

ActivIdentity Soft Tokens

Strong authentication that maximizes user convenience
and streamlines deployment



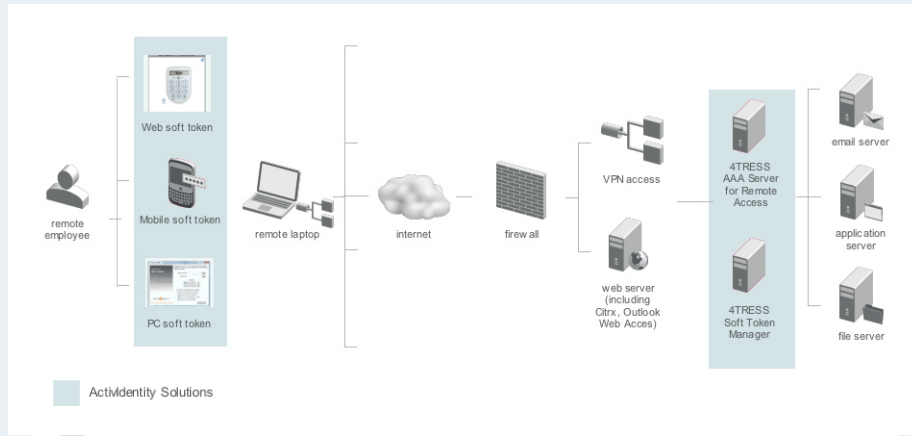
- Improve customer security for online account access
- Secure employee remote access with robust two factor authentication
- Provide an alternative to hardware tokens that deploys faster, costs less, and is more convenient for users and administrators
- Increase security by combining with other authentication methods for a layered security model

ActivIdentity™ Soft Tokens provide strong authentication while simplifying token deployment and activation. ActivIdentity Soft Token generate one-time-passwords (OTPs) on devices users already carry, including phones, personal digital assistants (PDAs), and laptops.

Smartphone and laptop usage is exploding. Organizations are rapidly reaching the point where the average user has multiple devices they need to use to access corporate data and applications. Static passwords are no longer sufficient to secure access, but deploying and carrying hardware tokens brings additional cost and procedures not appropriate for every user. What to do? Consider soft tokens.

A simple provisioning process eliminates the logistic hurdles associated with hardware tokens and allows businesses to deploy strong authentication quickly, securely and cost effectively. Administrators can assign soft tokens to users. Users download the tokens from a public website or app store and self initialize them. Administrators can view access logs and when necessary disable the tokens.

The ActivIdentity Soft Token family consists of three products: Mobile Soft Tokens, Web Soft Tokens, and PC Soft Tokens. All Soft Tokens support the open standards algorithms defined by the Initiative for Open Authentication (OATH).



Employee authentication using soft tokens with 4TRESS AAA Server - How it works.

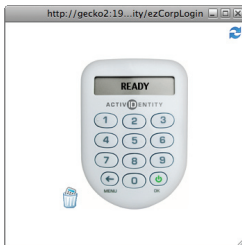


Mobile Soft Token

ActivIdentity Mobile Soft Tokens

The ActivIdentity Mobile Soft token is an application that runs on the user's phone. It can generate a one time password or sign a transaction parameter, eliminating data charges, latency and delivery issues associated with sending OTP via Short Message Service (SMS). It may be deployed with or without PIN protection.

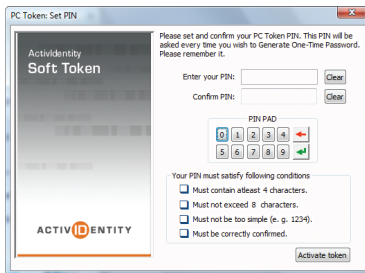
ActivIdentity Mobile Soft Tokens are available on leading handset operating systems, including BlackBerry®, Apple® iPhone®, Windows® Mobile®, Android OS 2.x, and many other Java™ 2 Platform, Micro Edition (J2ME™) enabled devices.



Web Soft Token

ActivIdentity Web Soft Tokens (Device ID)

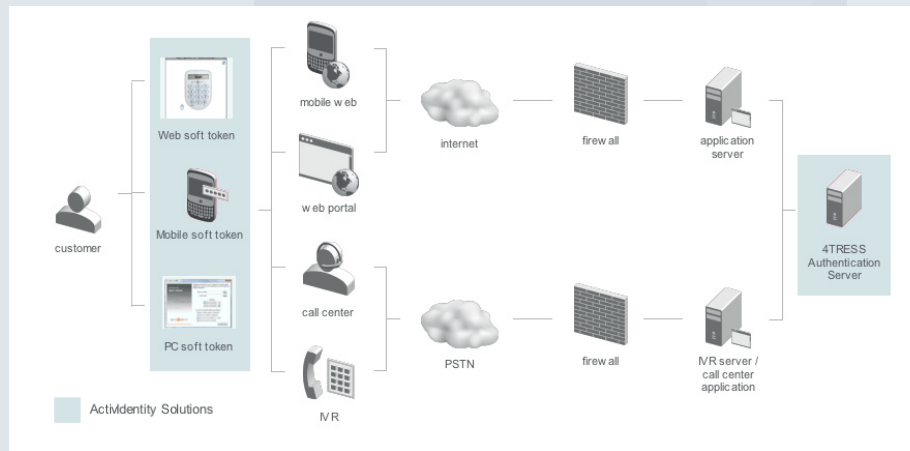
The ActivIdentity Web Soft Token requires no local install and hence provides an easy to deploy, unobtrusive first step to improving website security. The user registers machines which he or she uses to access the website. The web soft token runs within the browser and identifies the machine to the website during the login process. The user may register additional machines, having first authenticated using a method such as an activation code sent via SMS.



