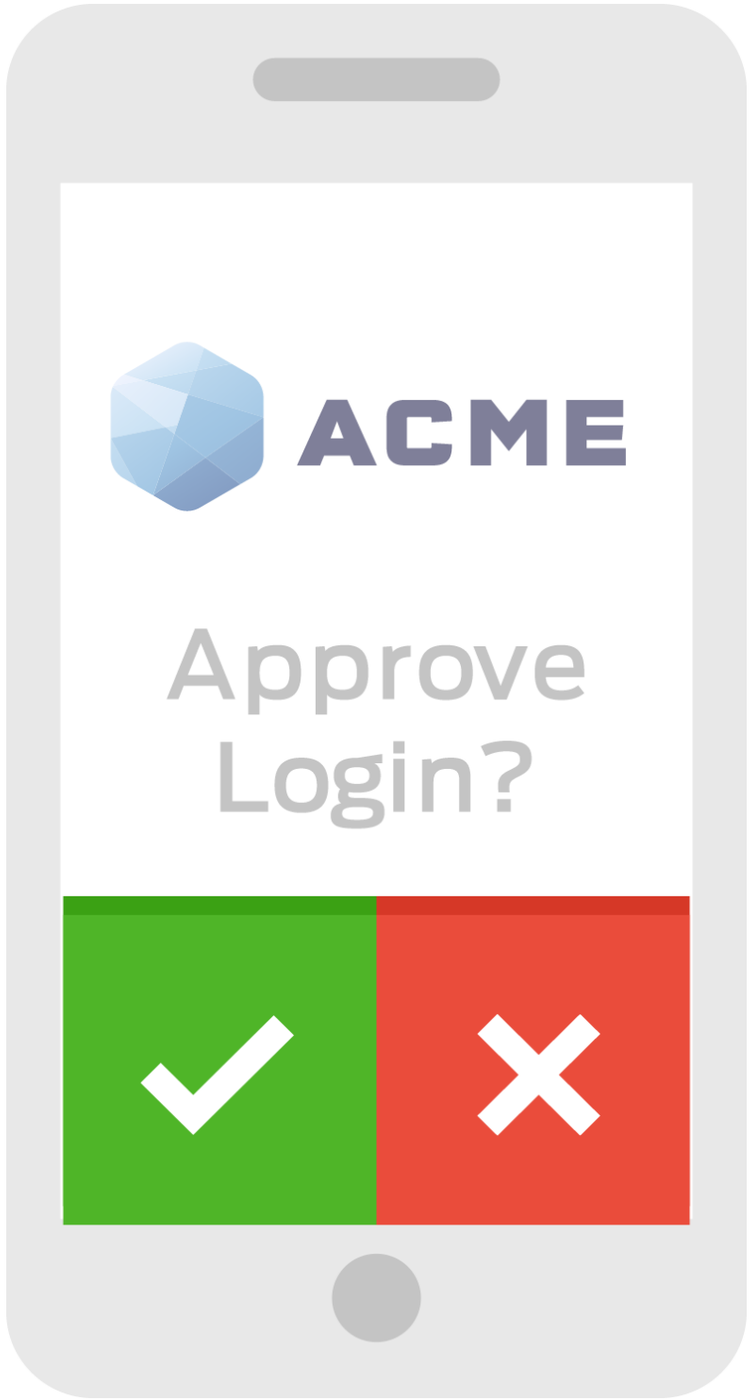
Two-Factor Authentication
Evaluation Guide

Learn what to look for when assessing and comparing two-factor authentication solutions.

A helpful guide from DUO

Two-Factor Authentication Evaluation Guide



In the physical world, we don't consider it odd when we're asked to confirm our identities before accessing facilities, funds, or high-value services. It's common to be asked to show a photo ID to enter a building, a passport to visit a country, or a driver's license when using a credit card. Many online systems and services require that added layer of protection, too.

