ActivCard®

## Product Announcement

# ActivCard Single Sign-On v5

www.activcard.com

# Table of Contents

# 1. Introduction

ActivCard is introducing a new version of the single sign-on solution suite with some significant enhancements our customers are asking for. ActivCard Single Sign-On v5 provides support for additional SSO applications, easier deployability for Adaptive Credential Managers (ACMs), better usability for end users and administrators, support for Microsoft and Novell GINAs and authentication, kiosk mode using password or smart card authentication, and the latest standards-based encryption.

ActivCard SSO v5 also offers integration with the full suite of ActivCard products (ActivCard CMS v3.6, ActivCard AAA Server v6.2, and ActivClient v5), giving you the ability to use ActivCard SSO for single sign-on up-front and later upgrade to additional capabilities, such as secure remote access with ActivCard AAA one-time passwords or corporate access cards and PKI services with ActivCard CMS. This document lists those features that are new since Trinity v4.2.

You will notice that with the release of ActivCard SSO v5, Trinity Client has been replaced by ActivClient v5 – ActivCard's new customizable client. See the ActivClient v5 Product Annoucement document for further details.

# 2. Product Positioning

ActivCard SSO is a client-side enterprise single sign-on solution that provides efficient and seamless access to many types of applications. Users can login quickly and securely to a wide range of applications, websites, and mainframe sessions with just one password or other authentication method. ActivCard SSO frees the help desk from the routine and costly task of resetting passwords. Finally, ActivCard SSO comes with a powerful wizard and scripting tools that enable administrators to easily extend SSO services to applications within the enterprise.

**Key Benefits:**

- ActivCard Single Sign-On enhances security, lowers help desk administration costs, and improves employee productivity:
- ActivCard Single Sign-On eliminates the need for users to remember the multitude of usernames and passwords beyond their primary network logon
- ActivCard SSO securely stores and manages the usernames and passwords that each user needs to access applications, and automatically submits them for the user as needed
- ActivCard Single Sign-On increases productivity because users are no longer required to manually enter repetitive usernames and passwords
- ActivCard SSO eliminates calls to the help desk concerning lost or forgotten passwords for those applications it manages

**Rapid Return on Investment:**

ActivCard Single Sign-On is a highly cost effective solution for reducing help desk operational cost and increasing user productivity. ActivCard Single Sign-On provides cost savings to organizations by dramatically reducing the time required for users to log in to their applications, resulting in efficient and productive use of time that would otherwise be spent remembering/finding and entering passwords. Additionally, password reset calls to the help desk can be reduced by using ActivCard Single Sign-On, resulting in valuable time savings for help desk staff and end users.

# 3. What's New in ActivCard Single Sign-On v5?

**SSO Application Extensibility**

ActivCard Single Sign-On v5 supports additional application types and several new enterprise applications that come pre-configured with the solution. This release also includes a ActivCard SSO Adaptive Credential Manager (ACM) Scripting Guide that documents all of the Application Programming Interfaces (APIs) that are built into ACMs for single sign-on and password management functionality.

| Features | Descriptions and Benefits |
|---|---|
| Java-based Applications that use the SWING or AWT UI framework | ActivCard SSO supports single sign-on to Java applications that use the SWING user interface (UI) framework or the AWT UI framework. These can be Windows, Internet, or Intranet Java applications. With this new functionality, organizations can, for example, enable single sign-on to Web-based enterprise applications or Web Services written in Java 2 Platform Enterprise Edition (J2EE), or PC desktop applications and applets written in Java 2 Platform Standard Edition (J2SE). |
| New Pre-Configured SSO Applications | Each release of ActivCard SSO includes new pre-configured ACMs for single sign-on to enterprise applications. Pre-configured ACMs are ideal because they provide SSO out of the box without scripting, reducing deployment time and cost. ActivCard SSO v5 adds off the shelf support for the following ACMs:<br>• IBM Host On-Demand v8<br>• IBM Personal Communications (PCOMM) v5.7<br>• Attachmate Extra! Enterprise 2000 v2000a<br>• SAP R/3 v6.2<br>• Lotus Notes v6.5<br>• Entrust Entelligence v6.1<br>• Entrust Entelligence v7.0<br>• Remedy Action Request System v5.1<br>• Citrix MetaFrame XP FR3 with ICA Client v7.0<br>• Cisco VPN Client v3.0.1 (firmware v3.5)<br>• CheckPoint VPN SecuRemote NG AI and NG FP3<br>• NetScreen v8.0.1<br>• Nortel Contivity VPN for Windows v4.6.5 |
| ActivCard SSO ACM Scripting | ACM Scripting is a new key feature of ActivCard SSO that enables single sign-on to a broad range of SSO applications. ActivCard SSO v5 includes Visual Basic Scripting Application Programming Interfaces (APIs) that address all ACM functionality, including login and password management behaviors for most applications. ActivCard SSO can do single sign-on to the following SSO applications:<br>• Windows<br>• Java<br>• Mainframe<br>• Terminal Server<br>• Internet<br>• Intranet |

| | |
|---|---|
| | • Websites<br>• UNIX (via terminal emulation)<br><br>With ACM Scripting capabilities it is not necessary for ActivCard SSO to have a pre-configured Adaptive Credential Manager (ACM) for every application in your environment. With ACM Scripting you can rapidly enable SSO by creating a script for almost any application without modifying the application's code. |
| ActivCard SSO ACM Scripting Training Program | ActivCard also offers a new ACM Scripting Training Program for those who will be implementing or supporting ActivCard Single Sign-On. This program is intended to provide participants with the skills to successfully create ACMs for single sign-on. The course contains instructor demonstrations, lecture based training, hands on exercises, and interactive quizzes. This course is ideal for ActivCard partners, SIs, and resellers. |

**Interoperability**

ActivCard Single Sign-On v5 offers tighter integration with the network operating system (NOS) authentication protocols, offering a seamless end user experience.

| Features | Descriptions and Benefits |
|---|---|
| Support for Microsoft and Novell Authentication Methods | ActivCard Single Sign-On services can be automatically started when the user logs into the workstation or network operating system using their primary Windows authentication (smart card or password) or Novell authentication (NDS password). This eliminates the cost of training users because you are not introducing a new authentication method that they have never before seen or used. |
| Uses Windows or Novell Graphical Identification and Authentication (GINAs) and Login dialogs | ActivClient v5 never replaces the Windows or Novell Graphical Identification and Authentication (GINA). This reduces the cost of support issues related to GINA replacements and having multiple GINAs present. If you are using an authentication method that is not supported natively by Windows or Novell NDS, i.e., smart card logon without a PKI, then ActivClient will display its own logon screen in front of the Windows or Novell GINA; it does not replace the GINA. |

**Usability**

ActivCard SSO offers many new single sign-on features and enhancements, extending SSO to kiosk environments, giving end users the ability to enable and disable SSO to their applications, and minimizing end user interaction.

| Features | Descriptions and Benefits |
|---|---|
| Kiosk Mode Using Smart Cards or Passwords for Authentication | ActivClient v5 can be configured to allow a single PC to be shared by multiple users inside the same Windows session without requiring a logoff and logon. In Kiosk Mode the PC is always logged on to Windows using a generic Windows account. Users login and logout of their SSO service as needed using either a password or smart card. This feature is ideal for manufacturing and hospital environments where multiple users share a single PC to access applications.<br>How Kiosk Mode Works: When a user opens an initial application from the kiosk, the user will be prompted to logon to their ActivCard Single Sign-On service. After entering their password or smart card |

| | |
|---|---|
| | PIN, they will be automatically logged into ActivCard SSO and the initial application that was launched. They will also have single sign-on to all of the applications they access during their kiosk session. When they are done, depending on whether the user logged in with a smart card or password, they either right click the ActivCard SSO system tray icon to logout or they simply remove their smart card from the reader. After doing so, the user will be logged out of the ActivCard SSO service and the kiosk is ready for the next user. |
| Streamlined Configuration of User Settings | ActivCard SSO v5 streamlines configuration of user policies by not requiring policy settings for the user's authentication method and location. Instead, these authentication parameters are enforced by the ActivClient configuration and the authentication credentials that have been issued to the user. |
| Stores Application Passwords On First Use With Single Click | When a user accesses an application for the first time after an administrator has enabled it for single sign-on using an ACM, end users are presented with the option to store their credentials (typically a username and password) in the encrypted Credentials Bank. This task has been reduced to a single dialog box requiring a single click. When done, ActivCard SSO manages the credentials and provides a single sign-on experience the next time the application is accessed. |

**Deployability**

Deploying SSO applications is much easier and more flexible, reducing the total cost of ownership of the solution.

| **Features** | **Descriptions and Benefits** |
|---|---|
| Deploy ACMs via Directory from ACM Designer Console | Administrators can now Publish, Update, and Revoke ACMs to the Directory from the ACM Designer Console. ACMs no longer have to be manually distributed to client workstations through a public server or copied to individual workstations locally. After an administrator creates an ACM for single sign-on to an application, the ACM is published to a directory via the ACM Designer Console, the management tool used for creating and managing ACMs. The newly published ACMs are automatically synchronized to client workstations when the user logs into the network or at a pre-defined interval of time set by the administrator (when the ActivClient set-up is configured). Administrators can also update and revoke published ACMs as needed. These new capabilities reduce the total cost of ownership by making SSO applications easier to deploy and manage. |
| Published ACM Folder and Draft ACM Folder | When Administrators publish an ACM to the directory for synchronization to user workstations, the ACM is automatically categorized in the Published ACMs folder in the ACM Designer Console. When an Administrator is in the process of creating an ACM and testing it, the ACM remains in the Draft ACMs folder. This new categorization allows administrators to more easily track and manage the lifecycle of their ACMs. |

| | |
|---|---|
| Time-Based Synchronization of ACMs and SSO Credentials | In addition to automated synchronization of ACMs and SSO credentials at each login to the network, ActivCard SSO v5 offers time-based synchronization between ActivClient and the user's encrypted store in the directory. This ensures the user's ACMs and stored credentials remain consistent and up to date. If the user is using a smart card, this synchronization will also update the SSO credentials encrypted in the card. Time-based synchronization is defined during the configuration of ActivClient. Administrators can set how often ActivClient will communicate with ActivCard SSO services for ACM and SSO credential synchronization. Administrators use the ActivClient configuration tool or a registry-based tool to update this setting as needed. |

**Manageability**

ActivCard SSO v5 offers many new capabilities that streamline management while making the solution more secure.

| Features | Descriptions and Benefits |
|---|---|
| Emergency Password Access to SSO Services | The Emergency Password capability is for smart card users using ActivClient smart card authentication. If a user is having difficulties authenticating with a smart card or has forgotten their smart card, the user can obtain an Emergency Password to login and gain access to their single sign-on services. The emergency password is valid for a predetermined time as set by the ActivCard SSO help desk administrator. If the user is using Microsoft smart card logon, then they can use a Windows password for emergency logon, not the ActivClient Emergency Password. |
| Advanced Password and PIN Rules | The ActivCard SSO Administration Tool now includes a console that allows ActivCard SSO administrators or help desk operators to define and enforce various password and PIN rules for the smart card PIN, Emergency Password, and Kiosk Password. |
| Full User Templates Allow Administrators to Easily Implement SSO Policies | Administrators can define a set of ActivCard SSO policies and save those policies in a ActivCard SSO User Template. This template can then be applied to new users as they are enrolled in ActivCard SSO for fast and consistent policy assignment. Administrators can define any number of User Templates for different groups of users based on their roles within the organization. |
| SSO Password Spillover for Smart Cards | If using a smart card to store SSO credentials and it becomes full, ActivCard SSO can automatically start managing the additional SSO credentials on the PC. ActivCard SSO will also manage the synchronization of these credentials between the directory, smart card, and PC, ensuring that the user's SSO credential bank stays consistent and up to date. |
| End Users can Disable and Re-Enable SSO On Per Application Basis | ActivClient User Console allows end users to disable and enable single sign-on on a per application basis. This feature is useful for troubleshooting and security issues. (ActivClient User Console is highly customizable and this particular feature can be turned off when the setup is created.) |

**Security**

ActivCard SSO v5 single sign-on solution offers new security features, including industry standard encryption algorithms and the broadest range of smart card support.

| Features | Descriptions and Benefits |
|---|---|
| AES Data Encryption of SSO Credentials | Usernames, passwords, and other identity data are encrypted on the client workstation and in the directory with the 256-bit Advanced Encryption Standard (AES), compared to competing solutions that use 168-bit 3DES encryption. National Institute of Standards and Technology (NIST) has approved the AES algorithm for validation as a Federal Information Processing Standard (FIPS). This standard specifies Rijndael as a 197 FIPS-approved symmetric encryption algorithm that may be used by U.S. Government organizations and other organizations to protect sensitive information. For more information visit the NIST AES homepage: http://csrc.nist.gov/CryptoToolkit/aes/ |
| Support for Additional Smart Cards, USB Keys, Card Profiles, and Readers | For organizations that want to use smart cards for stronger user authentication, ActivCard SSO v5 supports numerous new smart cards and USB keys, including those from ActivCard, Schlumberger, Gemplus, G&D, and Oberthur CS. Some of these smart cards are 64K Java Cards that are FIPS validated (Level 140-2). |

**Support for Other ActivCard Products**

ActivCard Single Sign-On can now be used with other ActivCard products if stronger methods of authentication are needed, such as smart cards, PKI, or one-time passwords. This functionality allows organizations to leverage the advanced authentication and credential management capabilities of ActivClient v5, ActivCard CMS v3.6, and ActivCard AAA Server v6.2. You can upgrade your SSO solution to include secure remote access, card-based PKI services, and corporate access card capabilities when needed.

| Features | Descriptions and Benefits |
|---|---|
| Support for ActivClient v5 | Trinity Client has been replaced by ActivClient v5, which is a new feature rich client that works with all ActivCard servers. Users can log into their SSO service with the advanced authentication methods supported by ActivClient v5. ActivClient v5 is built on ActivCard Gold middleware and client technology, which is deployed to 2 million users at the U.S. Department of Defense for its Common Access Card program. See the ActivClient v5 Product Announcement document for further details. |
| Support for ActivCard CMS v3.6 | ActivCard Single Sign-On can be used with any smart card issued by ActivCard CMS v3.6. ActivCard CMS issues an empty SSO credential bank onto a smart card that ActivCard SSO can then use for storing and managing SSO passwords. ActivCard SSO also benefits from the advanced card management capabilities in ActivCard CMS, such as issuance of temporary and permanent replacement cards. See the ActivCard CMS v3.6 Product Announcement document for further details. |
| Support for ActivCard AAA v6.2 | Using an ActivCard SSO Adaptive Credential Manager (ACM), ActivClient auto-submits the ActivCard AAA username and |

| | |
|---|---|
| | synchronous one-time password generated in the smart card for secure remote access applications, such as dial-up and VPN. This means the end user does not have to manually type the OTP into the application's authentication dialog. This functionality is available in online or offline mode. ActivClient is pre-packaged with ACMs for ActivCard AAA supported applications (e.g., Cisco VPN Client v3.0.1, Nortel Contivity VPN for Windows v4.6.5, CheckPoint VPN SecuRemote NG AI and NG FP3, and NetScreen v8.0.1). In the ActivCard SSO Administration Tool the administrator selects whether the SSO credential is a static password or dynamic one-time password. See the ActivCard AAA Server v6.2 Product Announcement document for further details. |
| Smart Cards, Card Profiles, Applets, Readers | All next-generation ActivCard products, including ActivCard SSO v5, support the same set of smart cards, USB keys, standard smart card profiles, applet v1.5 framework, and smart card readers. ActivCard offers standard smart card profiles that include enough space to store and manage 15 SSO credential sets on a 32K or 64K smart card. If the smart card becomes full, the PC is automatically used to store additional SSO credentials. |

