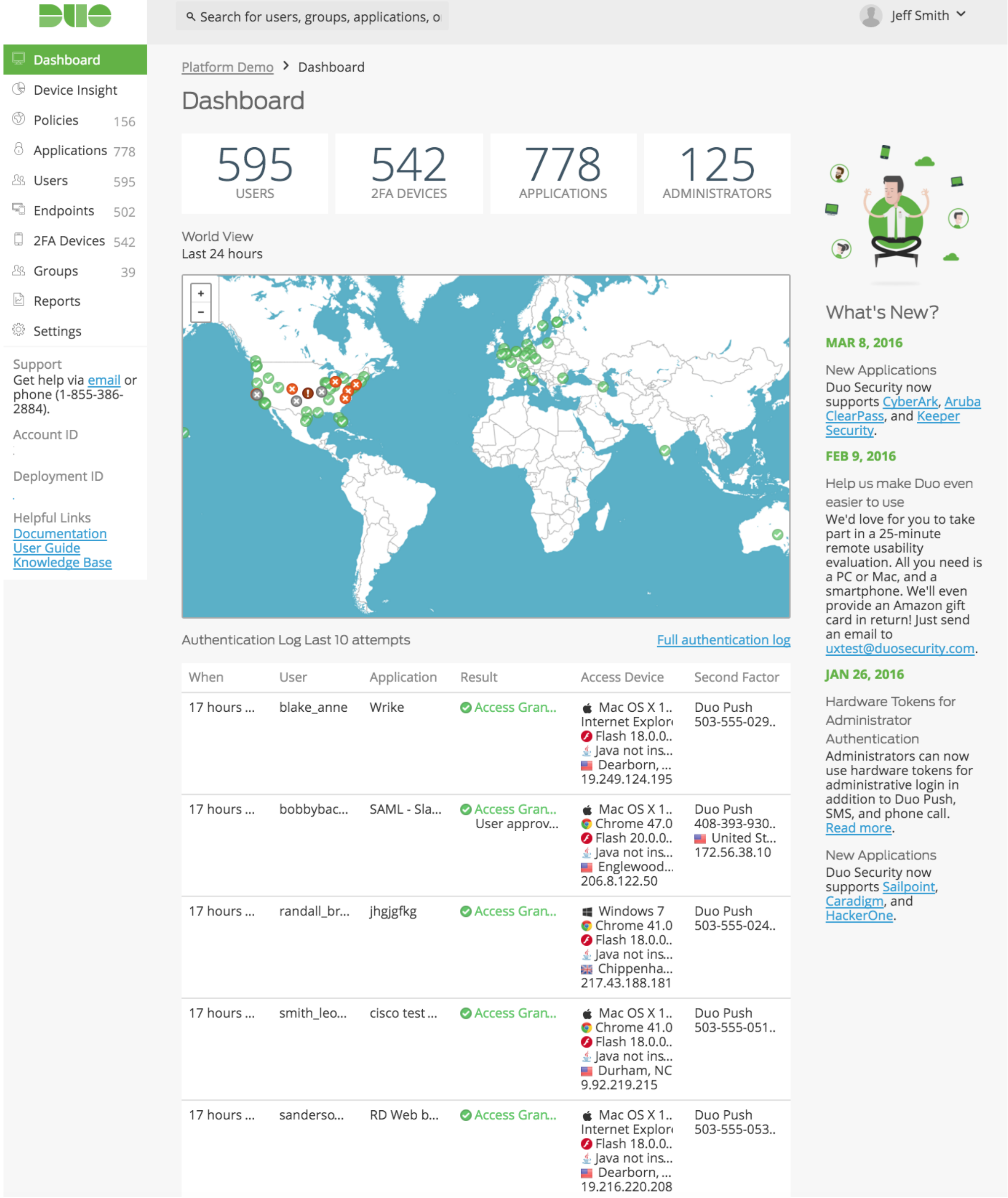
Bypass Codes

User	Bypass Code	Expires	Remaining Uses	
kvarnsen	••••••••• (show)	Today 03:17 PM UTC	1	Delete
sogilby	••••••••• (show)	Never	10	Delete

Show 10 bypass codes 1–2 of 2 total

3.1.1.10 Account Management Capabilities. The vendor must include the following capabilities for account management:

3.1.1.10.1 Multi-factor authentication access control for account management console. Every aspect of your Duo two-factor authentication system can be managed from the Duo Admin Panel. This includes creating and managing applications, enrolling and activating users, issuing and managing SMS passcodes and bypass codes, managing mobile devices, fine-tuning the user experience of your Duo installation, and more. The Duo Admin Panel is secured with two-factor authentication.