One of the most foolproof ways for an online system to confirm, "Is it really you?" is by adding two-factor authentication. This provides a second identity check — preferably through a separate channel — before allowing access to an online system. Sounds simple enough, right? Of course, the devil is in the details, and not all two-factor authentication solutions are created equal.

This guide walks through some of the key area of differentiation between two-factor authentication solutions and provides some concrete criteria for evaluating technologies and vendors.

The primary areas of differentiation are:

- **Security.** Can the solution protect your users' accounts from takeover?
- **Ease of Implementation.** How easy/difficult is it to install, integrate with your existing systems, and deploy to your users?
- **Ease of Use.** Is it easy, convenient, and flexible enough that your users will adopt it successfully and use it consistently?
- **Ease of Administration.** Is it architected to reduce ongoing administration tasks? Is it powerful enough to detect—and allow you to react to—any security issues in real time?
- **Total Cost of Ownership.** What is the total cost when you fully account for acquisition, implementation, support, and operational costs over time?

Security & Reliability

The most critical aspect of an authentication solution is its underlying security and reliability. If a service can't do the job then it's not worth implementing (at any cost!). Assess the security, availability, and ultimate scalability of the options.

Security

- Does the service protect against advanced attacks such as Man-in-the-Middle (MITM) attacks?
- Does the service securely manage keys and exchange data?

Reliability

- Does the service have carrier-grade uptime?
- Is that uptime backed by an SLA?
- Does the service offer 24/7 operational coverage?

Scalability

- Can the solution grow with your organization to support a future number of users and authentications you may need?
- Can you add new users to the service at anytime?
- Can it handle your expected volumes in 3 years?

TO CONSIDER

Two-factor authentication effectively defends against remote credential theft and man-in-the-middle attacks.

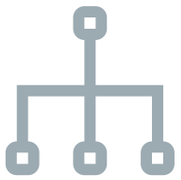
Make sure your vendor's service is secure by design with strong security for the service itself stored by the vendor.

Ensure that the vendor's cloud-based service uses multiple, independent PCI DSS Level 1 and ISO 27001-certified, SAS 70 Type II-audited service providers and is split across multiple geographic regions, service providers, and power grids for seamless failover.

Reliable vendors demonstrate 99.995% uptimes and should be backed by strong service level agreements (SLA).

The vendor's infrastructure should be fully scalable and elastic in order to accommodate any number of your users.

The vendor's subscription model should let you add users as you need them.



Ease of Implementation

Many two-factor authentication products require lengthy implementation phases, requiring special skills and consultants. Assess this area carefully and have your vendors walk through likely implementation scenarios with you. Cloud-based services tend to provide the fastest implementation times, while on-premises solutions tend to be the slowest. Also look into the time and cost associated with rolling out the solution to your user base.

Installation

- Can you use the service without installing a server?
- Does the service provide documentation and live support to help with installation?

Integration

- Does the service work natively with the types of access points in your environment?
- Does the service provide RADIUS-based integration?
- Does the service provide APIs that allow you to integrate to your custom systems or applications?

Deployment

- Does the solution require hardware or software be deployed to each user?
- Can users enroll themselves?
- Does the solution require extensive user training?

TO CONSIDER

Installation and deployment of on-premises solutions can be a major headache. Cloud-based authentication services are easy. They tend not to require installation of hardware or software.

Most security people don't want to write their own integration code. Select a vendor with drop-in integrations for all major VPNs, Unix, and MS remote access points; as well as a web SDK and APIs.

The best two-factor authentication services leverage something users already have, like their cell phones. Make sure that the service also works with landlines and tokens.

Evaluate a vendor's enrollment process. This could be a major time sink for an IT administrator. In some companies, managing tokens requires a dedicated resource. Easy self enrollment eliminates need to manually provision tokens, making it simple for everyone.

Look for a vendor with a subscription model that lets you add users as you need them.

Ease of Use

In the end, even the best security solutions can be defeated by grumpy users. The most effective solution will be the one your users actually use. The key here is to find a solution that doesn't get in the way of them doing their jobs — one that doesn't require lots of extra gizmos or steps in their login path. Usability, convenience, and flexibility are the key criteria that drive user adoption and impact productivity.

Usability

- Can users learn and use it without confusion?
- Is the authentication process at the remote access points clear and easy?
- Is the second factor itself easy to use?

Convenience

- Can users bring their own devices to use?
- Can users quickly authenticate in one tap to reduce interference with normal work activities?

Flexibility

- Will it work in all situations the user encounters? (e.g., with and without cell coverage)?
- Does it provide users with options (authentication methods) to match their circumstances?

TO CONSIDER

Users should be able to enroll themselves and set their preferred devices to use for authentication.

The authentication process should be part of their regular login process. Look for live status text to make it clear and easy to follow.

Test each vendors end-user experience for ease and speed. If it's hard for your users they might revolt.

Choose a solution that leverages something users already have: their mobile phones.

Make sure it also works with landlines and tokens - for that added flexibility in deployment models.

Most importantly ensure that the authentication process is fast and easy for users.

Make sure your vendor supports a range of authentication methods, including push (to a mobile app), passcodes (generated by a mobile app without Web access, a token, or sent via SMS), and phone callback.

Make sure you can give your users a choice. Allow them to flexibly choose the best authentication method to match their circumstances and preferences.

Ease of Administration

Like any good business tool, your two-factor authentication solution should give you the power you need to get the job done with a minimum of hassle. In particular, assess how well it will allow you to detect and react to threats, and whether it provides the necessary visibility and audit tools. In addition, be sure your chosen solution won't need its own babysitter. You may not want to set-it-and-forget-it, but you should be able to set-it-and-trust-it.

Detection

- Does the solution allow you to detect and react to security issues in real time?
- Does the solution allow you to set security policy at the level of granularity that ties to your business needs?
- Does it allow you to revoke and bypass credentials quickly and easily?

Reporting

- Does the solution give you visibility and actionable insight into user access of your network?
- Does the solution produce logs and audit trails you can work with?

Maintenance

- Are the ongoing maintenance tasks with the service minimal?
- Can you use existing staff to deploy and maintain this solution?
- Does the software/hardware itself need ongoing monitoring or tuning?

TO CONSIDER

Choose a solution that flags fraudulent behavior in real-time. Ideally your own users can help flag this behavior.

Make sure that the vendor's admin interface allows you to set your security policy, create and deactivate users and devices, and monitor all remote access.

The solution should provide real-time visibility into remote access and produce authentication logs for auditing and reporting.

If you want to keep your costs down, make sure that your solution requires minimal ongoing maintenance and management. Cloud-hosted solutions tend to have the lowest costs and hassles since the vendor maintains the infrastructure and handles all upgrades and maintenance.

Make sure you assess the ease of user management (adding and revoking credentials). Ideally you want a system that doesn't force you to manage or provision physical tokens.

Look for a system that provides a centralized admin interface to provide a unified, consolidated view of your two-factor deployments.

Total Cost of Ownership

Different pricing models often make it hard to quickly compare the costs of two-factor authentication solutions. Factor in your acquisition, implementation, and operating costs over a 1, 3, and 5 year window for each to get a sense of what your total cost of ownership for each will be.

Acquisition

- Does the service require additional hardware?
- Do I have to pay per device per user?
- Do I have to pay per integration?
- Does it require dedicated end-user devices? At what cost?

Implementation

- Will it cost extra to integrate the service with each of your systems?
- Can it get up and deployed using in-house resources?
- What will it cost to roll the solution out to your end-users in terms of setup and training?

Operating

- Is the service monitored for free as part of the subscription cost?
- Are routine tasks like adding new users, revoking credentials and replacing tokens simple enough to be negligible?
- Is support included in the subscription cost?

TO CONSIDER

Consider all of a vendor's costs in your analysis. Build a cost model that takes into account a "worst-case scenario" in which all of your applications and users require two-factor authentication.

Look for vendors with a simple subscription model. Watch out for setup fees, licensing fees, and hidden costs.

