

Version3

Simple Sign-On – Application Access Management

White Paper

Introduction to Version3 Simple Sign-On

Version3 Simple Sign-On provides seamless and secure access for users to run Windows and web-based applications. Users no longer have to remember a long list of application specific or web site specific names and passwords. System security is enhanced with Version3 Simple Sign-On by eliminating the need for identities and credentials to be written down.

Version3 Simple Sign-On is a full-featured identity management solution that gives users secure access to all needed line of business applications using one set of network security credentials. By leveraging Microsoft Active Directory Services, Version3 Simple Sign-On gains the power to manage passwords, control access to applications and simplify account management in a secure manner. This set of services applies not only for users' primary logons but also for all of the user's secondary logons to non-Microsoft back-ends such as Novell NetWare servers or IBM AS400s, along with vertical applications that require separate and sometimes proprietary security validation steps.

In order to appreciate what Version3 Simple Sign-On does and how it can help the administrator, it is important to first define what identity management is, the context it is performed in, and why it has fast become the focus for many IT departments.

Identity Management

An identity is represented by a set of credentials. Simply put, an identity is the name and password pair that a user presents to a security sub-system in order to gain access to the resource that it protects. While most users can immediately think of the name and password to gain access to their desktop, there are various other identities that the average user must remember. For example, one identity may be required to retrieve email, another to run the accounting software's payroll module, and yet another to access the company portal. It is easy to see from these examples why identities require management.

Identity Management Life-Cycle

Identity management has a life cycle. Understanding this life cycle provides a context within which various features of Version3 Simple Sign-On can be discussed.

Provisioning Identities

The identity management life cycle starts with provisioning. This is where the IT administrator creates the identities that a user needs based on the company's internal request processes. For example, one identity is created for the user's initial desktop and network logons, another identity may need to be created for the user's access to the company's customer relationship software (CRM), etc. Provisioning also takes place for a given user on an ongoing basis such as when role changes occur and access to new applications is required. This is the most visible stage of the identity management life cycle and must be performed rapidly and efficiently.

Provisioning Applications

The creation of identities is typically correlated with the provisioning of applications. Apart from the usual distribution methods related to getting applications installed (such as Microsoft's SMS product), there is the need to place and maintain application shortcuts on the user's desktop in a standardized location, and to ensure that the shortcuts are always available even after accidental deletion.

Applications that the administrator provisions fall into two general categories: Simple Applications and Enhanced Applications. Simple Applications are directly accessible to the user with no additional prompts at launch. Examples of Simple Applications include Notepad, Internet Explorer, Microsoft Word, etc. Enhanced Applications require the user to enter additional information such as separate application-recognized credentials before granting access to its core functionality. An example of an Enhanced Application is any Microsoft Access database that is password protected. Another example is software that connects to mainframes, AS 400s, Novell servers or even Linux-based systems.

Maintenance

The next stage of the identity management life cycle is generally called the maintenance stage. This stage focuses on maintaining the identities after periodic password changes and password resets when users forget them. Generally, the more identities a user owns, the more calls he or she makes requesting password resets. This stage tends to be the focus of IT departments' attempts at reducing costs.

Termination

The final stage of the identity management life cycle is called the termination stage. In this stage the administrator is responsible for de-provisioning or removing access from the user. The challenge for the administrator usually comes from having to track down all of the applications the user has been granted permission to and ensuring that the user can no longer access those applications.

Security Challenge

Identity management also occurs within the context of a corporate security policy. It may seem redundant, however it is important to remember that implementation of identity management must follow decreed security guidelines such as minimum password length requirements, password complexity requirements or periodic forced password changes. The challenge is in ensuring that the policy is enforced for all applications, not just the corporate desktop log on.

In a typical organization, there is a continuous demand to add new applications and services to meet the ever-evolving requirements of the user base. Quite often, those new applications represent new user names and passwords to be remembered by users and managed by administrators. The more of these important keys of information users are expected to retain, the more likely the passwords are actually being written down and "hidden" for reference, leaving the network vulnerable for compromise.

The need for a single sign-on solution

Version3 Simple Sign-On provides organizations with the means to eliminate concerns for network's security along with alleviating the annoyance to users by giving them the freedom to bypass all application logon sequences. In addition to better balance of usability and security, Version3 Simple Sign-On can decrease user support issues by as much as 30%-40%.

Version3 Simple Sign-On provides users with secure "single sign-on" access to virtually any Windows or web-based application. It is simple for administrators to use because it integrates with Microsoft's Active Directory, enabling administrators the ability access and manage Version3 Simple Sign-On configurations through the same familiar tools and policies used each day to manage the network.

There are several directory solutions available claiming to solve the authentication technology challenge commonly referred to as single sign-on. Identity management

software features have been defined in various ways by different vendors and research groups. The common threads between the many definitions include the following functions that are offered by identity management software vendors:

1. **Password Reset** – relieves the management burden and costs of password related support calls, while enforcing strong password policies by enabling users to reset their own passwords without the aid of a help desk.

