SAML in the SAP J2EE Engine 6.40

Responsible: PM Product Security, security@sap.com

Agenda

Introduction and Motivation

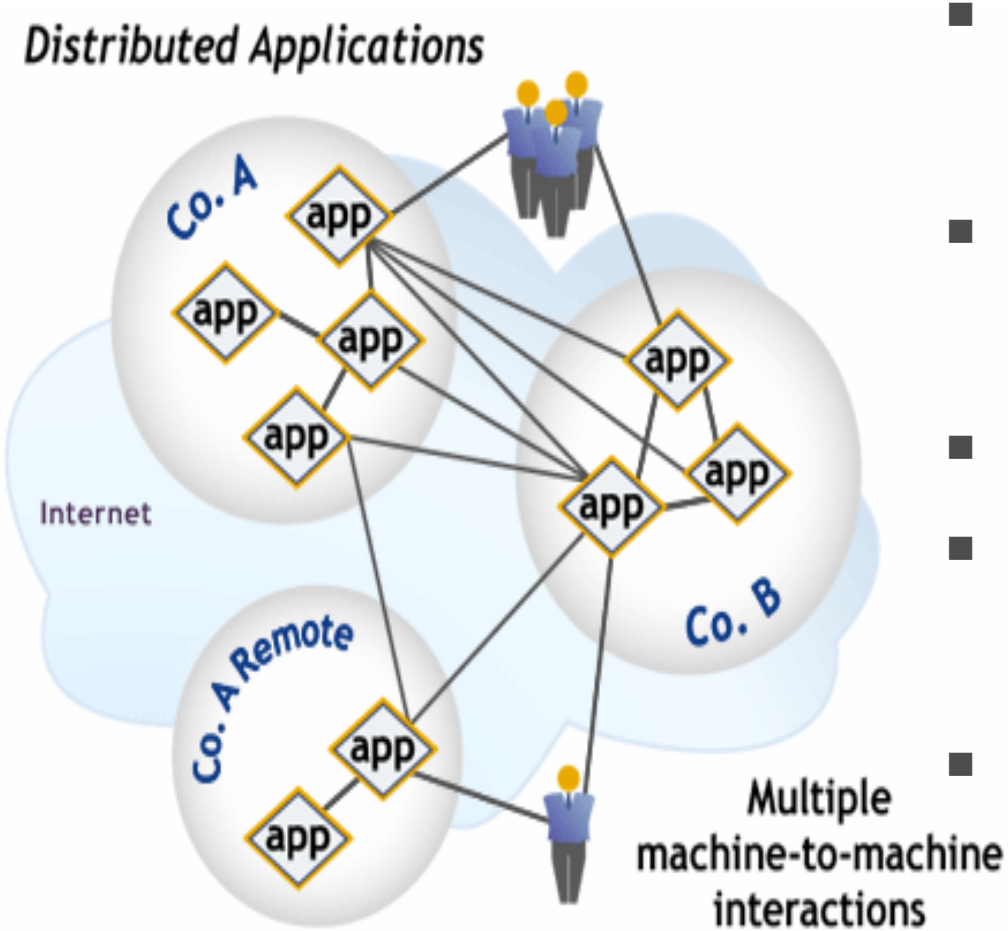
SAML Concepts

SAP J2EE and SAML

Configuring SAML for the SAP J2EE Engine

Summary

Security Requirements for Distributed Computing

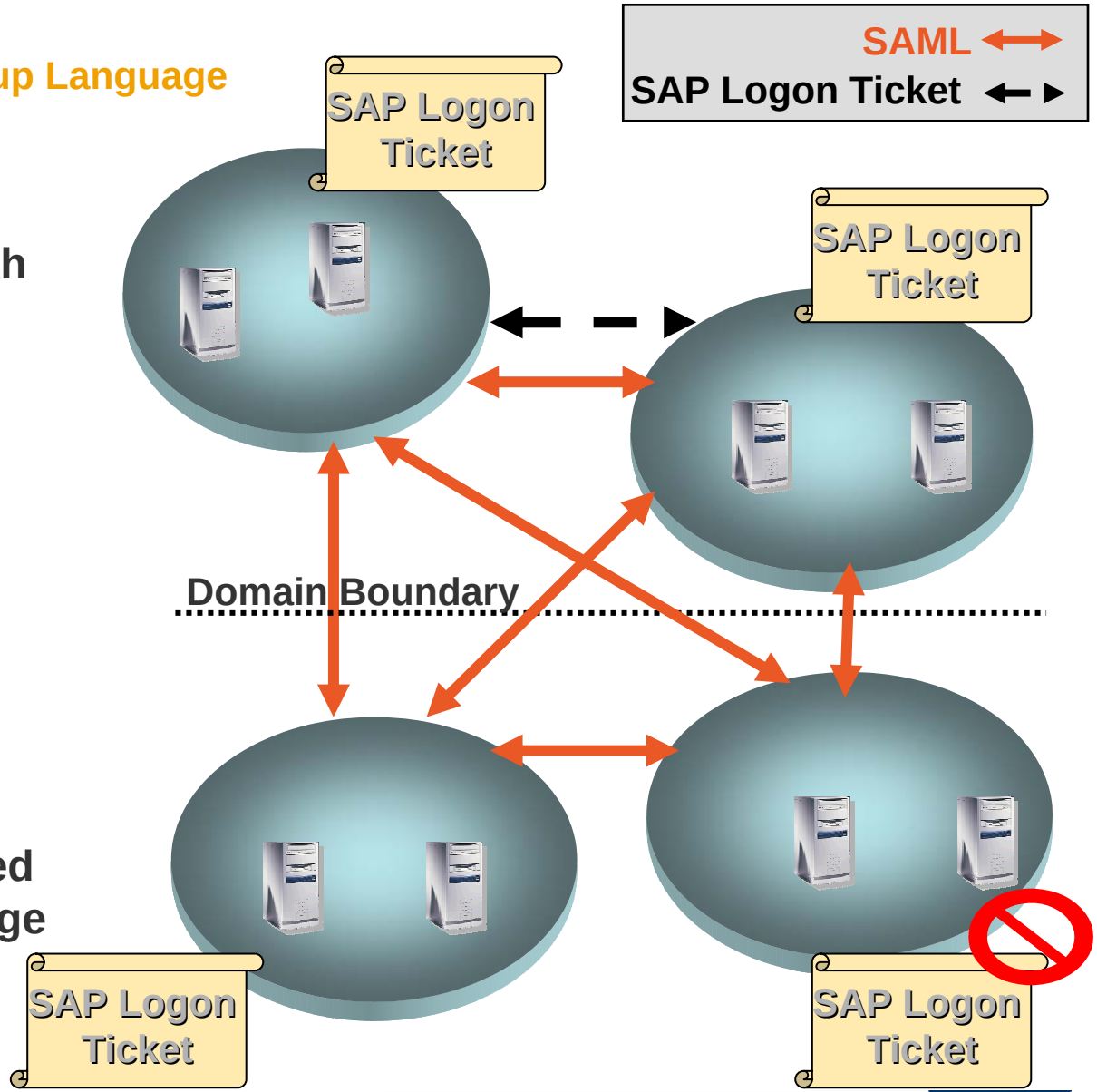


- Security in distributed applications, which span different companies, is crucial
- Current transport layer security protocols like SSL, TLS, IP Sec are not sufficient
- Application layer security is a must
- Security for Man-to-Machine and for Machine-to-Machine interaction is required
- Standard for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

