

SAML in the SAP J2EE Engine 6.40

Responsible: PM Product Security, security@sap.com

Introduction and Motivation

SAML Concepts

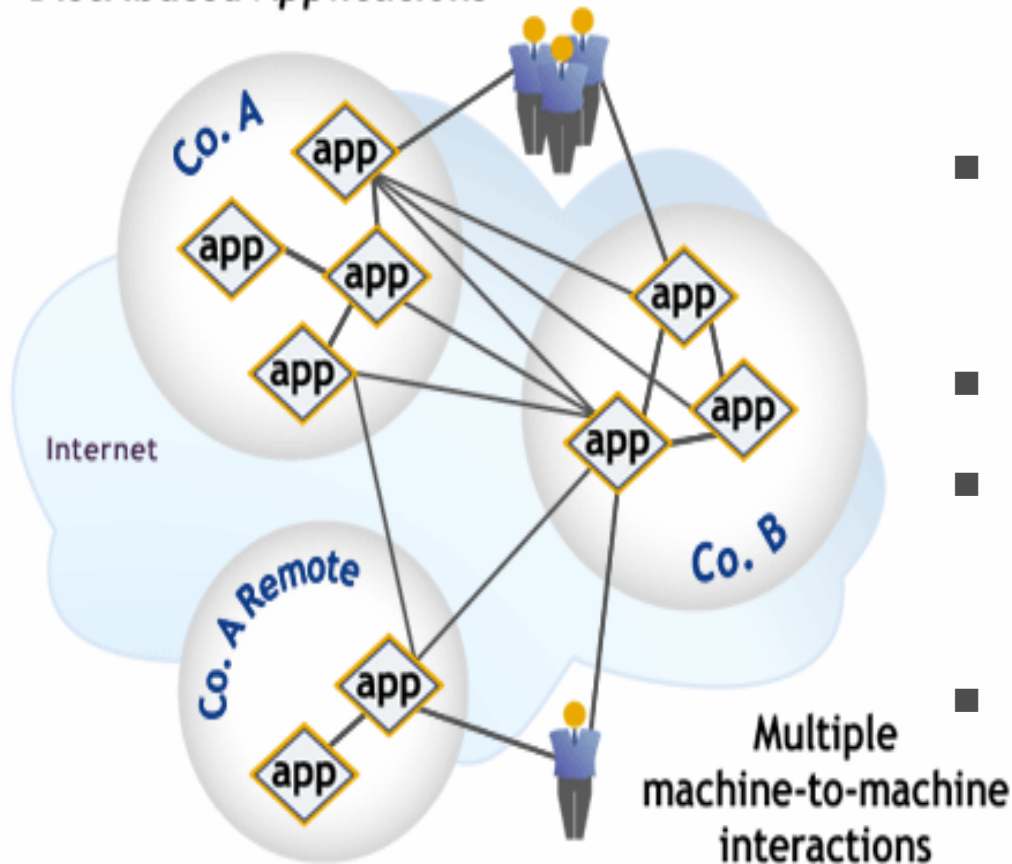
SAP J2EE and SAML

Configuring SAML for the SAP J2EE Engine

Summary

Security Requirements for Distributed Computing

Distributed Applications

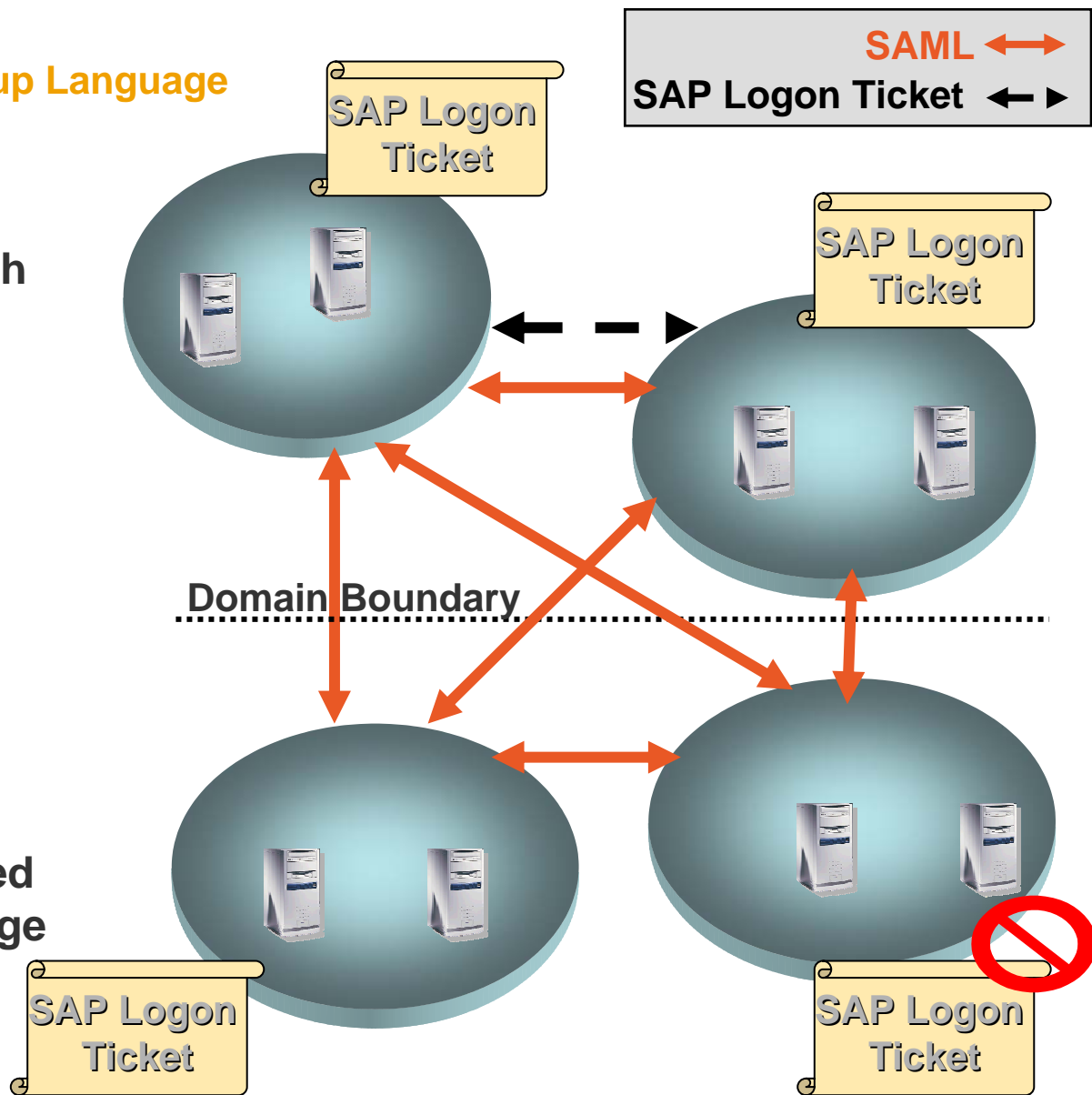


- Security in distributed applications, which span different companies, is crucial
- Current transport layer security protocols like SSL, TLS, IP Sec are not sufficient
- Application layer security is a must
- Security for Man-to-Machine and for Machine-to-Machine interaction is required
- Standard for distributed authentication and/or authorization is required

SAML Value Proposition

The Security Assertions Markup Language

- Interoperable security solutions to allow systems integration with great ease and minimal resources
- Enables remote access to protected resources by exchange of
 - Authentication Information
 - Authorization information
- Provides standard based mechanisms to exchange security information using SOAP, HTTP(s)



Introduction and Motivation

SAML Concepts

SAP J2EE and SAML

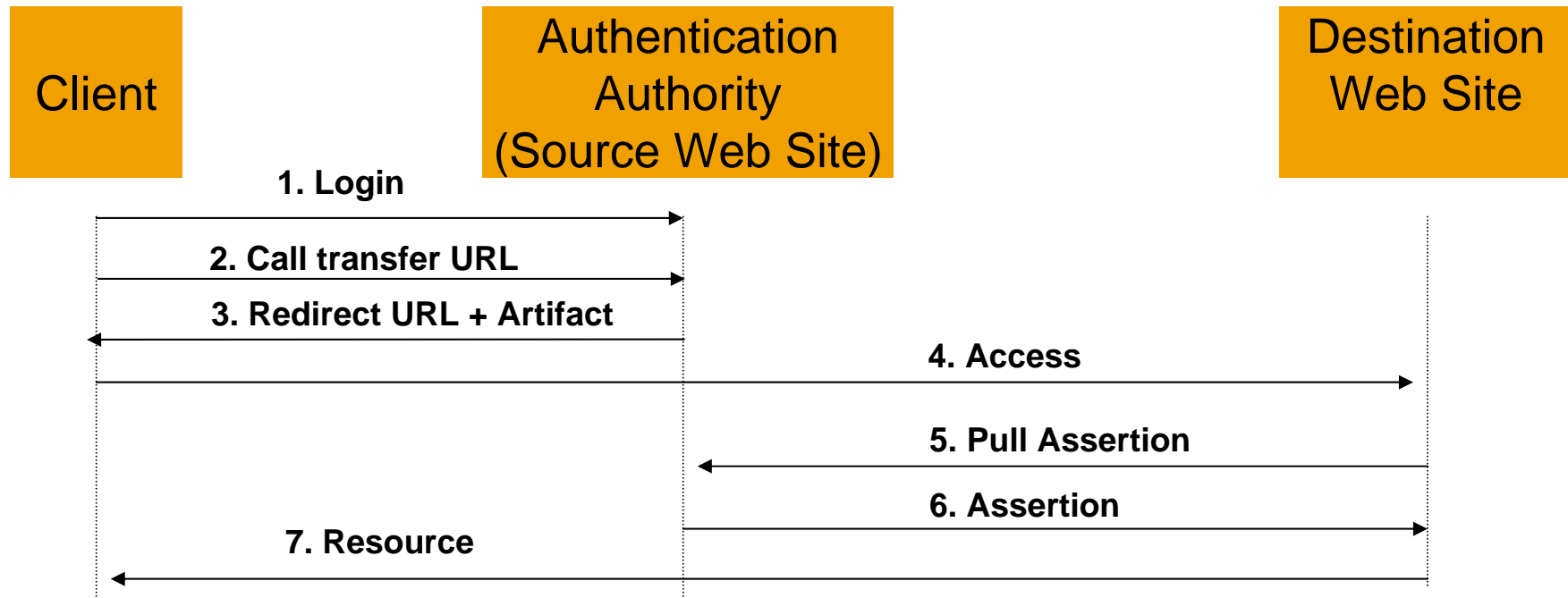
Configuring SAML for the SAP J2EE Engine

