SAML SSO Configuration on AS Java

Applies to:

SAP NetWeaver stack and SAP AS Java in specific.

For more information, visit the Identity and Access Management homepage.

Summary

This article provides the configuration steps in Visual Admin while configuring SAML (Security Assertion Markup Language) for SSO (Single-Sign-On) on SAP AS Java. This is a scenario where SSO is required from an external system to SAP AS Java. The basic SAML steps in this article have been referred from the article "Configuring Single Sign-On for SAP NetWeaver Application Server Java with IBM Tivoli Federated Identity Manager using SAML 1.0" by the author Peter Tuton. I would like to thank the author for the well written article. The main purpose of this article is to demonstrate the screen shots of Visual Admin involved in the SAML configuration.

Author: Suresh Santhana

Company: Infosys Technologies Ltd.

Created on: 17 August 2009

Author Bio

Suresh Santhana is working with Infosys Technologies Ltd as a Technical Architect in the Enterprise Portal domain. His area of expertise includes PDK, portal configurations like SSO to SAP and non-SAP applications, XML and related web technologies.

Table of Contents

Background

SAP NetWeaver Application Server Java (AS-Java) provides for the ability to use the SAML protocol to sign on to its applications (for example, SAP NetWeaver Portal).

Security Assertion Markup Language (SAML) is a standard produced by the Security Services Technical Committee (SSTC) within the Oasis Standards Organization. SAML consists of two distinct pieces of functionality: The SAML assertion (used to transfer information about a user) and the SAML protocol (the means of exchanging a SAML assertion).

SAML provides for:

- Browser/POST profile
- Browser/Artifact profile

With a Browser/Artifact profile, a pointer to the SAML assertion (called an artifact) is included in the query string of an HTTP 302 redirect to the service provider. The service provider in turn issues a direct SOAP/HTTP request back to the identity provider, exchanging the artifact for the actual SAML assertion. Currently SAP AS-Java supports the Browser/Artifact profile.

The screen shots provided in this article does not show the actual parameter values. Please note that this article does not provide the steps involved in Identity Provider configuration on the External System. The steps highlighted in yellow have dependency on the external system.

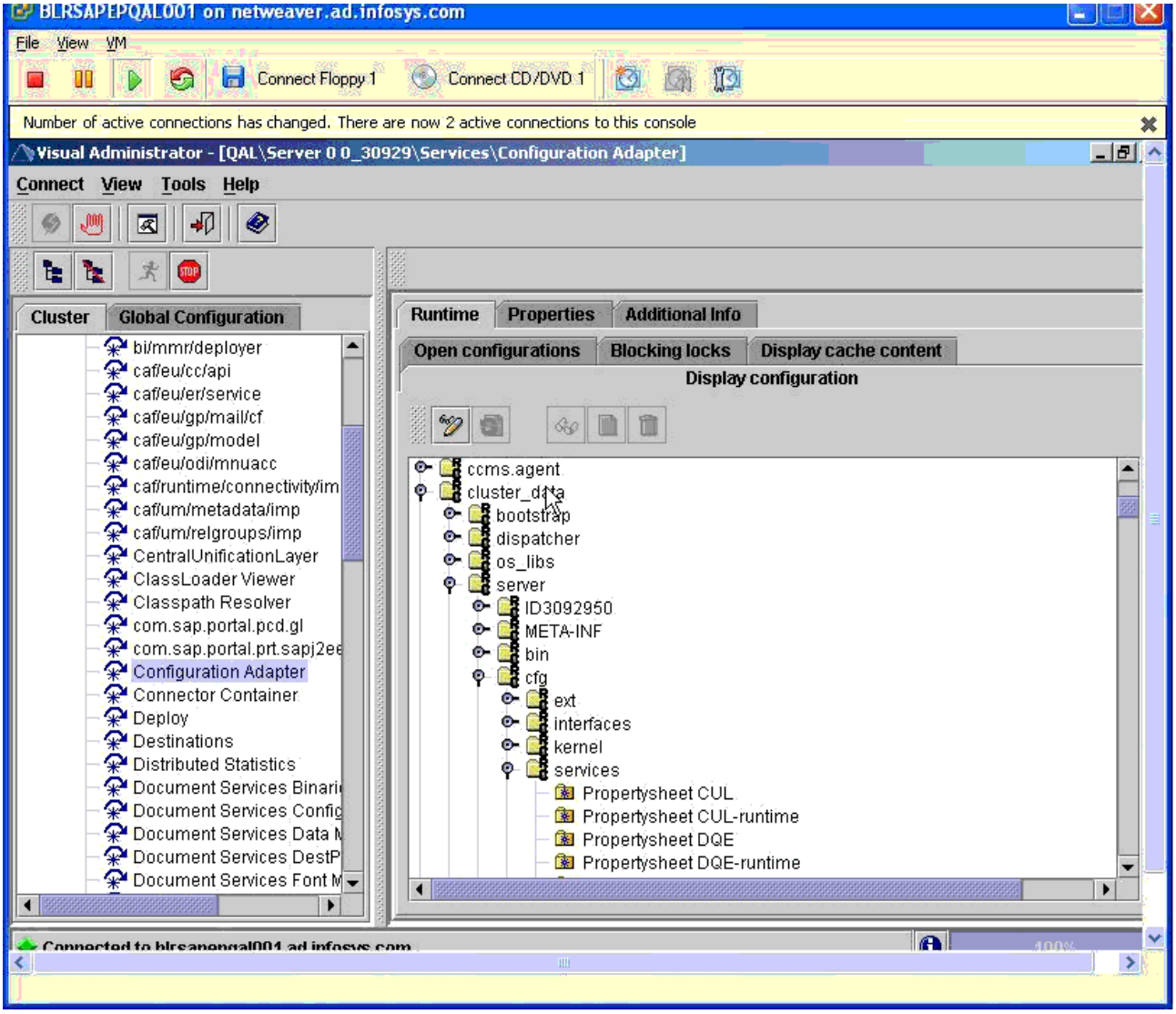
Step 1: Configuring SAP AS-Java

This section covers the steps required to configure SAP AS-Java to support SAML assertions.

