DATENBLATT

# Safeguard Authentication Services Single Sign-on für SAP®

## Verbesserung von Sicherheit, Datenschutz und Compliance Ihrer SAP Daten

## Vorteile

- Bietet "echtes" Active Directory-basiertes Single Sign-on für SAP auf Unix oder Linux
- Macht die Übertragung von Benutzerkennwörtern über das Netzwerk überflüssig
- Verschlüsselt SAP Daten sicher bei der Übertragung über das Netzwerk
- Bietet ein Audit-Trail für SAP Authentifizierungsaktivitäten mit AD
- Vereinfacht die Bereitstellung ohne Erfordernis einer PKI oder Zertifikatsinfrastruktur

## Systemanforderungen

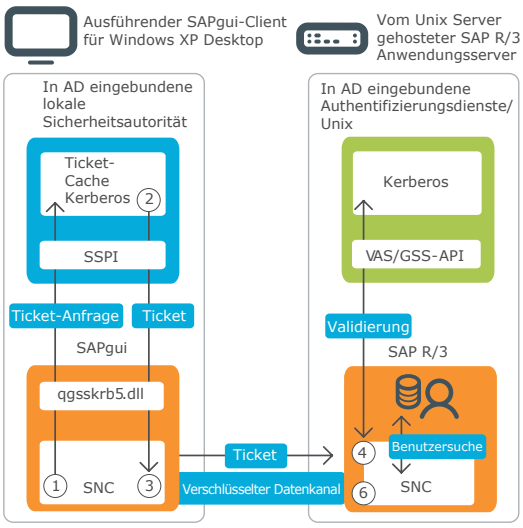
Eine vollständige Liste der Systemanforderungen finden Sie unter: www.oneidentity.com/products/safeguard-authentication-services

Für viele Unternehmen sind Anwendungen und Services von SAP® unerlässlich. Die Anwendungen von SAP müssen häufig jedoch strenge Standards erfüllen, die zur Einhaltung gesetzlicher Auflagen, aufgrund interner Kontrollen und gemäß den Best Practices des Unternehmens vorgegeben sind. Dazu zählen unter anderem folgende Dinge:

- Sicherstellung, dass nur die richtigen Personen Zugriff auf Daten haben
- Gewährleistung, dass diese Personen auf SAP zugreifen können
- Sicherung dieser unternehmenskritischen Informationen, während diese über das Netzwerk übertragen werden.

Single Sign-on (SSO) für SAP Kann Unternehmen dabei helfen, alle diese Ziele zu erreichen. Leider war die Implementierung von Single Sign-on bisher immer schwierig, vor allem in den heutzutage immer komplexer werdenden Multiplattform-Umgebungen – doch das ändert sich nun.

One Identity Safeguard Authentication Services Single Sign-on für SAP von Quest liefert echtes Single Sign-on für SAP für das ganze Unternehmen. Die Lösung ermöglicht es Benutzern, ihre SAP Anwendungen auf Windows, Unix und Linux mit den bei der Netzwerkanmeldung erhaltenen Anmeldedaten transparent zu authentifizieren. So stellt sie eine kostengünstige, für Unternehmen bewährte und standardbasierte Alternative zu umständlichen und komplexen Synchronisations- oder Metaverzeichnisdienstlösungen dar.




1. SAPgui fordert ein Kerberos Service-Ticket über qgsskrb5.dll von One Identity an, was GSS-API-Anfragen in SSPI umwandelt.
2. Es wird ein Windows KDC-generiertes Ticket zurückgesendet.
3. Der SAPgui-Client verbindet sich mit dem SAP R/3 Anwendungsserver und gibt so das zurückgesandte Ticket weiter.
4. Der SAP R/3-Anwendungsserver validiert das Ticket über die Authentication Services Unix GSS-API-Bibliotheken.
5. Der UPN des Kerberos-Ticket wird dem SAP R/3 Konto zugeordnet.
6. Mithilfe der Informationen im Kerberos-Ticket wird ein (optional) verschlüsselter Datenkanal erstellt.

*Safeguard Authentication Services Single Sign-on für SAP sicheres, unternehmensweites Single Sign-on für SAP, indem es Unix und Linux System erlaubt, sich mit der AD Domäne zu "verbinden".*

Microsoft® Active Directory® (AD) nutzt speziell die Branchenstandards Kerberos und LDAP, um eine konforme, sichere und skalierbare Infrastruktur für Authentifizierung, Autorisierung und Zugriff bereitzustellen. Safeguard Authentication Services Single Sign-on für SAP weitet diese Fähigkeiten auf SAP Benutzer mit Unix oder Linux System aus und erlaubt diesen Systemen, sich mit der AD Domäne zu "verbinden".