Summary

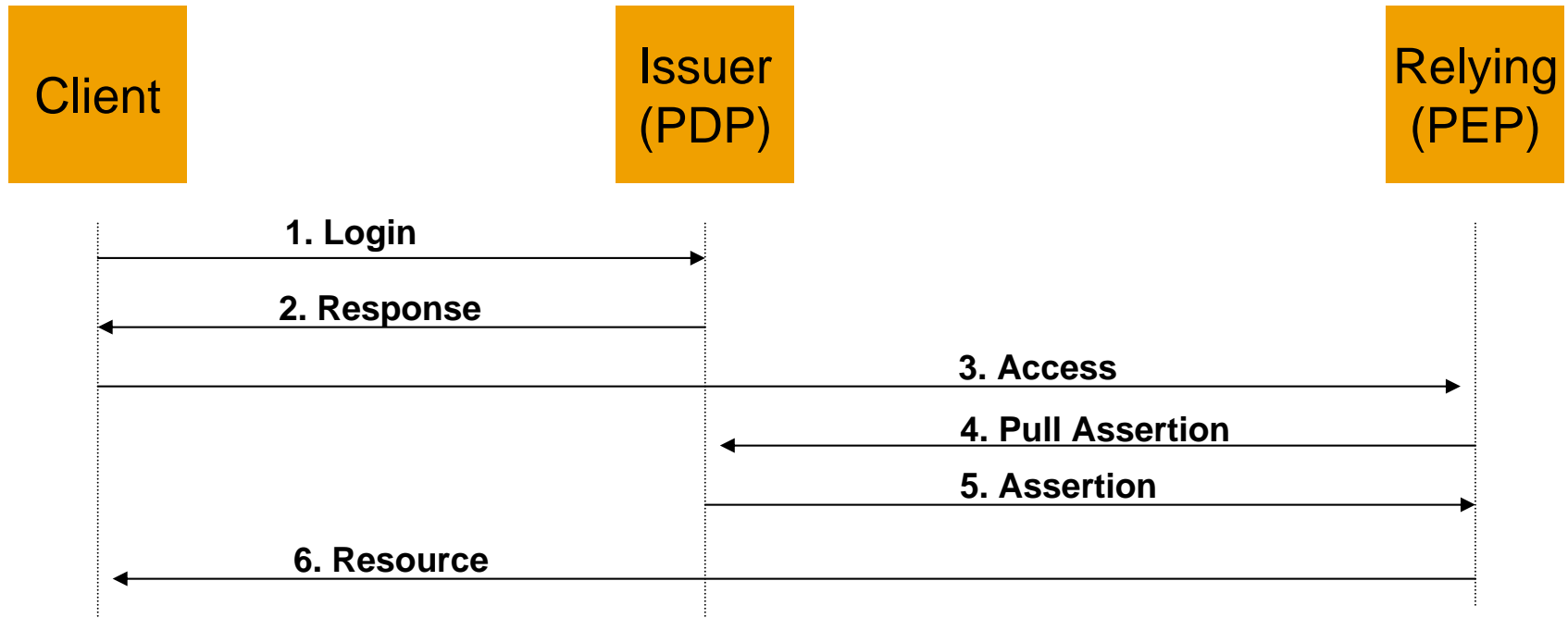
Facts about SAML:

- **SAML is a protocol for encoding security related information (assertions) into XML and exchange this information in a request/response fashion**
- **SAML does not authenticate users**
- **SAML relies for message exchange on Standard Security Protocols like SSL, TLS and uses XML signatures**
- **SAML authorities produce so called assertions on client requests. An assertion can be either an authentication or an authorization assertion**
 - ◆ **Authentication assertion - a piece of data that represents an act of authentication performed on a subject (user) by the authority**
 - ◆ **Authorization assertion: a piece of data that represents authorization permissions for a subject (user) on a resource**
- **SAML can be used for authentication and authorization requests and assertions**
- **SAML is an emerging OASIS standard**