Version3 Simple Sign-On takes this function even further by not requiring the user to remember the new password.

2. **Password Synchronization** – is also help desk friendly, requiring users to know just a single password across different systems, reducing the chance that they might forget one or more passwords. However, the user still has to enter an ID and password for each application. Synchronization products all require software that typically resides on a server and APIs that link the software to databases, help desks and security frameworks.

By storing multiple credentials per user, Version3 Simple Sign-On alleviates the need for password synchronization, making it much easier and faster to plan, deploy and implement than password synchronization solutions require.

3. **Single Sign-On** – can be considered a step up from password synchronization since it allows a user log on to a PC or network once and access multiple applications and systems using a single password. Typically, such products authenticate the user at log on and present the available applications on the desktop. When the user selects an application, the SSO agent presents the authentication credentials in the background. On the downside, most SSO technology requires its own infrastructure, such as an authentication server, that verifies user identity and permission rights before granting access to the various systems. As a result, SSO solutions are typically more costly and difficult to deploy and manage than password synchronization solutions.

Version3 Simple Sign-On uses nothing more than an organization's existing Active Directory for infrastructure and requires a small footprint, self-unloading agent on the client to function. Planning, deployment, and implementation require minutes to days, versus weeks to months.

4. **Access Management** – An effective access management system incorporates one or more methods of authentication to verify the user including passwords, digital certificates, hardware tokens or software tokens.

If Active Directory authentication alone is found to be insufficient, Version3 Simple Sign-On allows the administrator to easily integrate with any third-party access management software on the market today.

In its simplest form, **single sign-on** allows a user to log on to the network and to have all applications rely on the network to authenticate the user.

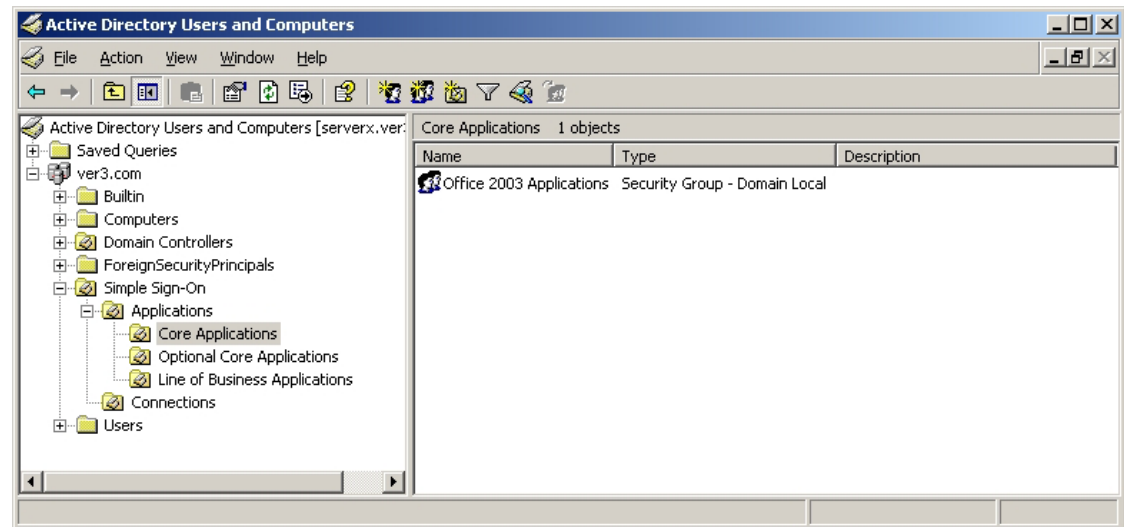
How does it work?

Version3 Simple Sign-On works by simulating actions that the user would normally perform from a Windows-based workstation. Almost anything a user can do, Version3 Simple Sign-On can do on the user's behalf. Since Version3 Simple Sign-On also adds an encrypted password store to Microsoft's Active Directory, user credentials can be presented to applications on behalf of each user.

A user must first authenticate a session with the network using any of the technologies supported by Active Directory. Based on the user's credentials, icons and shortcuts are created by Version3 Simple Sign-On representing the applications the user has been provisioned with. Once on the network, the user activates a Version3 Simple Sign-On application session by selecting an icon from the workstation desktop. As soon as the application challenges the user for credentials, Version3 Simple Sign-On supplies the secure information from the encrypted password store.

Like many network functions, configuration for Version3 Simple Sign-On is managed with the *Active Directory Users and Computers* console (see **Figure 0-1**). With this tool, the administrator can configure users, computers and applications across the enterprise.

Figure 0-1 Use the Active Directory Users and Computers console to manage Version3 Simple Sign-On.



