

Safeguard Authentication Services Single Sign-on for SAP®

提升您的 SAP 資料的安全性、隱私性及合規性

優點

- 為運行在 Unix 或 Linux 上的 SAP 提供真正以 Active Directory 為基礎的單一登入
- 消除使用者密碼在網路上的傳輸
- 當 SAP 資料透過網路傳輸時會進行安全加密
- 提供使用 AD 為 SAP 身分認證行為的稽核軌跡
- 簡化部署，無需 PKI (Public Key Infrastructure) 或認證基礎架構

對許多組織來說，SAP 應用程式和服務是極為關鍵的任務。然而，SAP 應用程式通常必須符合法規、內部控制以及企業最佳實踐所要求的嚴格標準，包括：

- 確保只有適當的人員有權存取資料
- 確保這些人可以存取 SAP
- 確保在關鍵任務資訊在網路移動時的安全

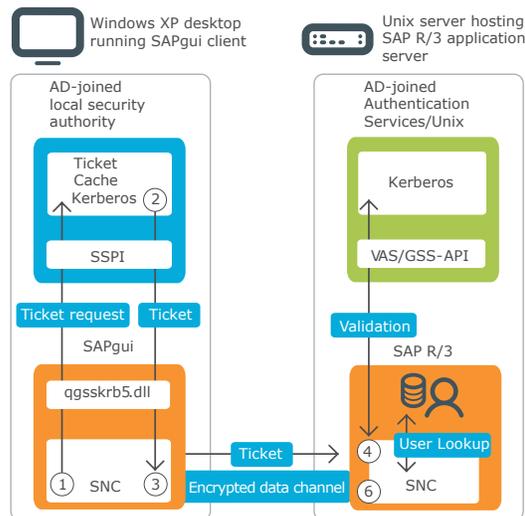
SAP 的單一登入 (SSO) 可幫助組織符合以上目標。不幸的是，單一登入一直難以實現，尤其在現今日益複雜的多平台環境中。

One Identity Safeguard Authentication Services Single Sign-on for SAP 為有使用 SAP 的企業提供真正的單一登入。此解決方案讓使用者在網路登入時獲得憑證的 Windows、Unix 及 Linux 上能夠透明公開驗證他們的 SAP 應用程式，為繁瑣複雜的同步或原始目錄解決方案，提供了另一種經濟高效、經過企業認證和以標準為基礎的替代方案。

Microsoft Active Directory (AD) 使用業界標準的 Kerberos 和 LDAP 為身分認證、授權和存取提供了合規、安全和可擴充的基礎架構。Safeguard Authentication Services Single Sign-on for SAP 透過允許 Unix 和 Linux 系統“加入”AD 網域，並將這些功能擴充到 SAP 使用者上。

系統需求

更多有關系統需求的完整資訊，請參考 www.oneidentity.com/products/safeguard-authentication-services



- 1 SAPgui 透過 One Identity 的 qgsskrb5.dll 請求 Kerberos Service Ticket，qgsskrb5.dll 將 GSS API 請求轉換為 SSPI。
- 2 回傳 Windows KDC 生成的 Ticket
- 3 SAPgui 客戶端利用回傳的 Ticket 連接到 SAP R/3 應用伺服器。
- 4 SAP R/3 應用程式伺服器使用身分驗證服務 Unix GSS API 資料庫驗證 ticket。
- 5 Kerberos ticket UPN 被對映到 SAP R/3 帳號。
- 6 使用 Kerberos ticket 中提供的資訊建立 (可選) 加密資料管道。

Safeguard Authentication Services Single Sign-on for SAP 透過允許 Unix 和 Linux 系統“加入”AD 網域，為 SAP 使用者提供安全的、企業範圍內的單一登入。

因此真正的單一登入消除了密碼管理問題、確保了卓越的使用者體驗、大幅減少了管理工作量，並提高了安全性。Safeguard Authentication Services Single Sign-on for SAP 利用先進的加密技術保護傳輸中的 SAP 資料，進一步提升安全性和合規性。

功能

異構環境中真正的 SAP 單一登入 — Safeguard Authentication Services Single Sign-on for SAP 在本地端的 Unix 和 Linux 系統上實施 Kerberos 和 LDAP，其實施方式與標準和在 Windows 中是相同的。藉由建立一個涵蓋 Unix、Linux 和 Windows 的單一“可信領域”，該解決方案為 SAP 提供了真正的單一登入，它還為 SAP 身分驗證行為提供了稽核軌跡。

降低的總擁有成本 (TCO) — Safeguard Authentication Services Single Sign-on for SAP 將您已部署的強大 AD 架構擴充至企業其他部門，無需再為非 Windows 的系統購買、部署和支援其他基礎架構、工具和技術。

簡化身分管理 — 由於 Unix 和 Windows 帳號被整合到單一身分儲存區 (Active Directory) 中，因此可以使用與 Windows 帳號相同的工具同時配置和取消配置 Unix 帳號，以及其他進階的身分管理功能，例如密碼管理、審核和角色管理，也都可以集中到 AD 中。

強大的、以標準為基礎的安全性 — SAP 的 Supply Network Collaboration (SNC) 介面提供 SAP 客戶端和伺服器具有獨立平臺的安全和身分驗證基礎架構，充分利用了本地 Windows 和 Unix 的安全機制。以 Windows 為基礎的 SAP 客戶端可以使用 Kerberos tickets 和 Unix 託管的 SAP R/3 伺服器交換安全身分驗證的 tokens。

進階的資料保護 — Safeguard Authentication Services Single Sign-on for SAP 支援 DES 和 RC4 加密方法，以保護傳輸中資料的隱私性，並且無需透過網路傳送使用者的密碼。

SAP 認證 — Safeguard Authentication Services Single Sign-on for SAP 已獲得 SAP 對 BC-SNC 4.0 介面的認證。它是唯一經過認證的 SAP 解決方案，也提供了 Unix 身分與 Active Directory 的全面整合。為必須登入 R/3 伺服器的 Unix 和 SAP 管理者提供的好處，讓他們可以利用 AD 使用者名稱和密碼憑證，或使用支援單一登入的終端客戶端進行透明公開的認證在 Windows 桌面上。

關於 One Identity

One Identity by Quest 幫助組織在內部部署、雲端或複合式環境中實施以身分識別為中心的安全性策略。憑藉其獨一無二、廣泛的身分和存取管理產品組合，包括帳號管理、身分治理與管理、特權存取管理，組織可充分發揮自身潛能，並以身分識別做為計畫核心，啟用對所有使用者類型、系統及資料的適當存取權，藉此達成安全性目標。更多詳細資訊請至 [Oneidentity.com](https://www.oneidentity.com)

© 2020 One Identity LLC ALL RIGHTS RESERVED. One Identity, and the One Identity logo are trademarks and registered trademarks of One Identity LLC in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.oneidentity.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.
Datasheet_SG-AuthServ-SSO4SAP_RS_63084