Sample SAML Scenario for Single Sign On



Sample SAML Scenario for Authorization Assertions



PDP: Policy Decision Point
PEP: Policy Enforcement Point

Example of SAML Request and Response

SAML authentication request:

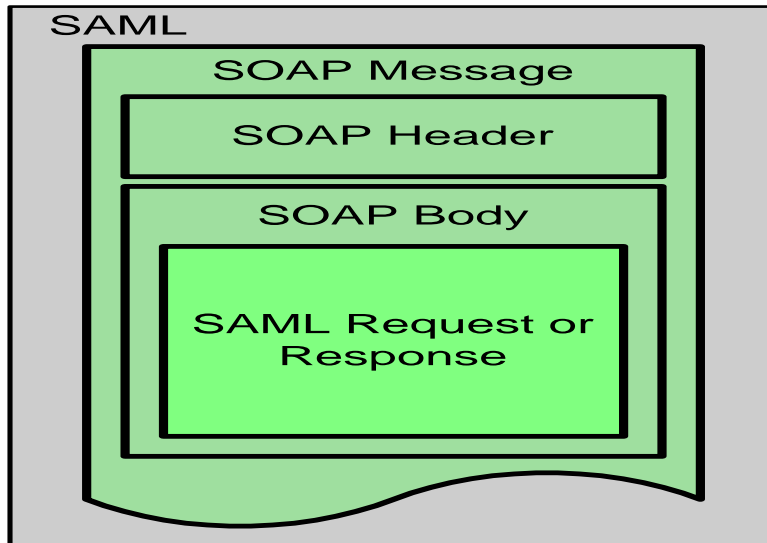
```
<samlp:Request
  MajorVersion="1" MinorVersion="0"
  RequestID="128.14.234.20.12345678" >
  <samlp:AuthenticationQuery>
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="smithco.com"
        Name="d030408" />
    </saml:Subject>
  </samlp:AuthenticationQuery>
</samlp:Request>
```

Authentication authorities SAML response with assertion:

```
<samlp:Response
  MajorVersion="1" MinorVersion="0"
  ResponseID="128.14.234.20.90123456"
  InResponseTo="128.14.234.20.12345678"
  StatusCode="Success">
  <saml:Assertion
    MajorVersion="1" MinorVersion="0"
    AssertionID="128.9.167.32.12345678"
    Issuer="Smith Corporation">
    <saml:Conditions
      NotBefore="2001-12-03T10:00:00Z"
      NotAfter="2001-12-03T10:05:00Z" />
    <saml:AuthenticationStatement ...>...
  </saml:AuthenticationStatement>
  </saml:Assertion>
</samlp:Response>
```

A binding is a way how to transport SAML requests and responses and therefore to secure the transfer. Possibilities are:

- **SOAP over HTTP(s) Binding**



- **Raw HTTP(s) binding (in future) ?**

Introduction and Motivation

SAML Concepts

SAP J2EE and SAML

Configuring SAML for the SAP J2EE Engine

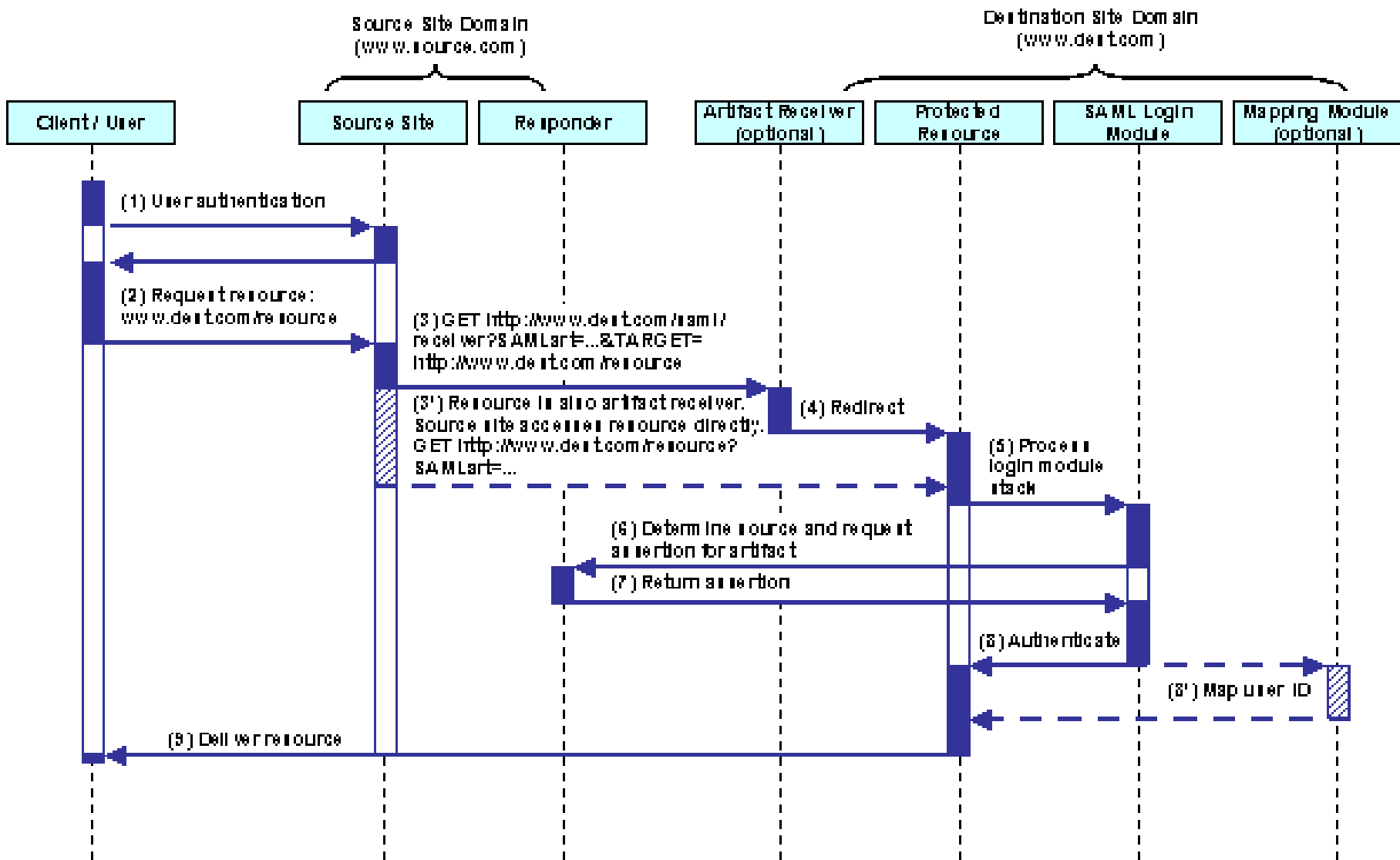
Summary

Only SAML client for authentication available at destination site is available.

Support limited

- **Only browser artifact scenario supported**
- **Digital signatures for SOAP documents are ignored**
- **No support for additional “Condition” elements**
- **The received assertion may only contain one authentication statement**
- **The authentication statement must contain the NameIdentifier**
- **AuthorizationDecisionStatement and AttributeStatement are ignored**

SSO - Process Supported in SAP J2EE Engine



Introduction and Motivation

SAML Concepts

SAP J2EE and SAML

Configuring SAML for the SAP J2EE Engine

Summary

Prerequisites:

- It is strongly recommended that you have configured SSL on the SAP J2EE Engine. SAML relies on secure transport mechanism

Steps for SAML configuration for the client SSO scenario in SAP J2EE Engine:

- Start the SAML Service
- Define a destination to the SAML responder
- Define SAML Parameters
- Adjust the JAAS login module stack for the services, which should be accessed by SAML

Start the SAML Service

The screenshot shows the SAP J2EE Engine Administrator interface. The title bar reads "SAP J2EE Engine Administrator - [J2E\Server 0 0_64129\Services\SAML]". The menu bar includes "Connect", "View", "Tools", and "Help". Below the menu is a toolbar with icons for navigation and actions. The left pane, titled "Global Configuration", shows a tree view of services under the "Cluster" node. A red arrow points to the "SAML" service, which is currently disabled (indicated by a red 'X' icon). The right pane, titled "Properties", has tabs for "Properties" and "Additional Info". It contains a table with columns "Key" and "Value", which is currently empty. Below the table are input fields for "Key:" and "Value:", and an "Update" button. At the bottom of the window, a status bar shows a green diamond icon and the text "Stop service SAML", along with a progress indicator at 100%.

Global Configuration

Cluster

- Basic Administra
- ClassLoader Vie
- Classpath Resol
- Configuration Ad
- Connector Conta
- Deploy
- Destinations
- EJB Container
- File Transfer
- HTTP Provider
- IIOP Provider
- JCo RFC Provide
- JDBC Connector
- JMS Connector
- JMS Provider
- JMX Adapter
- JMX Notification
- JNDI Registry
- Java Mail Client
- Key Storage
- Licensing Adapte
- Locking Adapter
- Log Configurator
- LogViewer
- Memory Info
- Message Info
- P4 Provider
- Remote Object C
- Runtime Info Pro
- SAML**
- SLD Data Suppli
- SSL Provider
- Secure Storage

Properties | **Additional Info**

Key	Value
-----	-------

Key:

Value:

Update

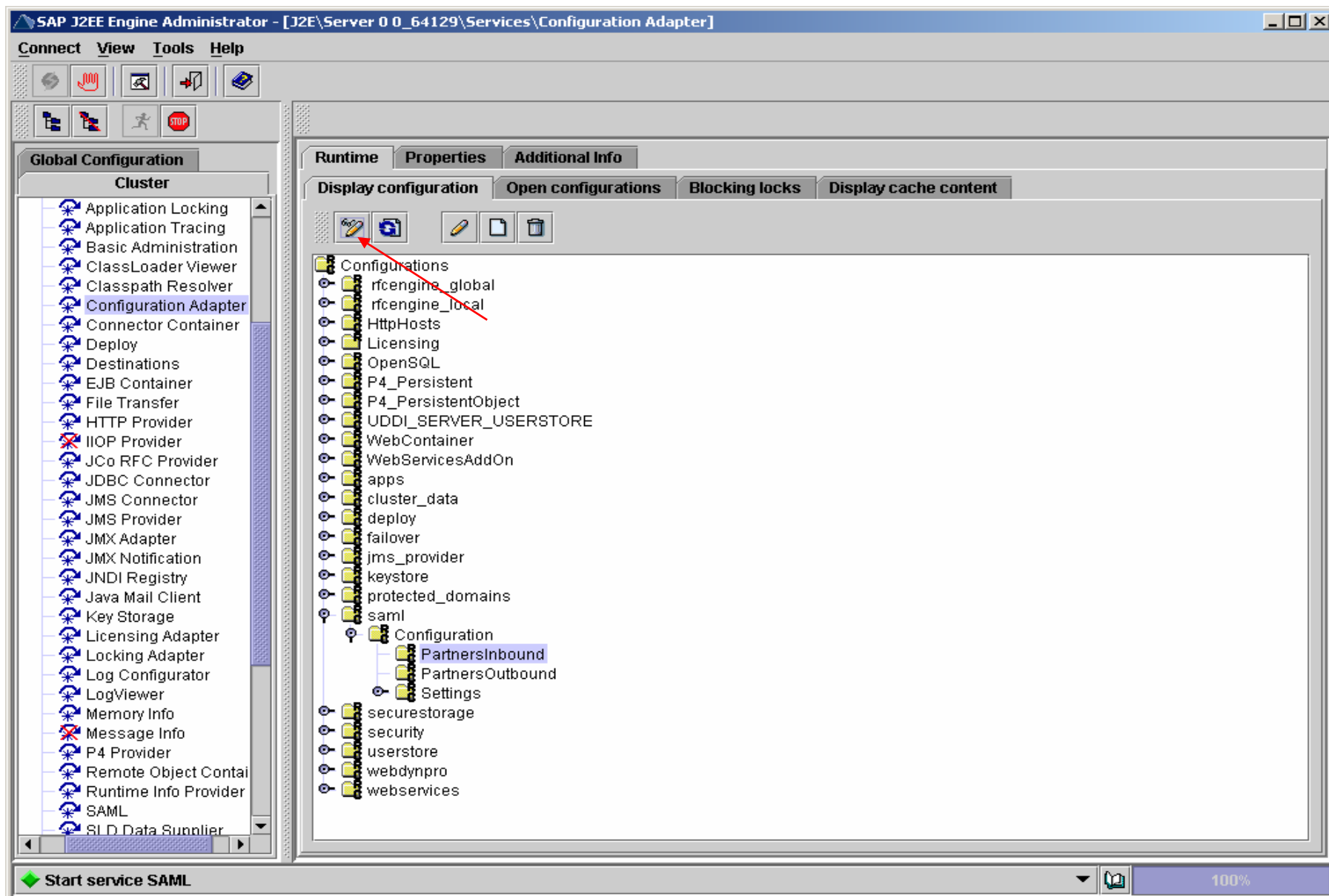
Stop service SAML | 100%

Create a Destination to the SAML Responder

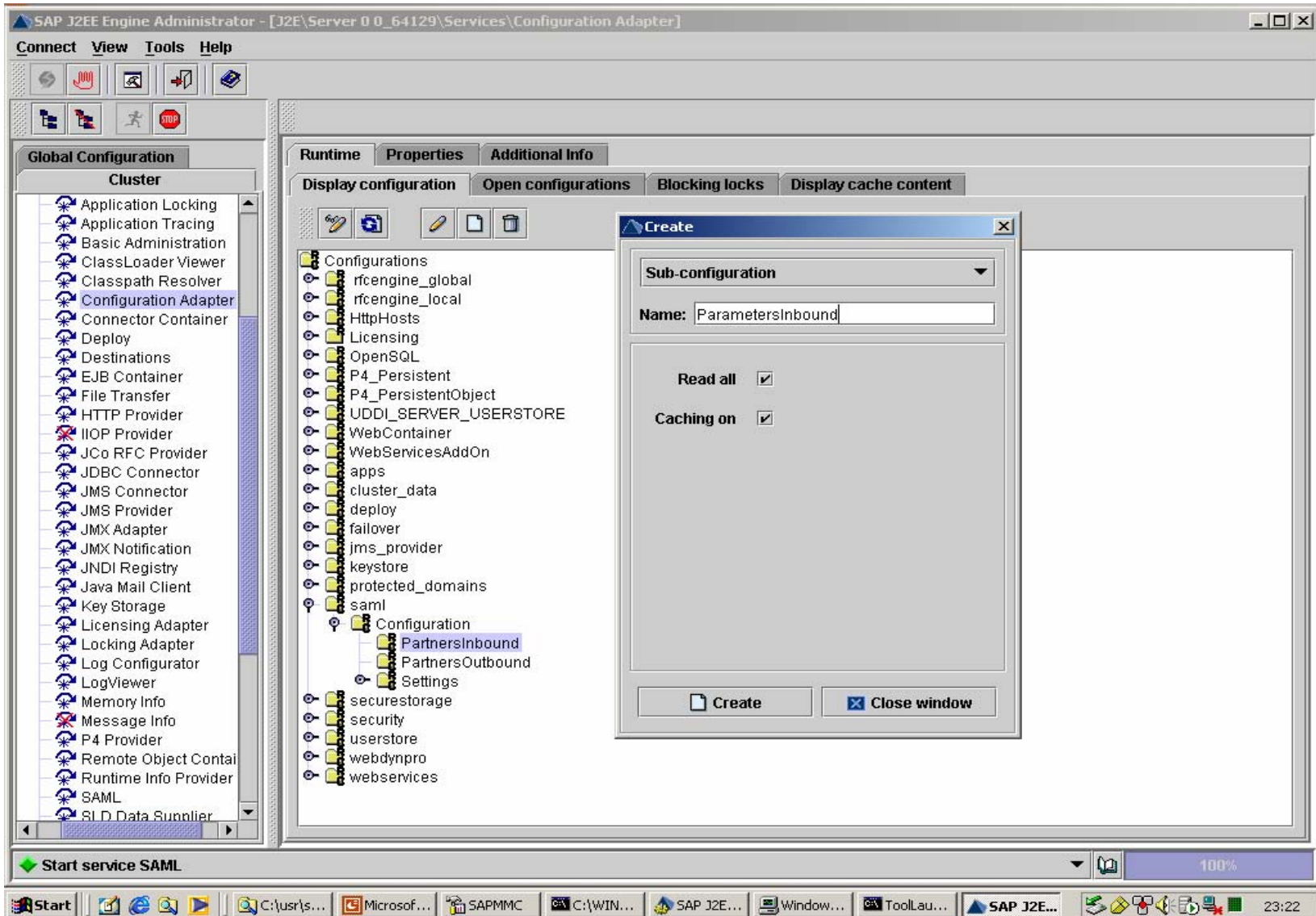
The screenshot displays the SAP J2EE Engine Administrator interface. The main window title is "SAP J2EE Engine Administrator - [J2E\Server 0 0_64129\Services\Destinations]". The interface is divided into several sections:

- Global Configuration:** A tree view on the left lists various services, with "Destinations" selected.
- Runtime Properties:** A tree view in the center shows the hierarchy: Destinations > HTTP > ToSAMLResponder.
- Configure HTTP Destination:** The main configuration area on the right, containing the following fields:
 - Name:** ToSAMLResponder
 - Destination:** HTTP
 - URL:** https://resp.partner.com/SAMLResponder
 - Authentication:** BASIC
 - Basic Authentication:**
 - Username:** myuser
 - Password:** *****
 - Client Certificate Authentication:**
 - Keystore view:** service_ssl
 - Certificate:** ssl-credentials
 - Server Certificates:**
 - Ignore server certificates
 - Accept certificates in keystore view **service_ssl**
- Buttons:** "New", "Delete ...", and "Save" are located at the bottom of the configuration area.
- Status Bar:** Shows "Start service SAML" and a progress indicator at 100%.

Enter SAML Parameters – View in the configuration Tree



Enter SAML Parameters - Create a Sub-Configuration



Enter SAML Parameters - Inbound Parameters

The screenshot displays the SAP J2EE Engine Administrator interface. The title bar reads "SAP J2EE Engine Administrator - [J2E\Server 0 0_64129\Services\Configuration Adapter]". The menu bar includes "Connect", "View", "Tools", and "Help".

The left sidebar, titled "Global Configuration", lists various system components. The "Configuration Adapter" component is selected and highlighted in blue.

The main window is divided into several tabs: "Runtime", "Properties", and "Additional Info". Under the "Runtime" tab, there are sub-tabs: "Display configuration", "Open configurations", "Blocking locks", and "Display cache content".

The main content area shows a tree view of configurations. The path "Configurations > saml > Configuration > PartnersInbound > ParametersInbound" is expanded, showing the following parameters:

- Active=true
- DestinationName="ToSAMLResponder"
- ParameterNameTarget="TARGET"
- SourceID="Hex:1264439456D983C12A6AEC1DF9FAD2C5E0C3F4AF"

At the bottom left of the window, a green diamond icon is next to the text "Start service SAML". The bottom right corner shows a zoom level of "100%".

