PUBLIC

SAP Single Sign-On 3.0 SP02

Document Version: 1.1 – 2024-03-27

SAP Single Sign-On Master Guide

THE BEST RUN SAP

Content

1 **Getting Started.** 3

1.1 Related Information. 3

1.2 Important SAP Notes. 3

2 **SAP Single Sign-On Overview.** 5

2.1 Secure Login. 5

2.2 Identity Federation. 7

2.3 Single Sign-On Extension Library. 7

2.4 One-Time Password Authentication. 8

2.5 Policy Scripts. 8

3 **Disclaimer.** 10

1 Getting Started

SAP Single Sign-On (SAP SSO) enables companies to eliminate the need for multiple passwords and user IDs. With SAP SSO, part of a comprehensive single sign-on portfolio for multiple user authentication processes, you can lower the risks of unsecured login information, reduce help desk calls, and help ensure the confidentiality and security of personal and company data.

The master guide provides an overview of SAP Single Sign-On, its software units, and its scenarios. Use it to help you design your single sign-on system landscape before you start the implementation phase. It refers you to the required detailed documentation.

- SAP Notes
- Installation and upgrade information for individual software components
- Configuration and operation information for individual software components
- Security information for individual software components

1.1 Related Information

For more information about planning topics not covered in this guide, see the content on SAP Service Marketplace, SAP Help Portal, and SAP Community Network.

Related Information

http://help.sap.com/sso30

http://scn.sap.com/community/netweaver-sso

https://service.sap.com/message

https://support.sap.com/notes

https://service.sap.com/rkt

https://service.sap.com/sap/support/pam?hash=pvnr%3d67837800100900006373

https://support.sap.com/swdc

1.2 Important SAP Notes

Read the following SAP Notes before you start the installation.

These SAP Notes contain the most recent information on the installation, as well as corrections to the installation documentation. Make sure that you have the up-to-date version of each SAP Note, which you can find on *SAP Service Marketplace*.

Related Information

https://service.sap.com/sap/support/notes/2338174

2 SAP Single Sign-On Overview

SAP Single Sign-On (SAP SSO) enables companies to eliminate the need for multiple passwords and user IDs.

To navigate the heterogeneous IT environments common to most systems within companies, people frequently must use multiple sets of authentication credentials. This reduces business user efficiency and increases risks to sensitive company and personal information. With SAP SSO, part of a comprehensive single sign-on portfolio for multiple user authentication processes, you can lower the risks of unsecured login information, reduce help desk calls, and help ensure the confidentiality and security of personal and company data.

SAP SSO consists of the following components:

- Secure Login
- Identity Federation
- Extension for Kerberos Constrained Delegation
- One-Time Password Authentication
- Policy Scripts

For more information about the scenarios in which you can deploy these components, see the relevant component documentation.

Related Information

Secure Login [page 5]
Identity Federation [page 7]
Single Sign-On Extension Library [page 7]
One-Time Password Authentication [page 8]
Policy Scripts [page 8]

2.1 Secure Login

With Secure Login, business users only have to authenticate when they initially log in.

Strong encryption provides additional security for communication with GUIs and web browsers. User activities are protected from unauthorized monitoring or manipulation. The application enables forced re-authentication for critical applications as well as digital signatures for legal contracts, and can allow access across firewalls.

This approach requires no additional public key infrastructure (PKI) solution because SAP Single Sign-On (SAP SSO) includes the necessary X.509 implementation. However, if a PKI solution is wanted, SAP SSO facilitates the integration of your existing PKI architecture.

The architecture that supports Secure Login offers a variety of possible combinations. The simplest implementation utilizes the Windows process that authenticates users when they log onto their computers in a certain domain and triggers the generation of an X.509 certificate. The user is then automatically logged into the SAP software he or she needs through a browser or Windows-based SAP GUI. Secure Login is flexible enough to integrate a wide variety of environments, even if the user IDs are not synchronized.

SAP SSO uses the standard encryption methods used in online banking applications based on Transport Layer Security (TLS) technology. Here, a cryptographic key "negotiated" between the client and server through the X.509 certificate encodes subsequent communications.

The following variants of a Secure Login solution are possible:

- Direct use of Windows-based Kerberos tickets for logging into SAP software
- Integration of other authentication procedures, such as Lightweight Directory Access Protocol (LDAP), the Remote Authentication Dial-In User Service (RADIUS), RSA SecurID, and smart cards
- Generation of X.509 certificates for web-based clients that have authenticated at an identity provider using Security Assertion Markup Language (SAML) 2.0
- Forced repeat authentication for critical applications that require more than basic verification, based on user names and passwords
- A client solution that requires only a minimum installation and grants browsers and instances of the Web GUI from SAP direct access to back-end systems across firewalls and domains through X.509 certificates
- Quick access to SAP GUI or browser based kiosk applications using RFID tokens for identification
- Client logon with SAP GUI using encrypted communication but without single sign-on
- Regular renewal of all or a group of certificates in defined AS ABAP / AS Java systems systems using certificate information from Secure Login
- Use of PKIs of Remote Certification Authorities (CAs), for example, with short-lived certificates and trust.
- Trust management using trusted CAs with the respective trust anchors for an Application Server ABAP

Using standard procedures, you can incorporate any number of target systems that employ X.509 certificates for client authentication into the SSO architecture. These methods combine the high level of security that strong encryption and authentication technologies offer based on open standards with the benefits of short implementation and roll-out times and the corresponding cost advantages. In other words, you no longer need additional proprietary or individually programmed solutions, and X.509 certificates will increase the integrity of your data. Users will be able to apply digital signatures to invoices and contracts, for example, by means of an interface included with SAP SSO.