PC Soft Token

ActivIdentity PC Soft Tokens

The ActivIdentity PC Soft Token is a lightweight application that runs on the end user's PC. It can generate a one time password in order to authenticate the user. It may be deployed with or without PIN protection and can be distributed easily on a public website or as part of a standard in-house machine build. Users can access their token from the Windows system tray or launch the application from the Windows Start menu.



Customer authentication using soft tokens with 4TRESS Authentication Server – How it works.

ActivIdentity Soft Tokens Features and Benefits

Features and capabilities

- Implement two factor authentication for customer online account access and employee secure remote access
 - User must be in possession of the device (mobile phone or registered computer) in order to successfully authenticate
 - Soft token can be PIN protected or deployed in combination with an existing password
 - Supports one time password and challenge response modes
- Provide a quick to deploy and easy to use, cost effective alternative to hardware tokens
 - The user can download soft token from public website or app store and then self activate
 - A single user license is valid for multiple soft tokens for that user
 - Soft tokens do not expire and the battery never runs out
 - There are no costs associated with replacing lost soft tokens
 - Soft token licenses can be recycled when an employee/customer leaves
- Combine with other authentication methods for a layered security model
 - Soft tokens can be combined with other authentication methods supported by 4TRESS Authentication Server, such as static passwords, security questions and out of band authentication.
 - Soft tokens can be deployed in a mixed environment where different types of hard and soft tokens are issued to different users, based on personal preferences and security considerations

ActivIdentity Soft Tokens offer the following benefits:

- **Lower total cost of ownership:** ActivIdentity Soft Tokens eliminate the cost of physical fulfillment and inevitable hardware token replacement necessitated by loss or expired battery. ActivIdentity Soft Token licenses can be re-assigned when users no longer need their token, maximizing business flexibility and minimizing expense.
- **Faster, more efficient deployment and management:** Administrators can assign / revoke soft tokens and define usage policies from a centralized authentication server capable of supporting a wide range of different authentication methods and rapid response to changing business needs.
- **Superior user convenience:** ActivIdentity Soft Tokens enable strong authentication on devices users already carry. Broad platform support for Internet browsers, smart phones, PDAs, and PCs ensures that organizations can deploy tokens to a user's preferred devices, which increases user acceptance and as a result, strengthens total security. ActivIdentity Mobile Soft Token

Technical Specifications

ActivIdentity Mobile Soft Token

OATH HOTP/TOTP compliant one-time password & OATH OCRA compliant challenge response, supported on the following platforms:

- Blackberry® OS 4.2 and later
- iPhone® iOS 3.x & 4.x
- J2ME™ MIDP2
- Android™ OS 2.x

ActivIdentity PC Soft Token

OATH HOTP/TOTP compliant one-time password & OATH OCRA compliant challenge response, supported on the following platforms:

- Microsoft® Windows® XP® Pro, Vista®, 7
- Microsoft Windows Server 2003®, 2008

ActivIdentity Web Soft Token

OATH HOTP/TOTP compliant one-time password & OATH OCRA compliant challenge response, supported on the following platforms:

- Java™ - JRE 1.5.x and later
- Microsoft Windows (XP Pro, Vista, 7)
- Linux®
- Apple® Mac® OS® X Snow Leopard® 10.6.x
- Microsoft Internet Explorer® 7, 8
- Mozilla® Firefox® 3.x
- Google™ Chrome™ 4.x
- Apple Safari® 4.x

For deployment with ActivIdentity 4TRESS Authentication Server

- Deploy 4TRESS Authentication Server v7.01 or higher (see 4TRESS AS data sheet for supported platforms).
- Deploy soft token end user activation portal or integrate activation into existing website/intranet

For deployment with ActivIdentity 4TRESS AAA Server for Remote Access

- Deploy ActivIdentity 4TRESS AAA 6.6 or higher
- Deploy 4TRESS Soft Token Manager
- Supports Windows 2003 Server SP1, SP2 R2-
- Installation pre-requisites:
 - ASP.NET 2.0 (Installer prompts for installation or upgrade option)
 - JRE 1.5 (Installer auto-installs JRE if not detected)

About ActivIdentity

Americas +1 510.574.0100
US Federal +1 571.522.1000
Europe +33 (0) 1.42.04.84.00
Asia Pacific +61 (0) 2.6208.4888
Email info@actividentity.com
Web www.actividentity.com

ActivIdentity Corporation (NASDAQ: ACTI) is a global leader in strong authentication and credential management, providing solutions to confidently establish a person's identity when interacting digitally. For more than two decades the company's experience has been leveraged by security-minded organizations in large-scale deployments such as the U.S. Department of Defense, Nissan, and Saudi Aramco. The company's customers have issued more than 100 million credentials, securing the holder's digital identity.