Enter SAML Parameters - General Parameters

The screenshot displays the SAP J2EE Engine Administrator interface. The title bar reads "SAP J2EE Engine Administrator - [J2E\Server 0 0_64129\Services\Configuration Adapter]". The menu bar includes "Connect", "View", "Tools", and "Help". Below the menu bar is a toolbar with various icons. The left pane shows a tree view under "Global Configuration" with "Cluster" expanded, listing various services. "Configuration Adapter" is selected. The right pane shows the "Runtime" tab with "Properties" selected. The "Display configuration" sub-tab is active, showing a tree view of configurations. The "saml" configuration is expanded, showing "Configuration" with "PartnersInbound", "PartnersOutbound", and "Settings". Under "Settings", two parameters are visible: "ParameterNameArtifact='SAMLart'" and "PermitInsecureConnections=false". At the bottom left, a green diamond icon indicates "Start service SAML". At the bottom right, a zoom level of "100%" is shown.

SAP J2EE Engine Administrator - [J2E\Server 0 0_64129\Services\Configuration Adapter]

Connect View Tools Help

Global Configuration

Cluster

- Application Locking
- Application Tracing
- Basic Administration
- ClassLoader Viewer
- Classpath Resolver
- Configuration Adapter
- Connector Container
- Deploy
- Destinations
- EJB Container
- File Transfer
- HTTP Provider
- IIOP Provider
- JCo RFC Provider
- JDBC Connector
- JMS Connector
- JMS Provider
- JMX Adapter
- JMX Notification
- JNDI Registry
- Java Mail Client
- Key Storage
- Licensing Adapter
- Locking Adapter
- Log Configurator
- LogViewer
- Memory Info
- Message Info
- P4 Provider
- Remote Object Contai
- Runtime Info Provider
- SAML
- SLD Data Supplier

Runtime Properties Additional Info

Display configuration Open configurations Blocking locks Display cache content

- Configurations
 - rfcengine_global
 - rfcengine_local
 - HttpHosts
 - Licensing
 - OpenSQL
 - P4_Persistent
 - P4_PersistentObject
 - UDDI_SERVER_USERSTORE
 - WebContainer
 - WebServicesAddOn
 - apps
 - cluster_data
 - deploy
 - failover
 - jms_provider
 - keystore
 - protected_domains
 - saml
 - Configuration
 - PartnersInbound
 - PartnersOutbound
 - Settings
 - ParameterNameArtifact="SAMLart"
 - PermitInsecureConnections=false
 - securestorage
 - security
 - userstore
 - webdynpro
 - webservices

Start service SAML

100%

Adjust Login Module Stack

The screenshot shows the SAP J2EE Engine Administrator interface. The main window is titled "SAP J2EE Engine Administrator - [J2E\Server 0 0_64129\Services\Security Provider]". The interface is divided into several panes:

- Global Configuration:** A tree view on the left showing various services. "Security Provider" is selected.
- Runtime Properties:** A central pane showing the configuration for the selected service. It includes tabs for "Policy Configurations", "User Management", "Login Sessions", "Protection Domains", and "Cryptography Providers". Under "Policy Configurations", the "Authentication" tab is active, showing a table of login modules.
- Authentication Template:** A dropdown menu set to "no".
- Login Modules Table:** A table with columns "Login Modules", "Flag", and "Options".

Login Modules	Flag	Options
SAMLoginModule	SUFFICIENT	{AcceptedAuthenticationMethods...
BasicPasswordLoginModule	SUFFICIENT	{}

At the bottom of the interface, there is a status bar with a green arrow and the text "Start service SAML".

Introduction and Motivation

SAML Concepts

SAP J2EE and SAML

Configuring SAML for the SAP J2EE Engine

Summary

SAML is a young evolving standard for transferring authentication and authorization information between security domains.

SAP J2EE Engine supports SAML at the moment in a limited fashion

SAML has strategic meaning for distributed business processes which use web services. Therefore it is also strategic for SAP.

- No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.
- Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.
- Microsoft®, WINDOWS®, NT®, EXCEL®, Word®, PowerPoint® and SQL Server® are registered trademarks of Microsoft Corporation.
- IBM®, DB2®, DB2 Universal Database, OS/2®, Parallel Sysplex®, MVS/ESA, AIX®, S/390®, AS/400®, OS/390®, OS/400®, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere®, Netfinity®, Tivoli®, Informix and Informix® Dynamic Server™ are trademarks of IBM Corporation in USA and/or other countries.
- ORACLE® is a registered trademark of ORACLE Corporation.
- UNIX®, X/Open®, OSF/1®, and Motif® are registered trademarks of the Open Group.
- Citrix®, the Citrix logo, ICA®, Program Neighborhood®, MetaFrame®, WinFrame®, VideoFrame®, MultiWin® and other Citrix product names referenced herein are trademarks of Citrix Systems, Inc.
- HTML, DHTML, XML, XHTML are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.
- JAVA® is a registered trademark of Sun Microsystems, Inc.
- JAVASCRIPT® is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.
- MarketSet and Enterprise Buyer are jointly owned trademarks of SAP AG and Commerce One.
- SAP, SAP Logo, R/2, R/3, mySAP, mySAP.com and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are trademarks of their respective companies.