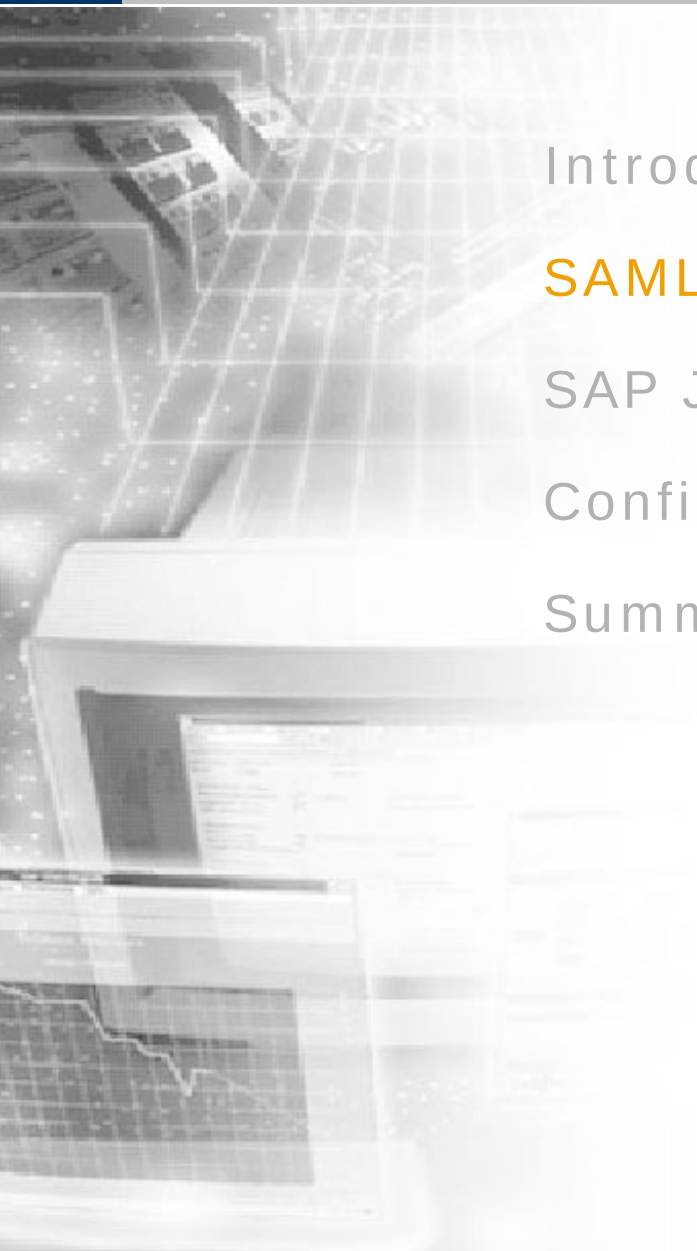
SAML Value Proposition

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)