Dank des daraus resultierenden echten Single Sign-on gibt es keine Kennwortverwaltungsprobleme mehr. So wird ein besseres Benutzererlebnis sichergestellt, der Verwaltungsaufwand erheblich reduziert und die Sicherheit verbessert. Darüber hinaus Safeguard Authentication Services Single Sign-on für SAP kann die SAP Daten durch erweiterte Verschlüsselungstechnologien bei der Übertragung schützen und verbessert so Sicherheit und Compliance.

## Funktionen und Merkmale

**Echtes Single Sign-on für SAP in heterogenen Umgebungen –**Safeguard Authentication Services Single Sign-on für SAP implementiert Kerberos und LDAP nativ in Unix und Linux Systeme. Dies erfolgt auf dieselbe Art und Weise, wie diese Standards auch bei Windows genutzt werden. Durch Erstellung eines einzelnen "Trusted Realm" (vertrauter Bereich), in dem Unix, Linux und Windows enthalten sind, liefert die Lösung echtes Single Sign-on für SAP und stellt gleichzeitig einen Audit-Trail für SAP Authentifizierungsaktivitäten zur Verfügung.

**Niedrigere Gesamtbetriebskosten –** Safeguard Authentication Services Single Sign-on für SAP weitet die robuste AD Infrastruktur, die Sie bereits bereitgestellt haben, auf das restliche Unternehmen aus. So ist es nicht mehr erforderlich, zusätzliche Infrastruktur, Tools und Technologien für Nicht-Windows-Systeme zu kaufen, bereitzustellen und zu betreuen.

**Vereinfachte Identitätsverwaltung –** Seitdem Unix und Windows Konten in einen einzigen Identitätsspeicher (Active Directory) integriert sind, können Bereitstellung und Aufhebung der Bereitstellung bei Unix Konten mit denselben Tools und zur selben Zeit erfolgen wie bei Windows Konten. Zudem können andere erweiterte Identitätsverwaltungsfähigkeiten, wie z. B. Kennwortverwaltung oder Audit- und Rollenmanagement, in AD zentralisiert werden.

**Robuste, standardbasierte Sicherheit –** Die SAP Supply Network Collaboration (SNC) Schnittstelle bietet SAP Clients und Servern eine plattformunabhängige Sicherheits- und Authentifizierungsinfrastruktur, die die nativen Windows und Unix Sicherheitsmechanismen voll ausschöpft. Windows-basierte SAP Clients können sichere Authentifizierungstoken über Kerberos-Tickets mit Unix-gehosteten SAP R/3 Servern austauschen.

**Erweiterter Datenschutz –** Safeguard Authentication Services Single Sign-on für SAP unterstützt sowohl DES- als auch RC4-Verschlüsselung, um die Vertraulichkeit der Daten zu schützen, während diese übertragen werden. So müssen Benutzerkennwörter nicht mehr über das Netzwerk übermittelt werden.

**SAP Zertifizierung –** Zusammen mit Active Directory ist Safeguard Authentication Services Single Sign-on für SAP von SAP für die BC-SNC 4.0 Schnittstelle zertifiziert. Somit handelt es sich um die einzige zertifizierte SAP Lösung, die auch eine vollständige Integration von Unix Identitäten in Active Directory bietet. Als zusätzlichen Vorteil ermöglicht sie es Unix und SAP Administratoren, die sich beim R/3 Server anmelden müssen, ihren AD Benutzernamen und ihr AD Kennwort zu nutzen oder sich transparent über einen Single Sign-on-fähigen Terminal Client auf einem Windows Desktop zu authentifizieren.

## Infos über One Identity

One Identity von Quest ermöglicht es Unternehmen, lokal, in der Cloud oder in einer Hybrid-Umgebung eine identitätszentrierte Sicherheitsstrategie zu implementieren. Dank unseres einzigartig breit gefächerten und integrierten Portfolios mit Angeboten zum Identitätsmanagement, einschließlich Kontoverwaltung, Identity Governance und Administration sowie Verwaltung des privilegierten Zugriffs, sind Unternehmen in der Lage, ihr volles Potenzial auszuschöpfen und Sicherheit dadurch zu erreichen, dass Identitäten in den Mittelpunkt des Programms gestellt werden und der ordnungsgemäße Zugriff für alle Benutzertypen, Systeme und Daten ermöglicht wird. Weitere Informationen finden Sie unter OneIdentity.com.


Datasheet_SG-AuthServ-SSO4SAP_RS_63084