Design overview

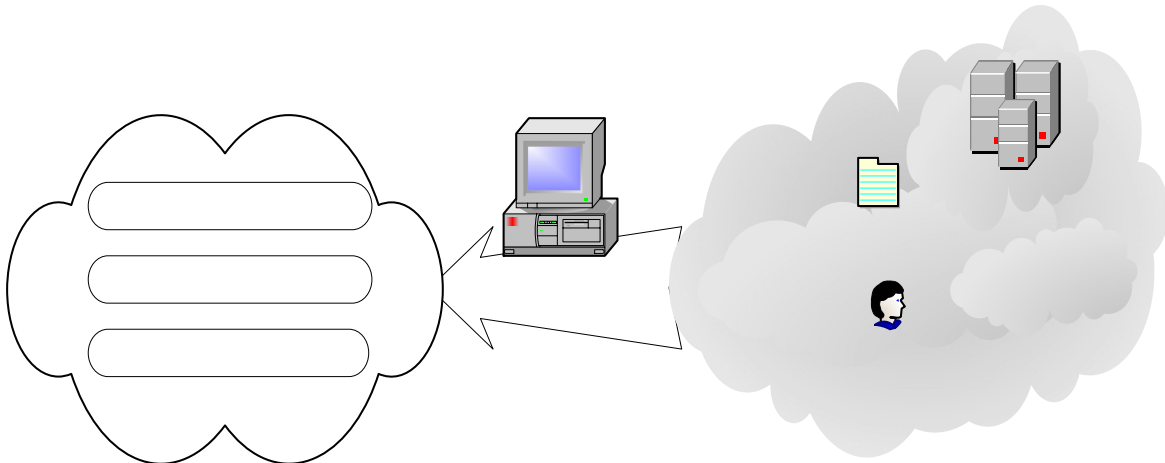
Version3 Simple Sign-On is a collection of integrated, Active Directory-enabled components. It uses Active Directory to store critical information about applications and users. To optimize the interaction with Active Directory's distributed engine, information stored in Active Directory is compressed, encrypted, and secured.

During installation, Version3 Simple Sign-On adds several properties to the Active Directory definitions of users and groups, along with a number of new Active Directory classes. The installation also makes additions to the Active Directory console tools to support the management of these Active Directory extensions.

Version3 Simple Sign-On stores all information in the Active Directory database; therefore, all information is replicated between domain controller servers in the same domain with no additional setup or configuration by the Version3 Simple Sign-On administrator.

With the Active Directory extensions in place, application definitions can be imported from the catalog of common applications or created from scratch using the Version3 Simple Sign-On script recorders. Version3 Simple Sign-On utilizes the Microsoft Windows scripting engine, which supports VBScript and JavaScript.

Figure 0-2



Version3 Simple Sign-On stores all application data and its respective logon credential information in the Active Directory database in an encrypted form. When a Version3 Simple Sign-On client requests an application, the logon credentials are passed from the domain controller across the network in a secure, encrypted format as well.

When defining applications for use by Version3 Simple Sign-On, an administrator can determine which users get the program group menu. This places control of applications in the hands of the administrator, not the users.

Also, Version3 Simple Sign-On requires a zero-footprint client to be installed on each workstation. The client manages access to all of the defined applications and merges the application definitions with user information to accomplish a seamless user logon sequence.

In addition, Version3 Simple Sign-On provides the following:

Application Publishing

The client portion of Version3 Simple Sign-On includes the ability to build icons and shortcuts in an administrator defined location. This means that the administrator has control over which user gets each shortcut and where the shortcut is placed. These shortcuts can be placed in the Programs Menu, on the desktop or anywhere else the administrator desires. The rebuilding of shortcuts is extremely fast and can be automated as part of a user's logon process thereby ensuring that all icons for critical applications are always available and that all shortcuts for disallowed applications are removed.

Identity Maintenance

Version3 Simple Sign-On allows administrators to provision identities for users and their applications and it allows administrators to maintain those identities with auto-password generation following defined rules at password change time. Users are not required to enter new complex passwords. Better yet, users don't need to remember the passwords or even be aware of them.

Connection Provisioning

Version3 Simple Sign-On comes with additional tools that give administrators the ability to easily define connections to network printers and folder shares. With this option, the administrator has a graphical interface to define these connections for the users based on the user account or the computer the user is logging on to. User and computer objects in the Active Directory Users and Computers console include an additional tab to define the properties of the connections.

Application Recorder

Application Recorder assists administrators in defining the responses to application logon processes. With the Application Recorder, actions that are required to enter the name and password for an application can be monitored and traced. This includes Windows, Internet, and extranet applications. In general cases, the Application Recorder create the scripts necessary to answer the application names and passwords. For more complex scenarios, a robust script editor is provided for modifying the scripts.

Version3 Simple Sign-On Extensibility

Many organizations today require stronger forms of authentication than what provided natively by Active Directory. For this reason, SecureID keys, biometrics such as fingerprint and retinal scans, and many other forms of secondary authentication are implemented within these organizations.

Version3 Simple Sign-On has additional identity management extensibility. This allows for integration of Version3 Simple Sign-On with virtually any third-party authentication tools.