Agenda



Introduction and Motivation

SAML Concepts

SAP J2EE and SAML

Configuring SAML for the SAP J2EE Engine

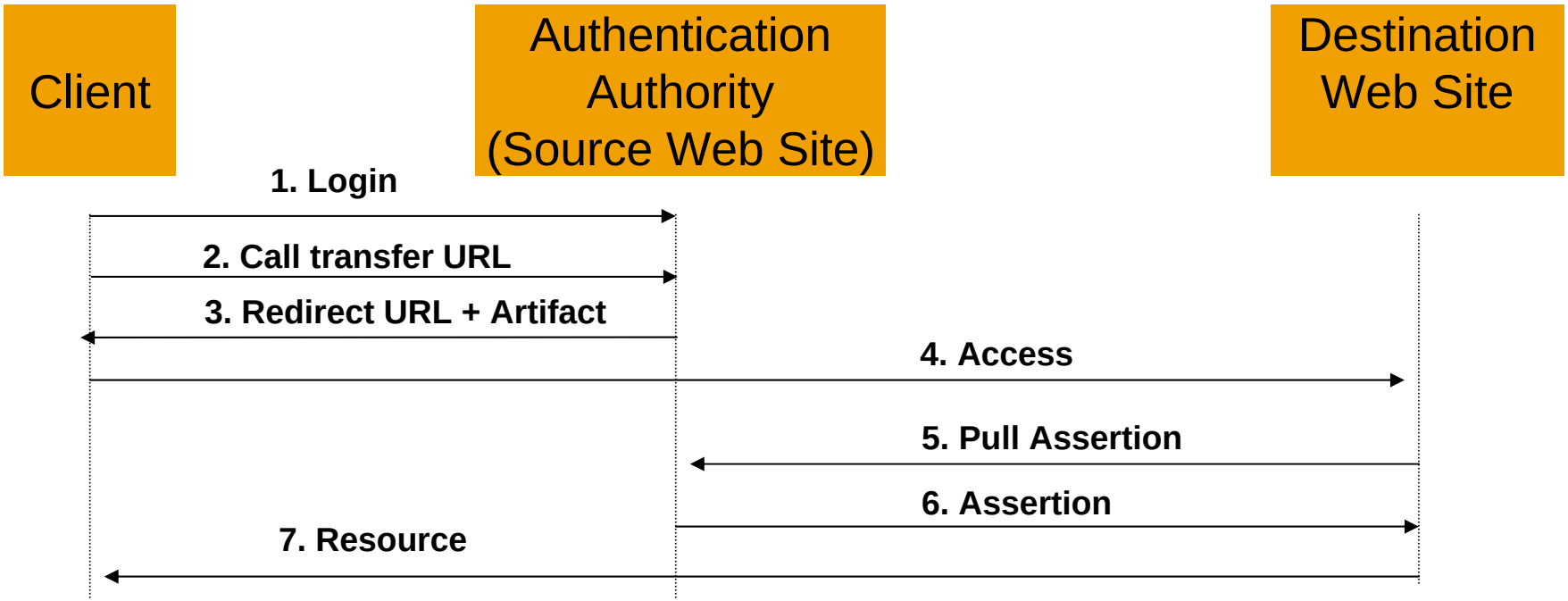
Summary

SAML Facts

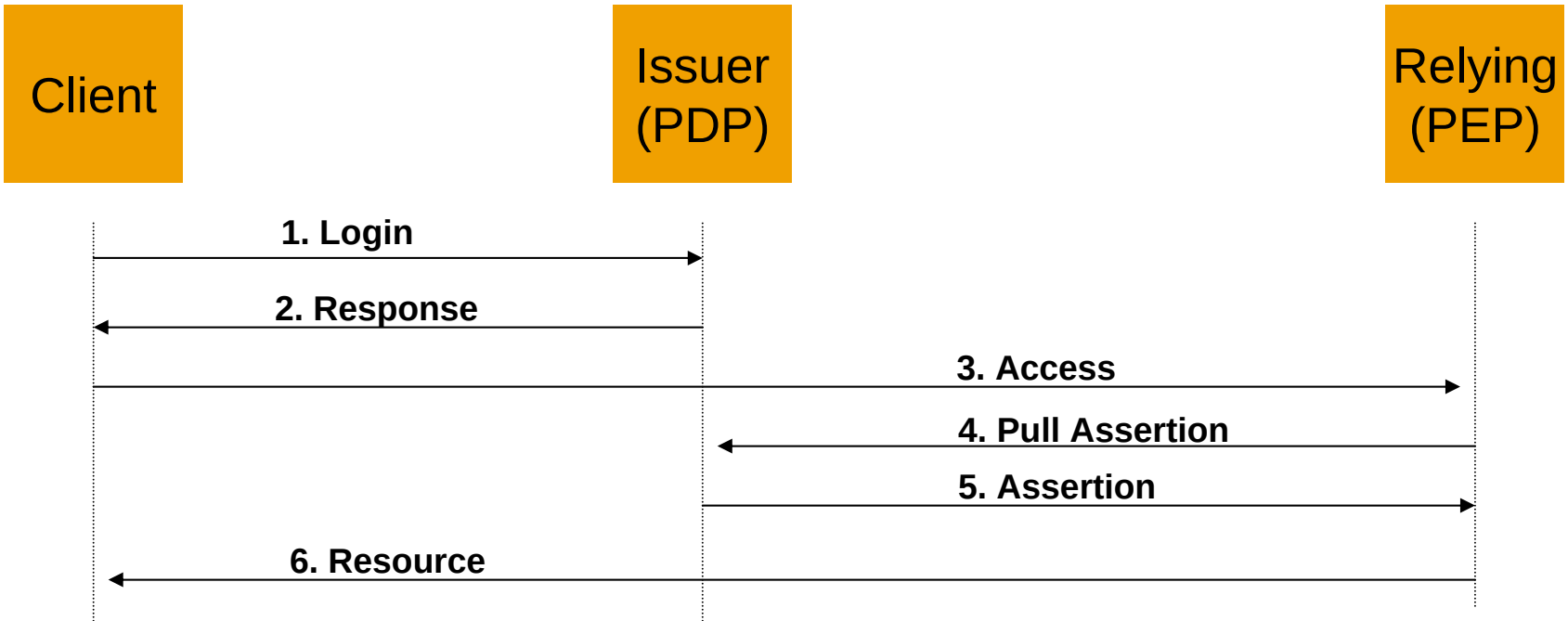
Facts about SAML:

- 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>
```

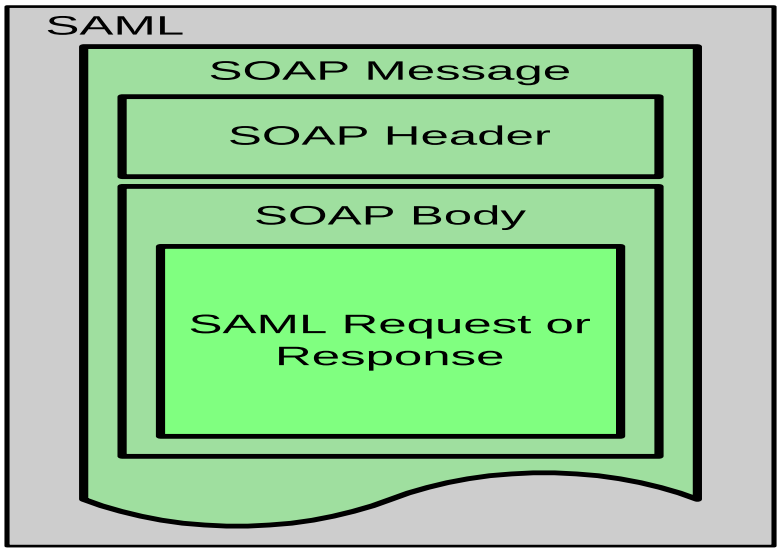
Authentication authorities SAML response with assertion:

```
<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>
```

Bindings

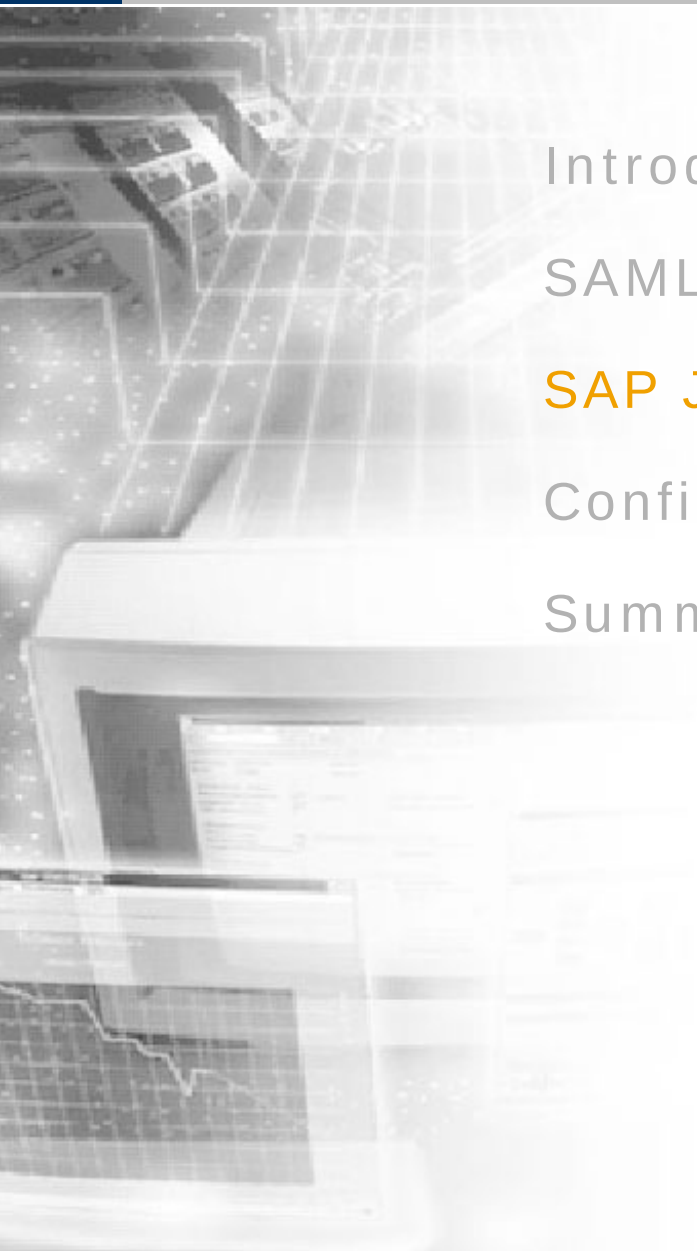
A binding is a way how to transport SAML requests and responses and therefore to secure the transfer. Possibilities are:

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



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

Agenda