Vendors that leverage your users' phones as their authenticators will save you money. There's no need to acquire and provision separate tokens (unless you want to!).

Make sure that your vendor has drop-in integrations for all the major VPNs, Unix, MS and web apps, in addition to easy-to-use APIs for your custom systems.

Do an objective comparison to see how long it take to be up and running with a vendor's solution. Simple integrations should take no longer than 15 minutes.

One of the benefits of cloud-hosted services is that monitoring and maintenance is done by the service's network and security engineers.

Routine tasks, like managing users, should be simple. Be sure to take it for a test run to see for sure.

Live support via email, chat, and/or phone should all be part of the vendor's service.

The Duo Advantage

Duo Security makes two-factor authentication radically easy to deploy, manage and use. Duo empowers any network or web administrator to easily protect user accounts by leveraging your users' mobile phones for secondary authentication.

Security

Duo's two-factor authentication effectively defends against remote credential theft and man-in-the-middle attacks. Duo is secure in both design and implementation. From modern exploit mitigation and defensive programming techniques, to time-honored least-privilege, data classification, and compartmentalization strategies, every component of our technology and infrastructure is the result of a careful, considered, approach to secure systems design and engineering.

In addition, Duo's cloud-based service uses multiple, independent PCI DSS Level 1 and ISO 27001-certified, SAS 70 Type II-audited service providers and is split across multiple geographic regions, service providers, and power grids for seamless failover and scalability. Duo has had 99.995% uptime since 2010 and is backed by the best SLA in the industry.

Implementing

Duo is a cloud-based authentication service and requires no installation of hardware or software. Our drop-in integrations for all major VPNs, Unix and Microsoft remote access points, as well as our web SDK and APIs makes integrating Duo with your environment fast and easy. Many customers can get a remote access point integrated and live in 15 minutes.

Duo uses something your users already have — their phones — for authentication, so there's no need to acquire and provision separate tokens. We also provide an easy user self-enrollment process so that you don't have to provision each user manually. And our clear enrollment and authentication steps reduce the need for ongoing training or support.

Ease of Use

With Duo, authentication is fast and easy for users. Duo supports a range of authentication methods, including one-tap Push authentication, passcodes (generated by Duo Mobile, a token, or sent via SMS), and phone callback. Users can flexibly choose from among them when they log in to match their circumstances and preferences. The authentication process is part of their regular login process and live status text makes it clear and easy to follow and Duo Mobile and Duo Push provide unparalleled usability.

Administration

Duo's web-based admin interface allows you to set your security policy, create and deactivate users and devices, and monitor all remote access. The admin interface provides real-time visibility into remote access and well as authentication logs for auditing and reporting. Plus any login attempts your users flag as potentially fraudulent initiate real-time alerts to you.

Duo requires minimal ongoing maintenance and management. As a cloud-hosted solution, our network and security engineers maintain the infrastructure and handle upgrades and maintenance so you don't have to.

Cost

Duo is a cloud-based authentication service with a simple subscription model and no setup fees, hardware costs, licensing fees, or hidden costs. In addition, because Duo uses something your users already have—their phones—for authentication, you don't have to incur the cost of acquiring and managing tokens (unless you want to!)

Routine tasks, like managing users, are also simple using Duo's web-based admin interface and our cloud-hosted service is monitored and maintained by our network and security engineers. Live support via email, chat, or phone is all part of the Duo service as well.

About Duo Security

Duo Security is the easiest two-factor authentication service to deploy, administer, and use. Duo's service can be set up in as little as 15 minutes and used immediately by any user with a phone. Over 2,500 organizations in over 80 countries rely on Duo to prevent online account takeover and data theft. Backed by Google Ventures and True Ventures, Duo has been deployed by some of the most security-conscious organizations on the planet, including with 3 of the top 5 social networks.

CONTACT DUO

617 Detroit St.
Ann Arbor, MI 48104
(855) 386-2884
info@duosecurity.com

FREE ACCOUNT

Visit www.duosecurity.com for a free account.