Secure Login also enables logon support for Simple and Protected GSS API Negotiation Mechanism (SPNego) to Application Server ABAP. With a browser that supports SPNego, you can log on to an AS ABAP with your Windows credentials without any interaction from you, the user.

Secure Login Client can run as SSH key agent for authentication.

The default SAP Cryptographic Library (which comes with Application Server ABAP) supports a cryptographic module with a FIPS 140-2, security level 1 certification. FIPS 140-2 certification ensures that the cryptographic module of the SAP Cryptographic Library (which enables end-to-end encryption of communication channels between servers or between client and server) is designed, tested, and implemented correctly and indeed protects sensitive data from unauthorized access.

Related Information

Secure Login for SAP Single Sign-On Implementation Guide on SAP Help Portal

2.2 Identity Federation

Identity federation includes a SAML 2.0 identity provider and a security token service (STS) using the WS-Trust 1.3 standard.

You can use the identity provider for single sign-on (SSO) with SAP or non-SAP service providers. As an identity provider, SAP Netweaver Application Server (SAP NetWeaver AS) Java can provide cross-domain SSO in combination with SAML 2.0 service providers and at the same time enable single log-out (SLO) to close all user sessions in the SAML landscape. SAML 2.0 also enables identity federation by defining a name ID to be shared between the identity provider and one or more service providers.

You can use the STS to provide cross-domain SSO for web service providers. The STS converts what are often proprietary authentication methods from a Web service consumer into a security token consumable by the web service provider. The STS supports X.509, SAML 1.1, and SAML 2.0 security token types.

The identity federation component runs separately from the rest of SAP Single Sign-On. It can be installed together with the other components, but there are no technical dependencies between the identity federation component and the other SAP Single Sign-On components.

You can deploy this software on SAP NetWeaver AS for Java release 7.2 SPS 2 with SAP Note 1471322 applied or SAP NetWeaver AS for Java release 7.2 SPS 3 or later. However, to use the security token service or the newest user interface improvements in the identity provider, you must install the latest identity federation software component archive (SCA) and upgrade the host SAP NetWeaver AS for Java to release 7.2 SPS 4 or later.

Related Information

Identity Provider for SAP Single Sign-On and SAP Identity Management
Security Token Service for SAP Single Sign-On and SAP Identity Management

2.3 Single Sign-On Extension Library

This library provides support for Kerberos constrained delegation, which consists of a Service-for-User-to-Self (S4U2Self) extension and a Service-for-User-to-Proxy (S4U2Proxy) extension. This functionality can be used to obtain Kerberos service tickets on behalf of the currently authenticated user.

> ⓘ Note
>
> The library currently supports only the `RC4-HMAC` encryption algorithm.

2.4 One-Time Password Authentication

The one-time password (OTP) solution in SAP Single Sign-On (SSO) enables strong authentication for access to corporate resources.

You can use it to authenticate with passcodes generated by the an authenticator mobile application. Passcodes are time-based and valid for one logon attempt, meaning they are more secure than the common static passwords.

The OTP solution allows administrators to configure the following types of passcodes:

- Passcodes generated by an authenticator app.
- Random passcodes sent by SMS, email, or another channel.
- External passcodes (for example, RSA SecureID passcodes)

You can use the OTP authentication to:

- Log on to systems using Secure Login Client.
- Log on to systems using SAML, using SAP NetWeaver (NW) Application Server (AS) Java as an identity provider.
- Log on to web applications running on SAP NetWeaver AS for Java.

The OTP solution provides support for single-factor authentication or two-factor-authentication. With single-factor authentication, you log on with only one factor (for example, a user name and a passcode), while with two-factor authentication you provide two means of identification (for example, a passcode and your corporate password, X.509 certificate or others).

For more information, see One-Time Password Authentication Implementation Guide.

2.5 Policy Scripts

The policy scripts component of SAP Single Sign-On is used to control access to business applications.

With the implementation of policy scripts, you can control how users are authenticated. The following authentication mechanisms are supported with policy scripts:

- Authentication via TOTPLoginModule
  These policy scripts are used to customize access to business applications based on risk and contextual information, such as time, origin, authentication method, or device. The login module processes the active version of the specified script and decides which type of authentication to use.
- Authentication via an Identity Provider (IdP)
  For the IdP authentication, you specify policy scripts for IdP extensions as you can set policies for a trusted service provider or for all trusted service providers. These policy scripts can define which authentication method should be used, whether or not an assertion should be issued, and can define the attributes passed to the issued SAML 2.0 assertion.

Related Information

One-Time Password Authentication
Policy Scripts Implementation Guide
Configuring Policy Scripts for Identity Provider Extensions

3 Disclaimer

SAP Library document classification: **PUBLIC**.

This document is for informational purposes only. Its content is subject to change without notice, and SAP does not warrant that it is error-free. SAP MAKES NO WARRANTIES, EXPRESS OR IMPLIED, OR OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

Coding Samples

Any software coding and/or code lines/strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.

Accessibility

The information contained in the SAP Library documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP specifically disclaims any liability with respect to this document and no contractual obligations or commitments are formed either directly or indirectly by this document.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you, or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon ➦ : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon ➦: You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP