

ActivIdentity ActivClient

Advanced Security Client to Protect Workstations and Networks with Smart Cards and USB Tokens




ActivIdentity ActivClient Benefits

- Provides versatility when deploying strong authentication for Windows login and remote access (e.g., OTPs for VPN, PIN-protected PKI certificates, or static passwords for Windows login)
- Allows enforcement of internal security policies
- Integrates easily with existing enterprise infrastructure
- Has a consistent, user-friendly interface that encourages a familiar “ATM-like” authentication experience
- Scales to tens of thousands of desktops using Windows utilities such as Microsoft System Management Services or Microsoft Active Directory®

The ActivIdentity ActivClient™ family of products helps IT managers, security professionals, and auditors to manage the risk of unauthorized access to workstations and networks. As a market-leading middleware for smart cards and USB tokens, ActivIdentity ActivClient consolidates identity credentials (e.g., private keys for public key infrastructure [PKI] certificates, symmetric keys for OTP generation, and static passwords) on a single secure, portable device. This capability – combined with support for a wide range of desktop, network, and productivity applications – enables organizations to use strong authentication, encryption, and digital signatures to protect high-value resources and interactions.

The ActivIdentity ActivClient product family includes the following features and capabilities:

- Interoperability with a wide range of remote access solutions, thin clients, applications (e.g., Microsoft® Outlook®, Adobe Acrobat®, and popular web browsers), smart cards, smart card readers, and USB tokens
- Compatibility with major certificate authorities and encryption utilities
- Simple automated deployment, updates, and diagnostics
- Open standards-based architecture, which is easily extensible using the companion software development kit



ActivIdentity ActivClient for Common Access Card Benefits

- Deployed on hundreds of thousands of desktops across the U.S. DoD
- Meets U.S. DoD Common Access Card Middleware Requirements v3.0
- Pre-installed DoD root certificates

ActivIdentity Authentication Client Benefits

- Provides emergency access for in-office and remote users whether they are online or offline – even if help desk personnel are not available
- Lowers the cost of smart card deployment by eliminating the requirement to deploy public key infrastructure
- Allows customized security policies for knowledge-based (e.g., question and answer) authentication

- Alternate authentication methods available to access Microsoft Windows® workstations using the ActivIdentity™ Authentication Client
- Supports standard U.S. Government-issued Common Access Cards and Federal Information Processing Standards (FIPS) 201 certified Personal Identity Verification (PIV) cards

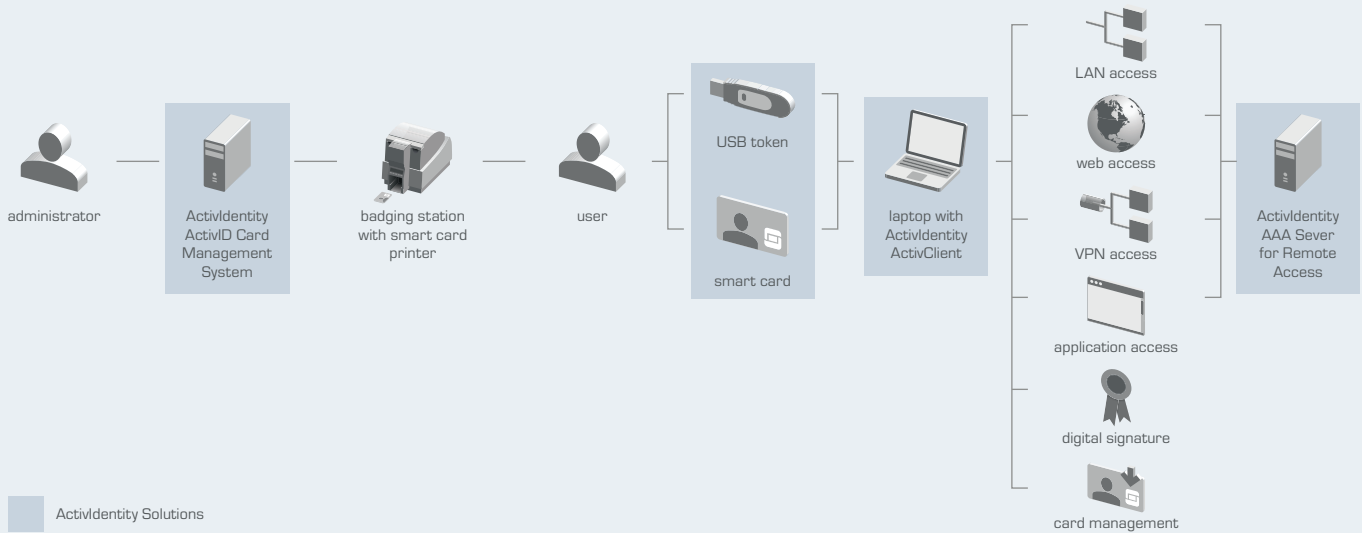
ActivIdentity ActivClient

ActivIdentity ActivClient allows organizations to protect Windows workstations and internal networks from unauthorized access. Using ActivIdentity ActivClient, IT managers can easily enforce strong authentication policies when users log in to their Windows desktop, or access the organization's network using a virtual private network (VPN), thin client, or remote desktop session. In addition, IT professionals can store user credentials securely and encrypt data exchanged between the desktop and the smart card or USB token.

ActivIdentity ActivClient can be deployed with ActivIdentity SecureLogin™ Single Sign-On to enhance user productivity and streamline password management. It can be used with ActivIdentity 4TRESS™ AAA Server for Remote Access for one-time password validation. For larger deployments, organizations can take advantage of the full credential life cycle management and PKI interoperability of ActivIdentity ActivID™ Card Management System.

Additional Operating System Support for ActivIdentity ActivClient

Versions of ActivIdentity ActivClient are available on Linux®, Mac OS® X, and Solaris™. Please see the Technical Specifications table for specific operating system requirements and features.



ActivIdentity Solutions

ActivIdentity ActivClient for Common Access Card

ActivIdentity ActivClient for Common Access Card includes all the features and benefits of ActivIdentity ActivClient and is configured with specific policies required by the U.S. Department of Defense (DoD).

ActivIdentity ActivClient SDK

The ActivIdentity ActivClient security client offering also includes a software development kit (SDK) for systems integrators and independent software vendors to third-party and custom applications. Software developers do not need specific knowledge of smart card technology to integrate ActivIdentity ActivClient services into their applications.

ActivIdentity Authentication Client

ActivIdentity Authentication Client provides organizations with an alternate method to access Windows workstations. When users lose a smart card or forget a password, ActivIdentity Authentication Client provides an emergency Windows login using knowledge-based (e.g., question and answer) authentication. Once users access the desktop, ActivIdentity Authentication Client allows them to reset their password. ActivIdentity Authentication Client also enables organizations to support PIN-protected smart card-based static password authentication for Windows login. This capability extends the advantages of strong authentication with smart cards to organizations that do not issue digital certificates.

Third-Party Interoperability

- Cisco Systems Technology Partner
- Citrix Ready
- Entrust Ready
- Novell
- Microsoft Gold Certified

Technical Specifications

	ActivIdentity ActivClient 6.2 and ActivIdentity ActivClient for Common Access Card 6.2	ActivIdentity Authentication Client 2.0.1
System Requirements	Microsoft® Operating Systems (ActivClient and ActivClient for Common Access Card) <ul style="list-style-type: none">- Windows® 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, and Windows Server 2008 (32- and 64-bit) Linux® Operating Systems (ActivClient – version 3.0) <ul style="list-style-type: none">- RedHat® Enterprise Linux® 4, 5 (x86), SuSe 10 Linux (x86)- GNOME Desktop Manager (GDM), GNOME and K Desktop Environment (KDE) desktop Mac OS® X Operating Systems (ActivClient – version 3.0.1) <ul style="list-style-type: none">- Mac OS X 10.5.6 or greater (Intel®)	Operating Systems <ul style="list-style-type: none">- Microsoft Windows XP Professional, Windows Vista, Windows Server 2003 (x86)
Government Standards	<ul style="list-style-type: none">- FIPS 201 certified for Personal Identity Verification cards- U.S. Government Smart Card Interoperability Specifications GSC-IS v2.1- Applets – FIPS 140-2 Level 2 and 3 certified- FDCC / SCAP 1.1 compliant- Section 508 compliant	
Security Services	<ul style="list-style-type: none">- Secure workstation and network login: Windows® Smart Card Logon, Novell® Login, MacOS Login and Linux Login- Secure dial-up / VPN with Check Point®, Cisco®, Microsoft® and Nortel® and many other remote access solutions- Secure Web Login with Microsoft Internet Explorer®, Firefox® and Apple Safari- Secure remote access via Citrix XenApp and Windows Terminal Server- Secure Email (signature and encryption) with Microsoft Outlook®, Thunderbird®, Apple Mail and Microsoft Entourage- Support for Entrust® Entelligence™ Security Provider and Entrust Entelligence™ Desktop Solutions- Secure Documents through Digital Signature with Adobe® Acrobat® and Microsoft Office- Secure Files through Microsoft Windows Encrypting File System (EFS)- Pre-boot authentication, disk and file encryption with PointSec, SafeBoot®, WinMagic and more.	<ul style="list-style-type: none">- Windows Login with static password stored on smart card- Emergency Access to Windows using question and answer, Windows self-service password reset – available both online and offline- Automated logon to Cisco VPN with a smart card-based one-time password – available at Windows Logon and in the Windows session
Management Services	<ul style="list-style-type: none">- User console for end-users to view and manage their smart card and credentials- Change PIN / unlock card- Initialize / reset card- Digital Certificates: Certificate viewer, import / export user and CA certificates- Generate OTP in synchronous or challenge / response mode, resynchronize event counter- View personal information for US DoD Common Access Cards and US Government Personal Identity Verification (PIV) cards- Automatic and secure card update, post issuance, via ActivID™ Card Management System- Troubleshooting and Advanced Diagnostics Wizards	
Smart Card Support	<ul style="list-style-type: none">- Smart Cards and USB tokens from ActivIdentity, Athena, Atmel®, CardLogix, Gemalto, Giesecke & Devrient, Keycorp, Oberthur, Safenet, Sagem Orga	
Compatibility with Other ActivIdentity Software Products	<ul style="list-style-type: none">- ActivIdentity SecureLogin Single Sign-On, ActivIdentity Authentication Client, ActivIdentity 4TRESS AAA Server for Remote Access, ActivIdentity ActivID Card Management System	

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.