Dashboard	
Device Insight	
Policies	156
Applications	778
Users	595
Endpoints	502
2FA Devices	542
Groups	39
Reports	
Settings	

Support
Get help via email or phone (1-855-386-2884).

Account ID

Deployment ID

Helpful Links
Documentation
User Guide
Knowledge Base

Platform Demo > Dashboard

Dashboard

595	542	778	125
USERS	2FA DEVICES	APPLICATIONS	ADMINISTRATORS

World View
Last 24 hours

Authentication Log Last 10 attempts

Full authentication log

When	User	Application	Result	Access Device	Second Factor
17 hours ...	blake_anne	Wrike	✓ Access Gran...	Mac OS X 1.. Internet Explor Flash 18.0.0.. Java not ins... Dearborn, ... 19.249.124.195	Duo Push 503-555-029..
17 hours ...	bobbybac...	SAML - Sla...	✓ Access Gran... User approv...	Mac OS X 1.. Chrome 47.0 Flash 20.0.0.. Java not ins... Englewood... 206.8.122.50	Duo Push 408-393-930.. United St... 172.56.38.10
17 hours ...	randall_br...	jhgjgfkg	✓ Access Gran...	Windows 7 Chrome 41.0 Flash 18.0.0.. Java not ins... Chippenha... 217.43.188.181	Duo Push 503-555-024..
17 hours ...	smith_leo...	cisco test ...	✓ Access Gran...	Mac OS X 1.. Chrome 41.0 Flash 18.0.0.. Java not ins... Durham, NC 9.92.219.215	Duo Push 503-555-051..
17 hours ...	sanderso...	RD Web b...	✓ Access Gran...	Mac OS X 1.. Internet Explor Flash 18.0.0.. Java not ins... Dearborn, ... 19.216.220.208	Duo Push 503-555-053..

What's New?

MAR 8, 2016

New Applications
Duo Security now supports CyberArk, Aruba ClearPass, and Keeper Security.

FEB 9, 2016

Help us make Duo even easier to use
We'd love for you to take part in a 25-minute remote usability evaluation. All you need is a PC or Mac, and a smartphone. We'll even provide an Amazon gift card in return! Just send an email to uxtest@duosecurity.com.

JAN 26, 2016

Hardware Tokens for Administrator Authentication
Administrators can now use hardware tokens for administrative login in addition to Duo Push, SMS, and phone call. Read more.

New Applications
Duo Security now supports Sailpoint, Caradigm, and HackerOne.

3.1.1.10.2 Reporting capability for authentication logging and administrative actions.

Duo provides portal access to authentication, administrative, and telephony logs. Administrators can search or export these reports via CSV or JSON or to a log management or SIEM via our AdminAPI.

Authentication logs provide a date/timestamp, the user, the application accessed, the result of the authentication request, the access device used, and the second factor method. By normalizing the pattern of user, you can be alerted if abnormal activity occurs.

Administrator log events let you track the username, time and type of administrator activity, including groups, user, integration and device management. This lets you know if any major administrative changes occur, and if there's any suspicious administrative activity.

Telephony logs give you insight into the type of telephony event (SMS or phone), phone numbers, and the number of telephony credits used.

The logs may be exported to a log management system using the Admin API. Documentation for accessing the logs via the Admin API are available here: https://duo.com/docs/adminapi#logs

An example script for importing logs into Splunk are available on Github: https://github.com/duosecurity/duo_client_python/tree/master/examples/splunk

3.1.1.10.3 Administrative management console application program interface (API).

Duo's REST based Admin API provides programmatic access to the administrative functionality of Duo Security's two-factor authentication platform.

The Admin API lets developers integrate with Duo Security's platform at a low level. The API has methods for creating, retrieving, updating, and deleting the core objects in Duo's system: users, phones, hardware tokens, admins, and integrations.

In addition, developers can write applications that programmatically read their Duo account's authentication logs, administrator logs, and telephony logs; read or update account settings; and retrieve reports and other information.