# 4. Solution Key Differentiators, Key Advantages

## Compelling Value Proposition

For companies currently using password protected authentication or access control, the ActivCard Single Sign-on solution can offer a significant value proposition. The platform is the only commercially available product that simplifies sign-on for end-users, reduces helpdesk support costs for password resets, and improves security through multi-factor authentication in a single centralized environment. The platform allows administrators and users to authenticate using:

- **Passwords**
  Users can authenticate using a single password, or combine multiple authentication methods. Administrators can define requirements for password format, enforce a password to expire after a given number of days elapse, enforce a password change at the next user login, and enforce a password lock after a given number of bad attempts.

- **Roaming**
  End-users can authenticate from any client workstation in the enterprise, as their personal credentials are securely stored in the corporate directory. Roaming is ideal in work environments where a single user must use more than one computer or multiple users must share a single computer.

- **Smart Cards**
  Smart Cards provide an effective place for secure storage and offline access to user credentials ? such as login passwords, biometric fingerprint templates, digital certificates and private keys ? as well as to provide a common platform for physical identification through photographs and building access. Additionally, administrators have the ability to ensure that various levels of security policies are enforced by the Smart Card even if it is used while offline.

- **USB Keys**
  USB Keys provide users with multi-application functionality of a smart card but with a

smaller and more portable form factor that can be used on any workstation with an available USB port. This form factor eliminates the need for a reader since it is built-in, and further enhances security by not providing external clues as to the assigned owner of the credentials contained within the key. These features significantly improve the end-to-end security of this device.

## Centralized and Easy to Use

By consolidating multiple authentication methodologies onto a single platform, administrators have a centralized repository to add, change and remove user's credentials across any large distributed environment. End-users experience the same login interface for all of their platforms and applications. The platform enriches the distributed management nature of an organization by supporting several administrative roles for the various help desk and administrative roles employed by a typical enterprise organization.

## Device Interoperability and Support

ActivCard supports several different multi-factor authentication devices ? including a range of fingerprint biometric scanners, smart card readers, and combination readers in a variety of form factors ? from standalone desktop peripherals to combo readers integrated into keyboards. Organizations can select the most suitable scanner or reader for the personalized needs of individual users, ensuring that each user can authenticate in a way that works best for their specific environment and needs, while ensuring consistent security policy enforcement across the organization.

## Multiple Combined Authentication Methods

Multiple combined authentication methods not only make single sign-on to platforms and applications more convenient, they can also make it more secure. Multi-factor authentication using smart cards, fingerprint biometrics, hardware tokens, passwords, or a combination of these methods is a valuable alternative to single password authentication. Administrators can easily assign a combination of authentication methods on a user-by-user basis. For example, a user may have a default method of Smart Card + Password + Fingerprint and the ability to use an alternative method of Fingerprint + Password only.

# 5. Detailed Product Description

## 5.1 Single Sign-On

ActivCard SSO provides single sign-on to a wide range of different enterprise application types, both when the user is online (i.e., connected to the network) or offline (i.e., disconnected from the network):

- Windows applications (32-Bit), Web applications (Java and HTML), some Terminal Emulators (HLLAPI and WinHLLAPI), and Java Applications (Swing and AWT)
- ActivCard SSO comes with pre-configured Adaptive Credential Managers (ACMs) for single sign-on to commonly used enterprise applications, reducing deployment time and cost associated with scripting and testing scripts
- ActivCard SSO also includes both an ACM Designer Wizard that auto-generates ACMs for single sign-on to applications and documented Application Programming Interfaces (APIs) for Visual Basic-based scripting of new ACMs
- Kiosk Mode allows a single computer to be shared by multiple, alternating users inside the same Windows session without requiring a logoff of the operating system

- Roaming allows users to logon from any computer in the enterprise and still have access to their SSO services
- If a user has multiple accounts for a single application, ActivCard SSO supports SSO to a default account and allows the user to select an alternative account when needed for that application

## 5.2 Password Management

ActivCard SSO password management capabilities are powerful and cover all types of application login dialogs that an application my present to a user:

- ActivCard SSO can synchronize passwords at change password requests and add the new password to its secure credentials bank
- When a change password request is recognized, ActivCard SSO can auto-generate a random password based on rules set by the administrator, submit it to the application, and store it in the user's credentials bank
- ActivCard SSO automatically detects failed login attempts and re-synchronizes the credentials bank with the correct password
- All SSO credentials are stored encrypted using standard AES encryption in the directory and PC
- If a smart card is used for authentication, ActivCard SSO can automate the management of the SSO credentials stored in the card by synchronizing them with the store in the directory

## 5.3 Authentication Methods

ActivCard Single Sign-On supports multiple types of authentication methods – from basic passwords to advanced multi-factor authentication using cryptographic smart cards or USB keys:

- Users can login to ActivCard SSO services using native Windows or Novell authentication methods (password or smart card PKI logon) and GINAs (Graphical Identification and Authentication)
- For organizations that want a higher level of user authentication security, ActivCard SSO supports numerous new smart cards and USB keys, including 64K Java Cards that are FIPS validated (Level 140-2)
- If the administrator wants to provide a higher level of security for a particular application, a policy can be set on a per application basis that requires the user to re-authenticate to the SSO application

## 5.4 Extensible to Other ActivCard Products

ActivCard Single Sign-On can be used with other ActivCard products if stronger methods of authentication are needed, such as smart cards, PKI, or one-time passwords. This functionality allows organizations to leverage the advanced authentication and credential management capabilities of ActivClient v5, ActivCard CMS v3.6, and ActivCard AAA Server v6.2. You can upgrade your SSO solution to include secure remote access, PKI services, and corporate access card capabilities when needed:

- Trinity Client is now ActivClient v5, which is a feature rich client that works with all ActivCard servers. Users can log into their SSO service with the advanced authentication methods supported by ActivClient v5
- ActivCard Single Sign-On can be used with any smart card issued by ActivCard CMS v3.6. ActivCard CMS issues an empty SSO credential bank onto a smart card that ActivCard SSO can then use for storing and managing SSO passwords
- Using a ActivCard SSO Adaptive Credential Manager (ACM), ActivClient auto-submits the ActivCard AAA username and synchronous one-time password generated in the smart card for secure remote access applications, such as dial-up and VPN, eliminating the need for the end user to manually type the OTP into the application's authentication dialog

## Legal Disclaimer

This document is intended to assist business and IT professionals in developing an understanding of ActivCard products and services used in certain network security implementations. The information is not intended as a specification of any programming interfaces that are provided by ActivCard and other ActivCard subsidiaries, or partners.

This publication is intended for informational purposes only. ActivCard makes no warranties, express or implied in this document. Furthermore, the information contained in this document has not been submitted to any formal testing and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by ActivCard for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

ActivCard products, programs, or services referenced in this publication may not be available in all countries in which ActivCard operates due to export restrictions or changes in market conditions. Any reference to an ActivCard product, program, or service is not intended to state or imply that only ActivCard's product, program, or service is necessary to achieve the results contained herein. Any functionally equivalent program that does not infringe on any of ActivCard's intellectual property rights may be employed as an alternative to an ActivCard product, program, or service.

Information in this publication was developed in conjunction with the use of the hardware, software, and networking arrangements specified and is thus limited in application to those specific hardware and software products and levels.

ActivCard may have patents, pending patent applications, and/or other intellectual property rights covering subject matter contained in this document. The furnishing of this document does not imply or expressly provide a license to any of ActivCard’s intellectual property. Cross-licensing of ActivCard’s intellectual property is available for enabling the exchange of information between independently created programs and ActivCard products. Cross-licensing agreements are subject to appropriate terms and conditions, including in some cases, payment of a fee. Licensing or other intellectual property inquiries should be sent in writing, to the Director of Intellectual Property, ActivCard Corp., 6623 Dumbarton Circle, Fremont, CA 94555 USA.



**www.activcard.com**

**ActivCard, Inc.**
TEL: +1 (510) 574 0100
FAX: +1 (510) 574 0101
info@activcard.com