Introduction and Motivation

SAML Concepts

SAP J2EE and SAML

Configuring SAML for the SAP J2EE Engine

Summary

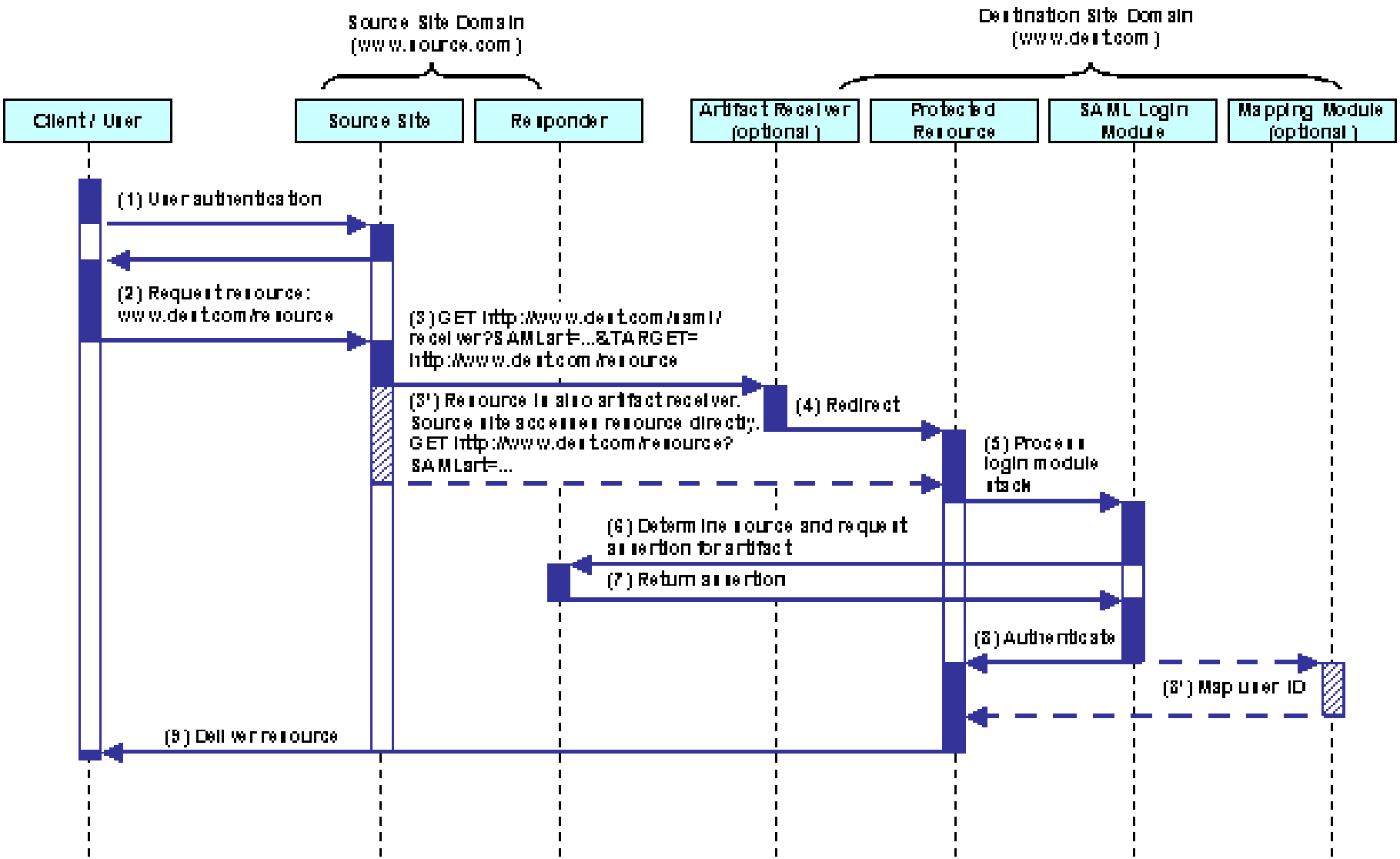
Support of SAML in the SAP J2EE Engine

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



Agenda

Introduction and Motivation

SAML Concepts

SAP J2EE and SAML

Configuring SAML for the SAP J2EE Engine

Summary

Configuration Steps

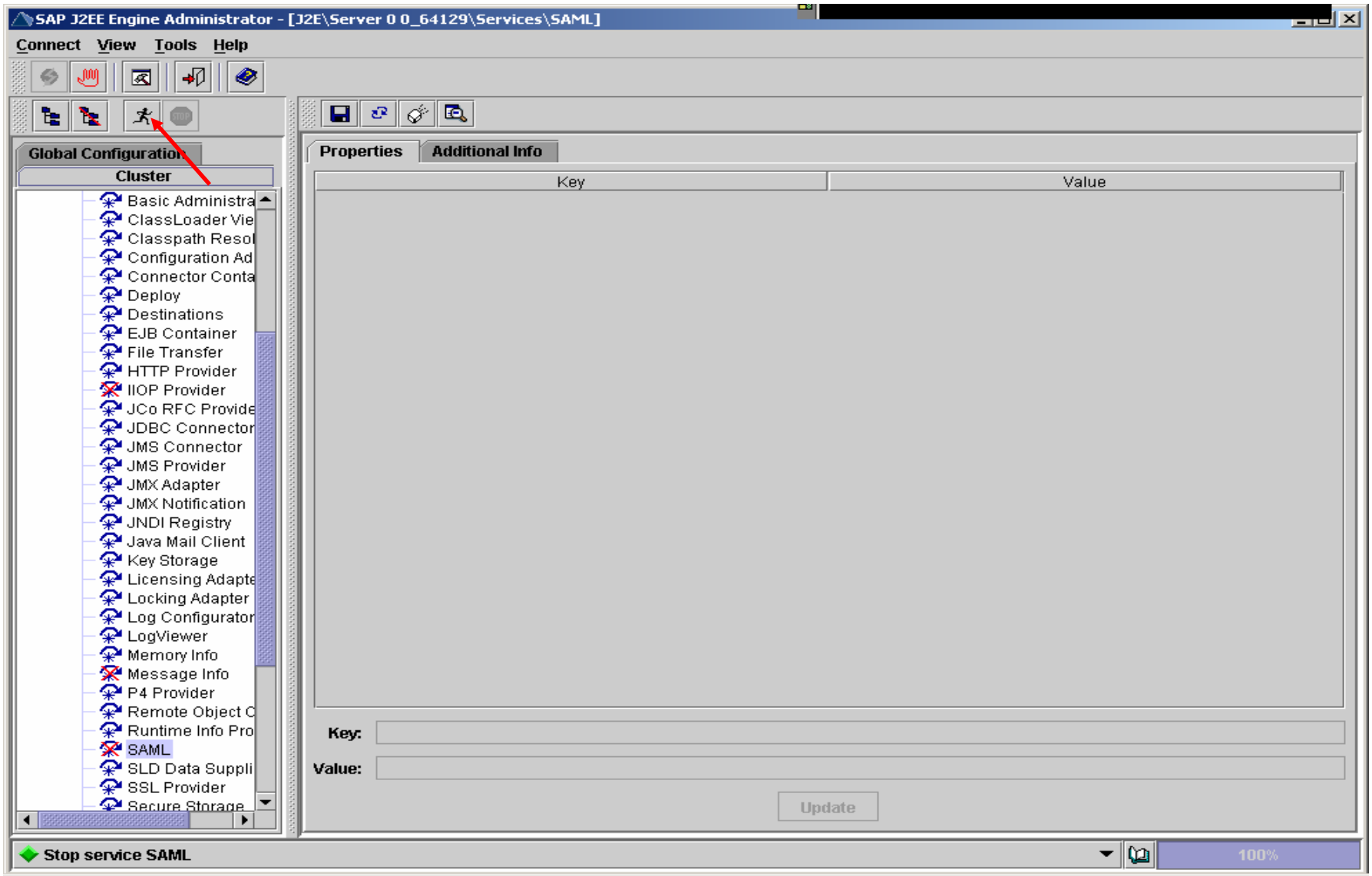
Prerequisites:

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

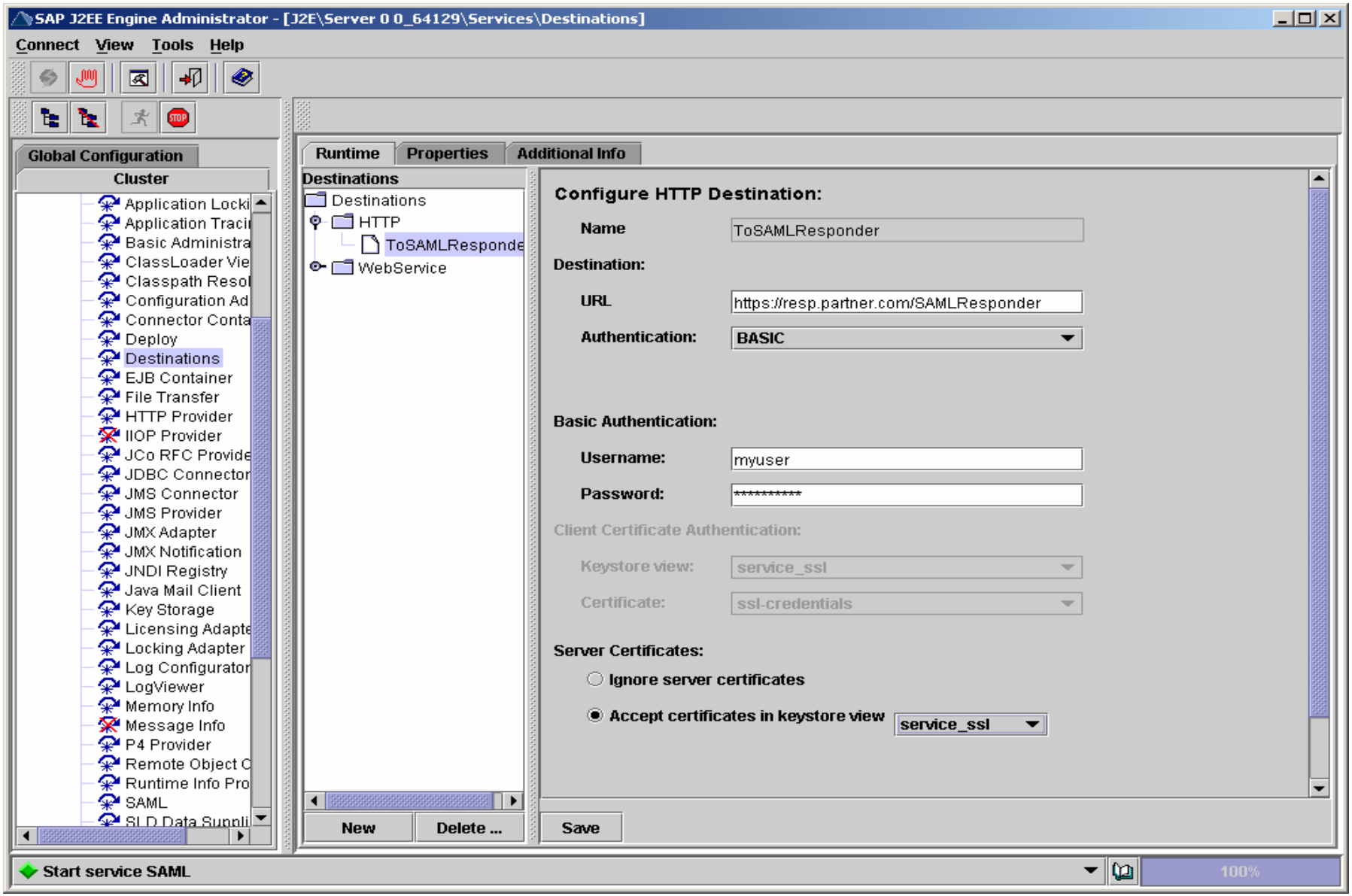
Steps for SAML configuration for the client SSO scenario in SAP J2EE Engine:

- **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**

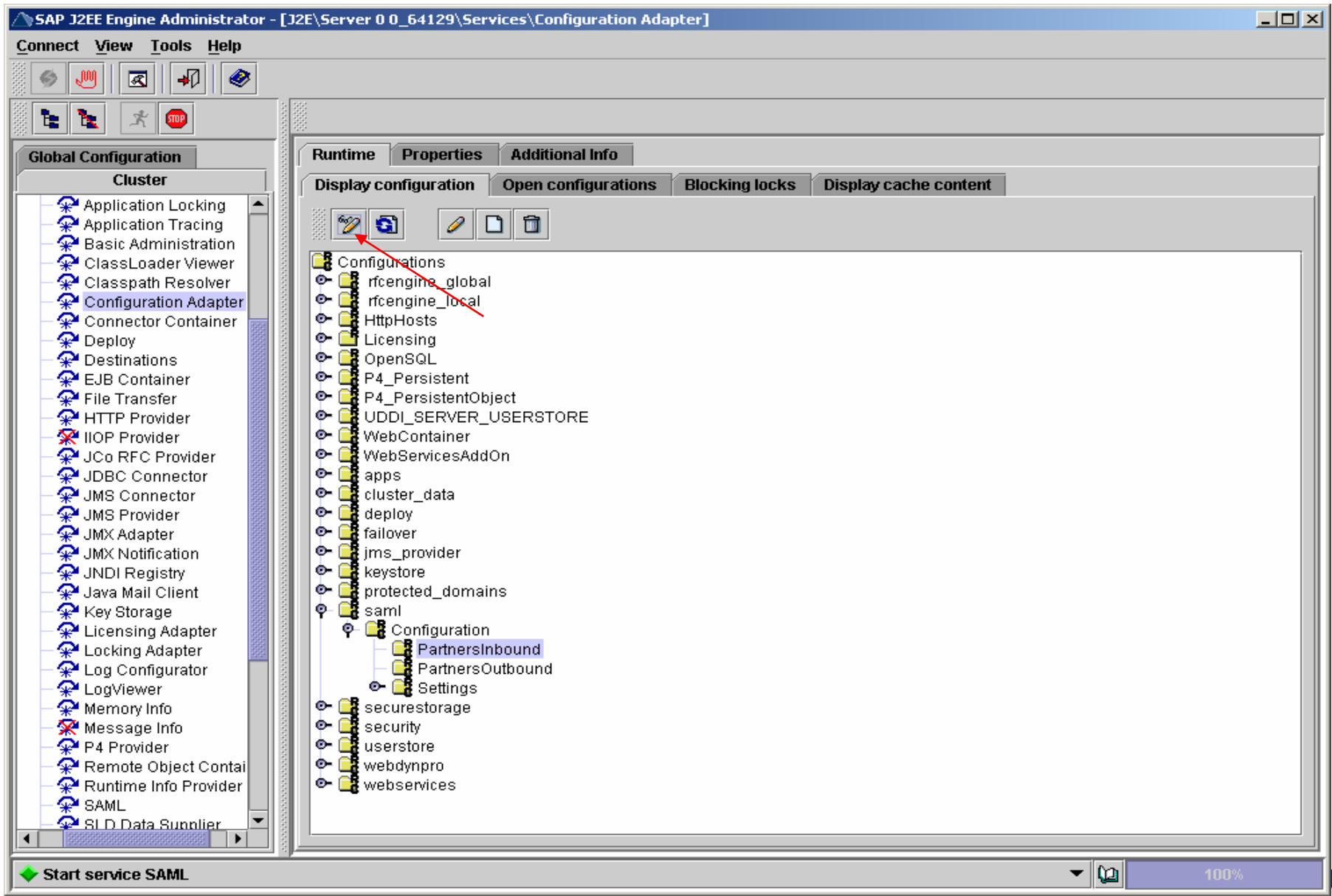
Start the SAML Service



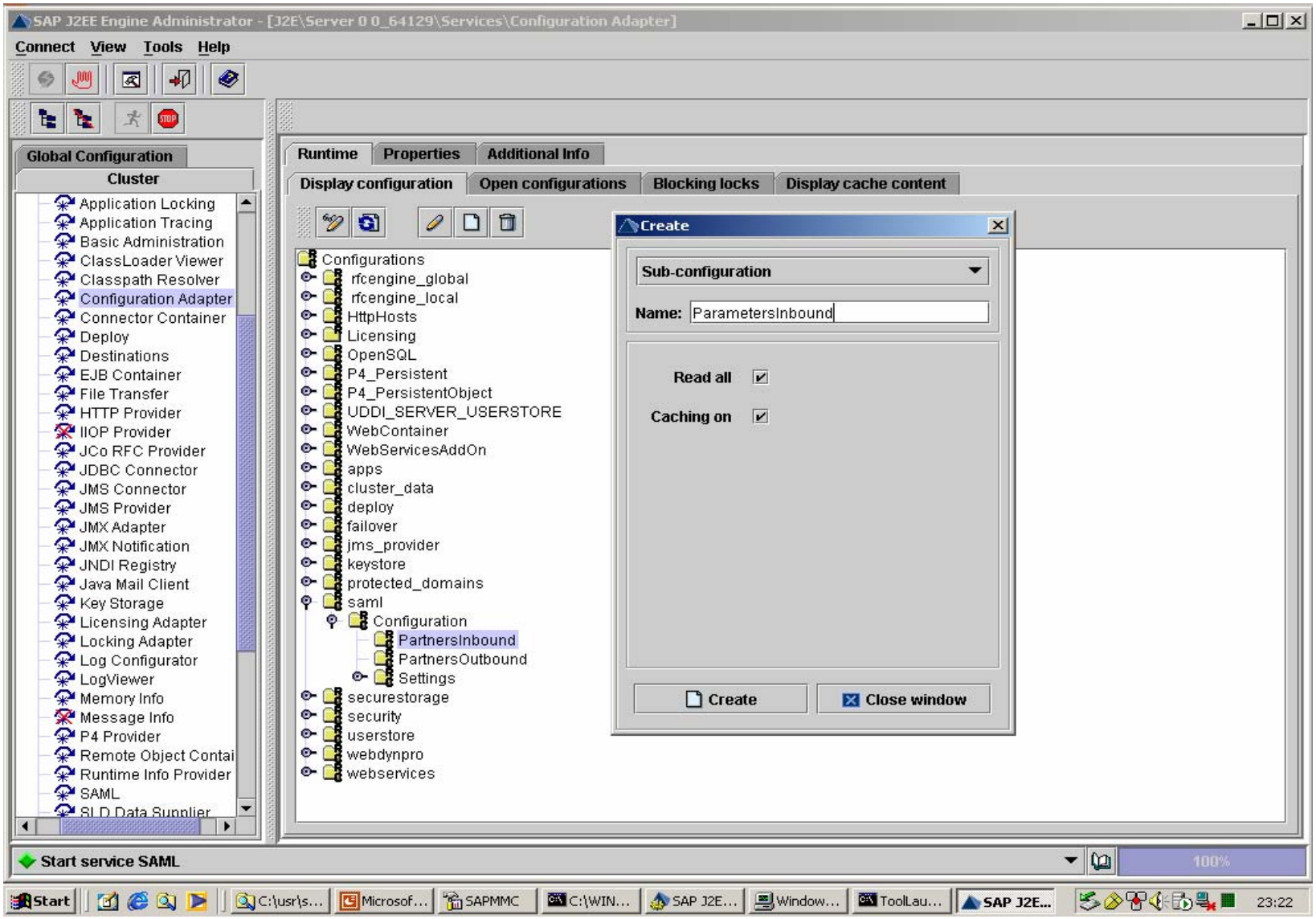
Create a Destination to the SAML Responder



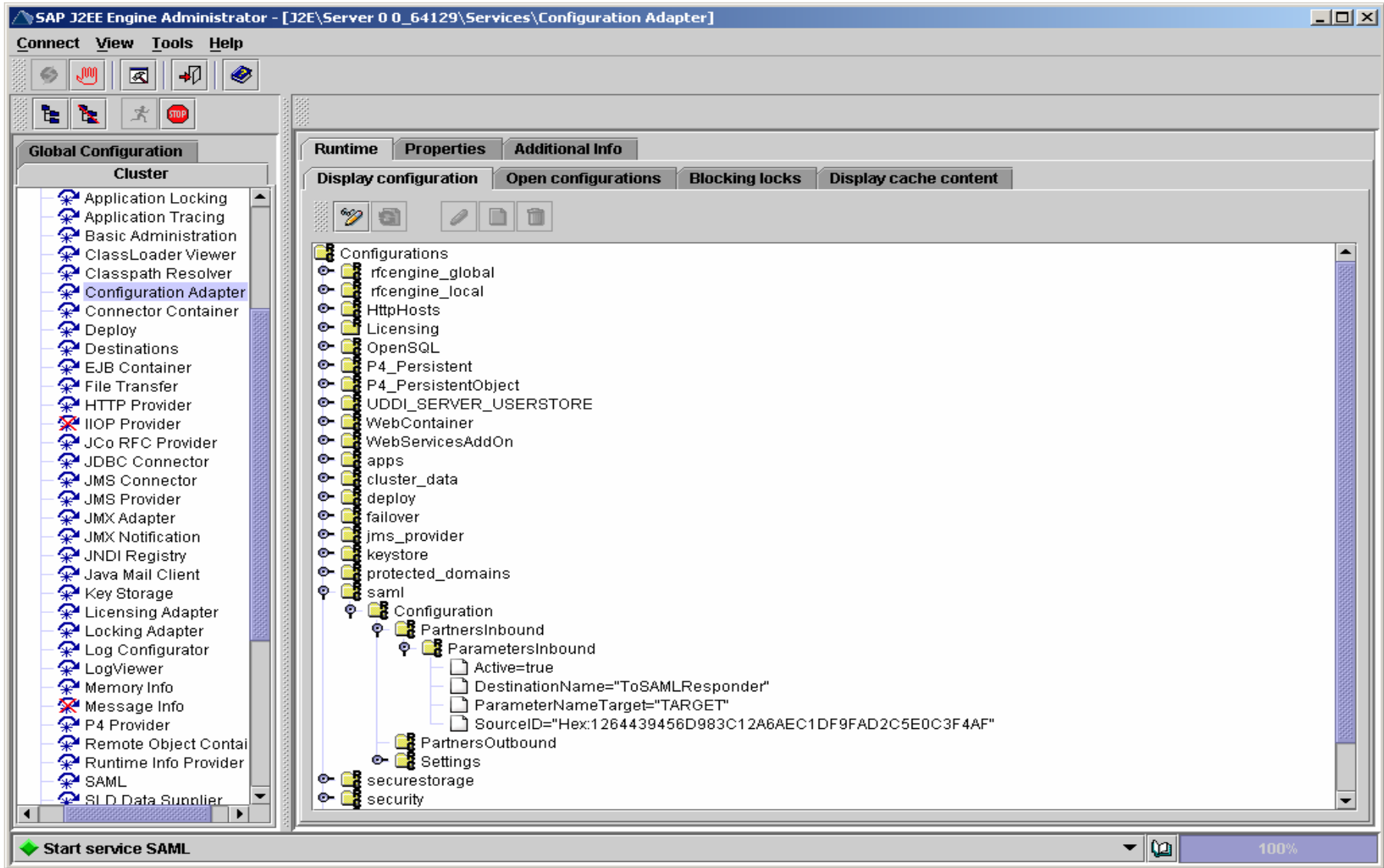
Enter SAML Parameters – View in the configuration Tree



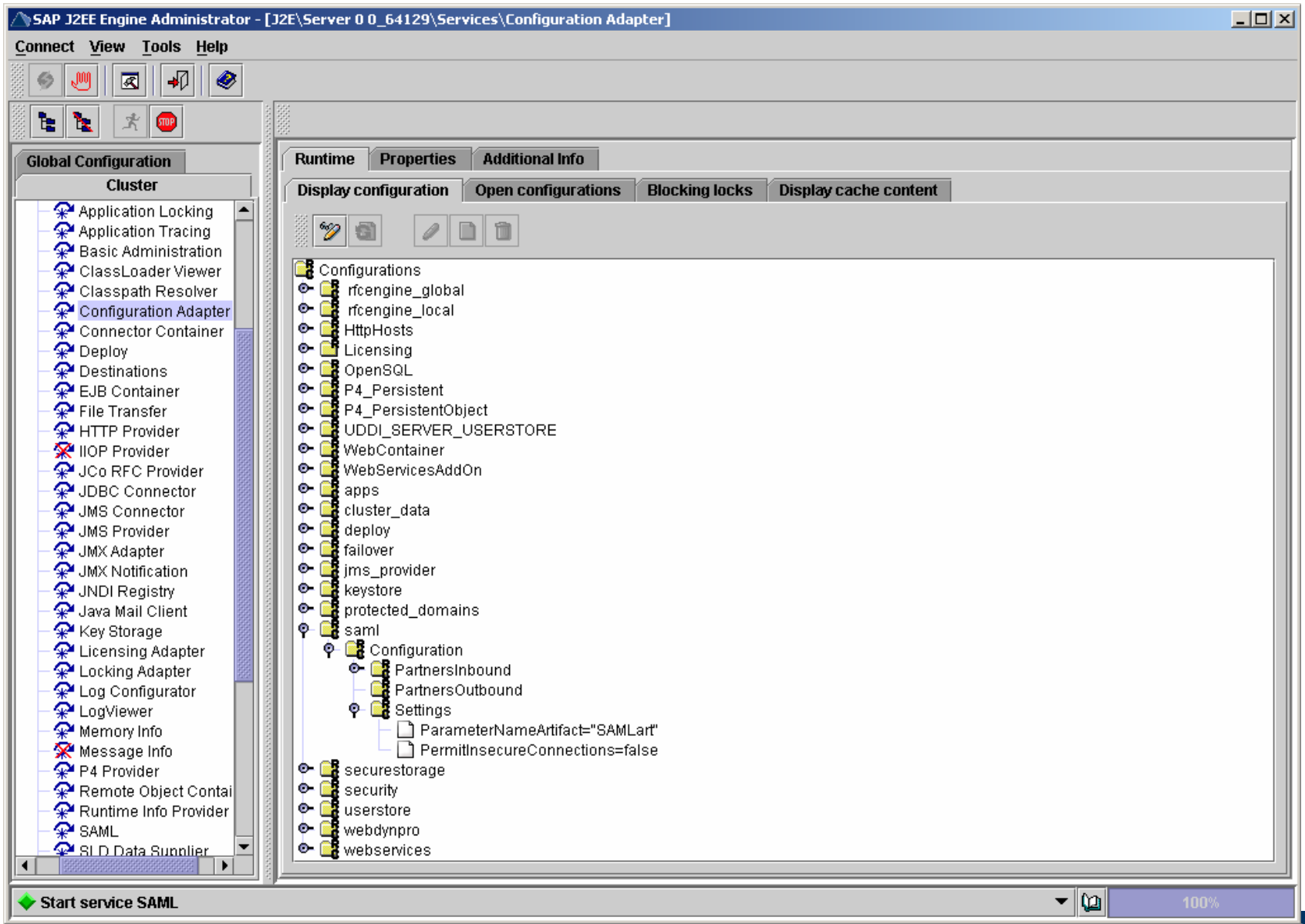
Enter SAML Parameters – Create a Sub-Configuration



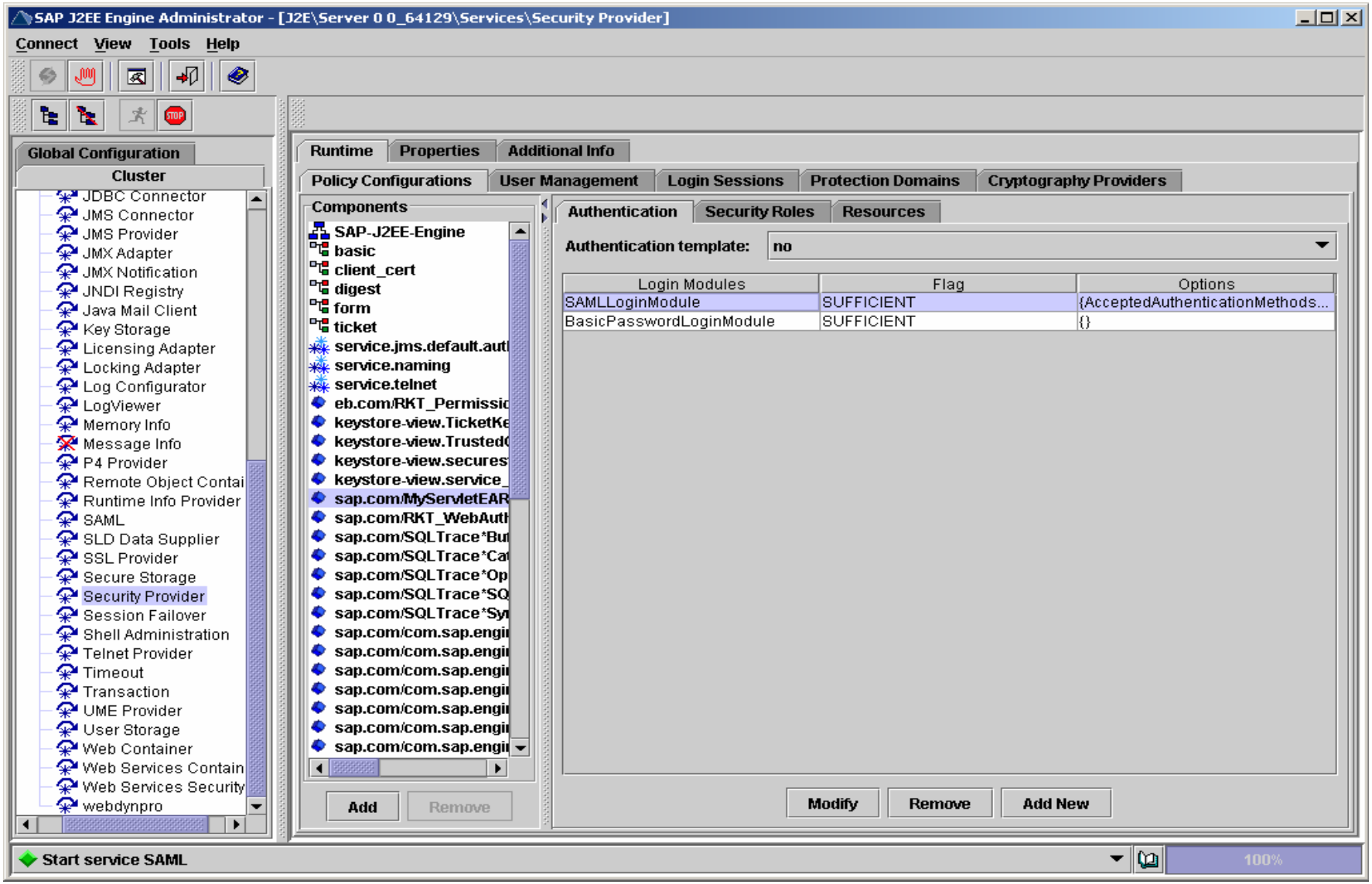
Enter SAML Parameters – Inbound Parameters



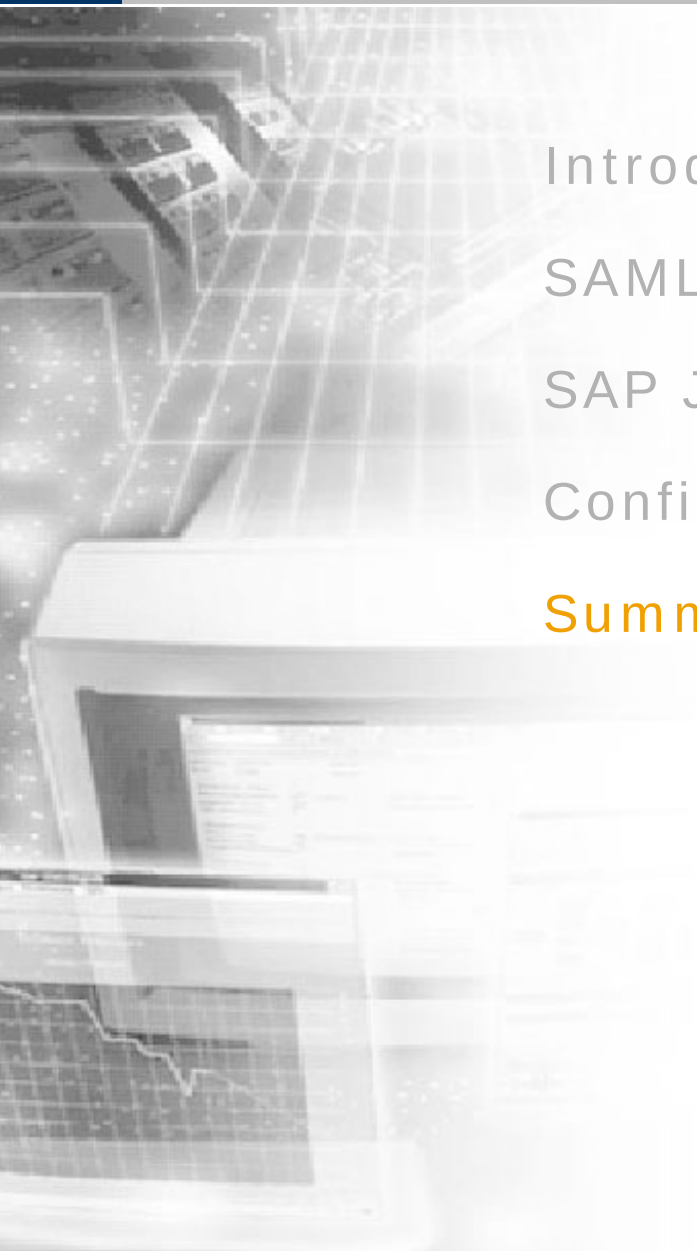
Enter SAML Parameters – General Parameters



Adjust Login Module Stack



Agenda



Introduction and Motivation

SAML Concepts

SAP J2EE and SAML

Configuring SAML for the SAP J2EE Engine

Summary

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.

Copyright 2004 SAP AG. All Rights Reserved