

SAP and Sphinx:

How organizations using SAP can increase their IT security with Sphinx.

The purpose of this overview document is to point out the types of organizations that can benefit from using Sphinx with their SAP installations, and how Sphinx can increase IT security while making overall logon processes faster and more convenient for end users.

1 Types of targeted organizations

Sphinx can benefit all companies, government organizations, and institutions that

- Have implemented or plan to implement SAP,
- Are using Windows client computers or thin clients for their users,
- Want to enable their users to logon to Active Directory and/or their SAP accounts more securely,
- Want to remove the burden and risk associated with end users handling complex passwords, and want to make their logon processes more secure, faster and more convenient.

2 Government compliance regulations

Strong authentication security has never been more important. In many sectors such as government, healthcare, finance, and others it may already be a requirement to implement improved security policies that include two-factor authentication.

SAP is in use in many heavily regulated sectors such as healthcare, e-government, and companies working in security sensitive fields. It is therefore likely that many organizations using SAP are required by law to elevate their efforts to protect their IT environment from unauthorized access.

3 No impact on infrastructure

For organizations using SAP it is important to note that Sphinx can be installed on their system without impacting their existing IT infrastructure. Sphinx does not change or require any changes relating to the organization's Active Directory or SAP configuration. Nor does

Sphinx require modifications to the existing user accounts. Sphinx simply provides end users with the means to adhere to the most stringent password policies with ease.

4 Configuration and deployment

Sphinx is easy to install and configure. Sphinx CardMaker, the server and card management application, can be installed within minutes, typically on a dedicated or virtual server. Configuration of program preferences, group policies for cardholders, and pre-defined card content can all be centrally performed before cards are issued, and can later be updated in real time while cards are in circulation.

For SAP users, the administrator can easily configure cardholder groups, and each group can be assigned with pre-configured logon entries for specific SAP modules. For end users, the interaction is as simple as entering their Windows and/or SAP logon credential to self enroll upon first use of their card with Sphinx. Once users have self enrolled, the administrator has the option to have Sphinx update the Windows/SAP passwords to strong, random strings, since the passwords will be stored by the card and the end user no longer needs to know them. Sphinx can also be set to automatically update the Windows/SAP passwords on a regular basis, further strengthening password policies. Thereafter, users only need to present their card and optionally enter a short card PIN whenever a Windows or SAP authentication is required.

Sphinx can be pre-configured so that new users can self enroll using newly issued cards, or they can use cards that they may already have in use. Sphinx is compatible with 50+ different card types, which makes it the optimal choice for companies that already have corporate ID cards like contact smart cards (PIV, CAC, Java, Multos ...), or RFID facility access cards (NXP Mifare/DesFire, HID Prox/iClass ...) in circulation.

If a user loses or forgets to bring his card, Sphinx allows user to self re-enroll with a new or temporary card. Administrators can grant or revoke the permission to self re-enroll.

5 Why IT administrators, users, and decision makers love Sphinx

SAP consists of many modules and allows for many different user types. User types can be distinguished via a myriad of specific access privileges. Sphinx makes it easy for the administrator to transition from an environment where passwords had to be manually entered and managed by the end user, to a more secure workplace, where end users only need to present their ID card and enter an optional PIN.

Since passwords are now kept in a secure place, users are relieved of the otherwise burdensome tasks of adherence to complex password policies, managing different passwords, regular password changes, etc.

While end-user managed passwords can be a security as well as a help desk nightmare, end users who use Sphinx enjoy a much more convenient way of logging on. There is no need to look up or enter passwords, no typos while entering passwords, no forgetting of passwords, and no sticky notes with passwords on monitors and desks.

Decision makers are pleasantly surprised how Sphinx provides full-featured two-factor authentication, supported by over a decade of satisfied installations, at a reasonable cost. The cost to install and run Sphinx is typically well below other vendors in the marketplace. Part of this savings is because initial configuration requires no infrastructure changes or installation of proprietary hardware systems with their accompanying costs. Ongoing maintenance fees are also minimal, boiling down to a standard software support contract. And since licenses are reusable and transferrable - a feature that most vendors in the marketplace do not offer – new licenses only need to be purchased when the organization expands.

6 Key benefits of Sphinx

For organizations using SAP it will be important that Sphinx can be installed on their system without impacting their existing IT infrastructure. Sphinx does not change or require any changes related to the organization's Active Directory or SAP configuration, nor does it require modifications to the existing user accounts - Sphinx simply provides end user with the means to adhere to the most stringent password policies with ease.

While it is difficult to exactly quantify the benefits of warding off potential attacks to an organization's IT infrastructure, the potential risks associated with data loss, loss of Intellectual Property, lawsuits after an intrusion due to lack of security, are enormous. Sphinx can mitigate these risks while providing employees with the convenience to easily adhere to strict password security.

In summary, some of the key benefits are:

- Increased overall IT security.
- Reduced help desk calls due to forgotten passwords.
- Allows organizations to implement more secure password policies.
- Increases employee efficiency.
- No changes to existing IT infrastructure.
- ROI is achieved in a matter of months, not years.



Open Domain Sphinx Solutions, Inc.
www.odsphinx.com

© 2012 Open Domain Sphinx Solutions, Inc. All rights reserved.

This White Paper is for informational purposes only. Open Domain Sphinx Solutions has provided the information contained herein to the best of its knowledge but cannot guarantee the accuracy of any information presented in this paper. Product or company names mentioned herein may be the trademarks of their respective owners.

OPEN DOMAIN SPHINX SOLUTIONS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.