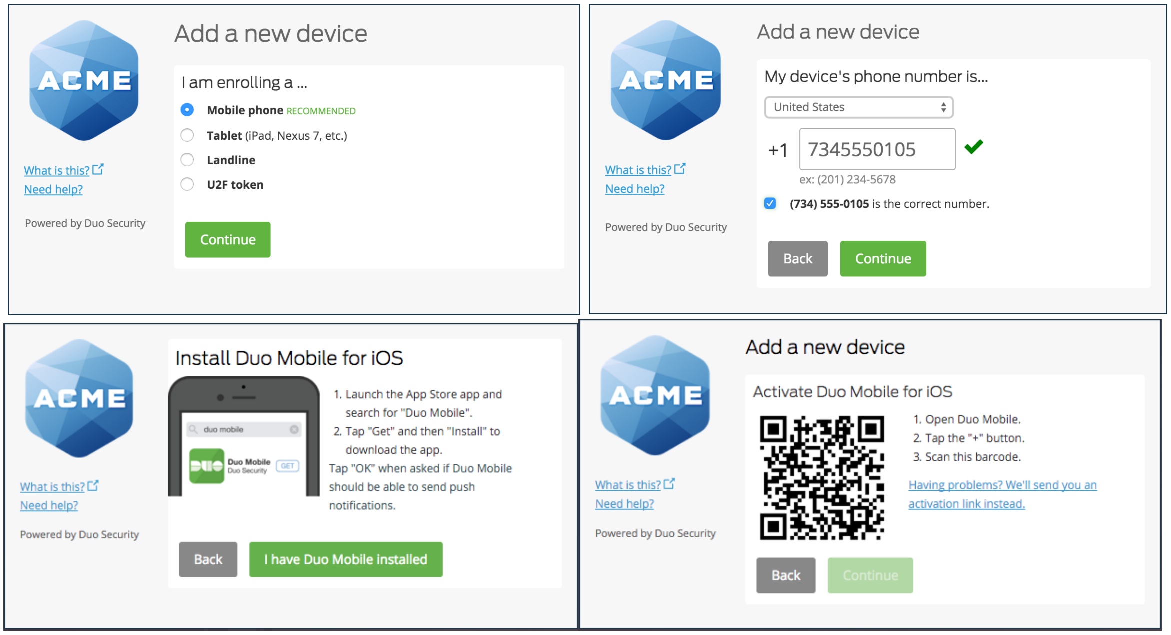
Documentation: https://duo.com/docs/adminapi

3.1.1.11 Self-service Portal Capabilities. The vendor must include the following capabilities for user self-service:

3.1.1.11.1 Ability for user self-enrollment.

Duo's flexible provisioning options also provide end users the ability to self-enroll in-line as they are accessing applications with little to no training needed. End users are also able to walk through the same enrollment process through enrollment links send to their email.

Enrollment Options: https://duo.com/docs/enrolling_users



Add a new device

I am enrolling a ...

● Mobile phone RECOMMENDED
○ Tablet (iPad, Nexus 7, etc.)
○ Landline
○ U2F token

Add a new device

My device's phone number is...

United States

+1 7345550105 ✓

ex: (201) 234-5678

☑ (734) 555-0105 is the correct number.

Install Duo Mobile for iOS

1. Launch the App Store app and search for "Duo Mobile".
2. Tap "Get" and then "Install" to download the app.

Tap "OK" when asked if Duo Mobile should be able to send push notifications.

Add a new device

Activate Duo Mobile for iOS

1. Open Duo Mobile.
2. Tap the "+" button.
3. Scan this barcode.

Having problems? We'll send you an activation link instead.

3.1.1.11.2 Custom branding capability.

Duo provides customers the ability to brand the enrollment, authentication prompt, and Duo Push notification with a custom logo and customer name.

3.1.1.12 Subscription and Services:

3.1.1.12.1 Enterprise Edition subscription “or Equal”.

Please refer to pricing XLS also attached to bid

3.1.1.12.2 Vendor must bill based upon a per user account, per month basis.

Please refer to pricing XLS also attached to bid

Exhibit A - Multi-Factor Authentication (SaaS)

Pricing Sheet

Line Item Number	Item Name	Description	Alternative Item SKU	Alternative Item Name and Description	Unit of Measure	Quantity	Unit Price	Extended Unit Price
3.1		**Mandatory Contract Item Requirments**						
3.1.1	**Software as a Service Capabilities (SaaS) Account**	All items listed under "Software as a Service Capabilities (3.1.1)". Two (2) year initial implementation contract.		Enterprise Edition	User Account	5000	$24/user/year	$120k/year
3.1.2		**Renewal of Software as a Service Capabilities (SaaS)**						
3.1.2.1	**Software as a Service Capabilities (SaaS) Account**	**OPTIONAL RENEWAL YEAR 3**		Enterprise Edition	User Account	5000	$24/user/year	$120k/year
3.1.2.2	**Software as a Service Capabilities (SaaS) Account**	**OPTIONAL RENEWAL YEAR 4**		Enterprise Edition	User Account	5000	$24/user/year	$120k/year
3.1.2.3	**Software as a Service Capabilities (SaaS) Account**	**OPTIONAL RENEWAL YEAR 5**		Enterprise Edition	User Account	5000	$24/user/year	$120k/year
						Total Bid Price		$600,000