Step 1: Changing the Startup Mode for the SAML Service

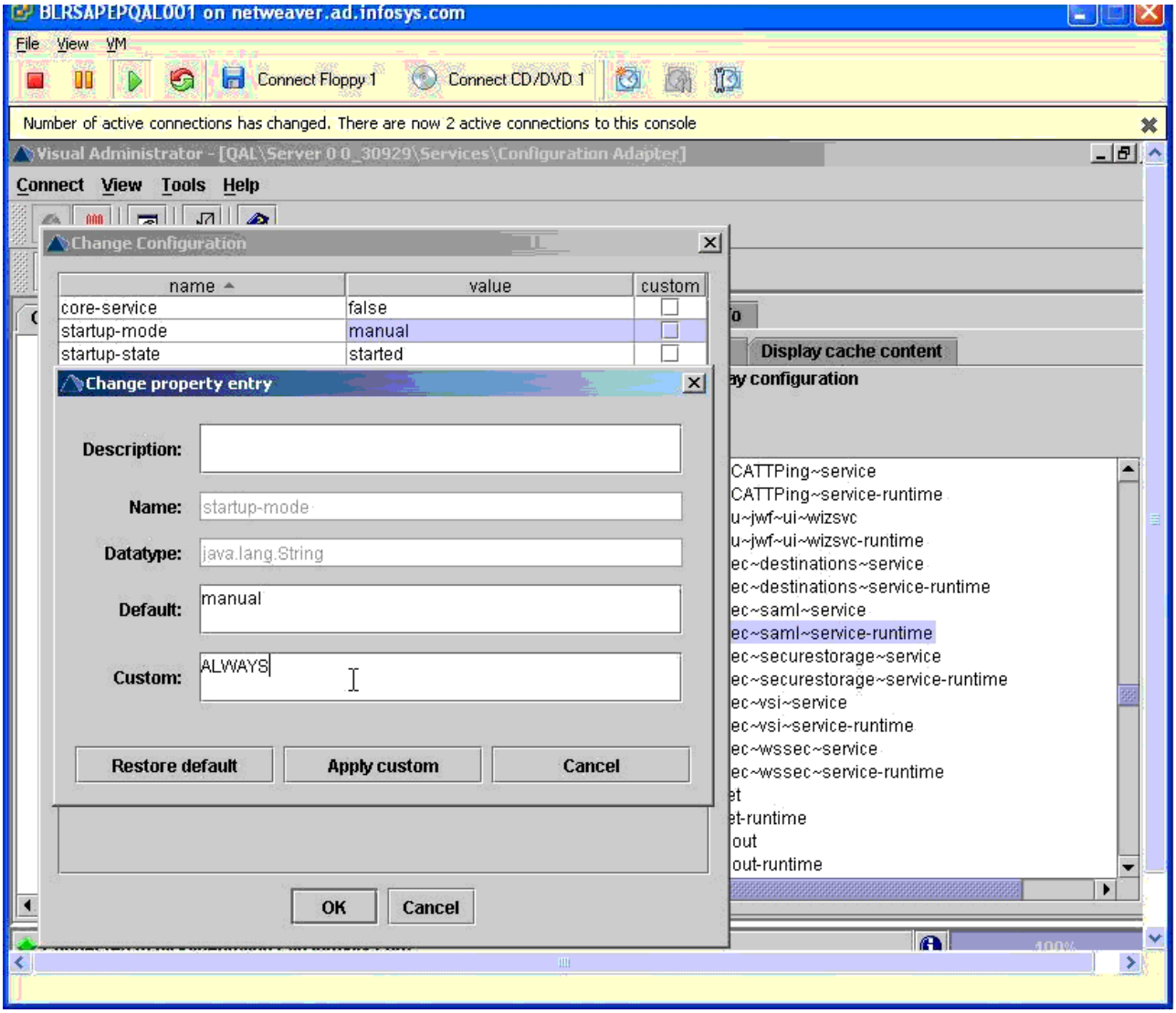
Perform the following steps using the **Configuration Adapter** in the **Visual Administrator** to change the startup mode for the SAP SAML Service.

1. Select Server > Services > Configuration Adapter.
2. Expand Configurations - cluster_data - server - cfg - services.



3. Switch to edit mode. Click **Yes**.
4. Select **Propertysheet tc~sec~saml~service-runtime** and click the pencil representing **Show the details of the selected node**. The *Change Configuration* page appears.
5. Select **start-up mode**. The *Change property* entry page appears.

6. In the **Custom** field, enter the value `always` and click **Apply custom**. You return to the *Change Configuration* page.

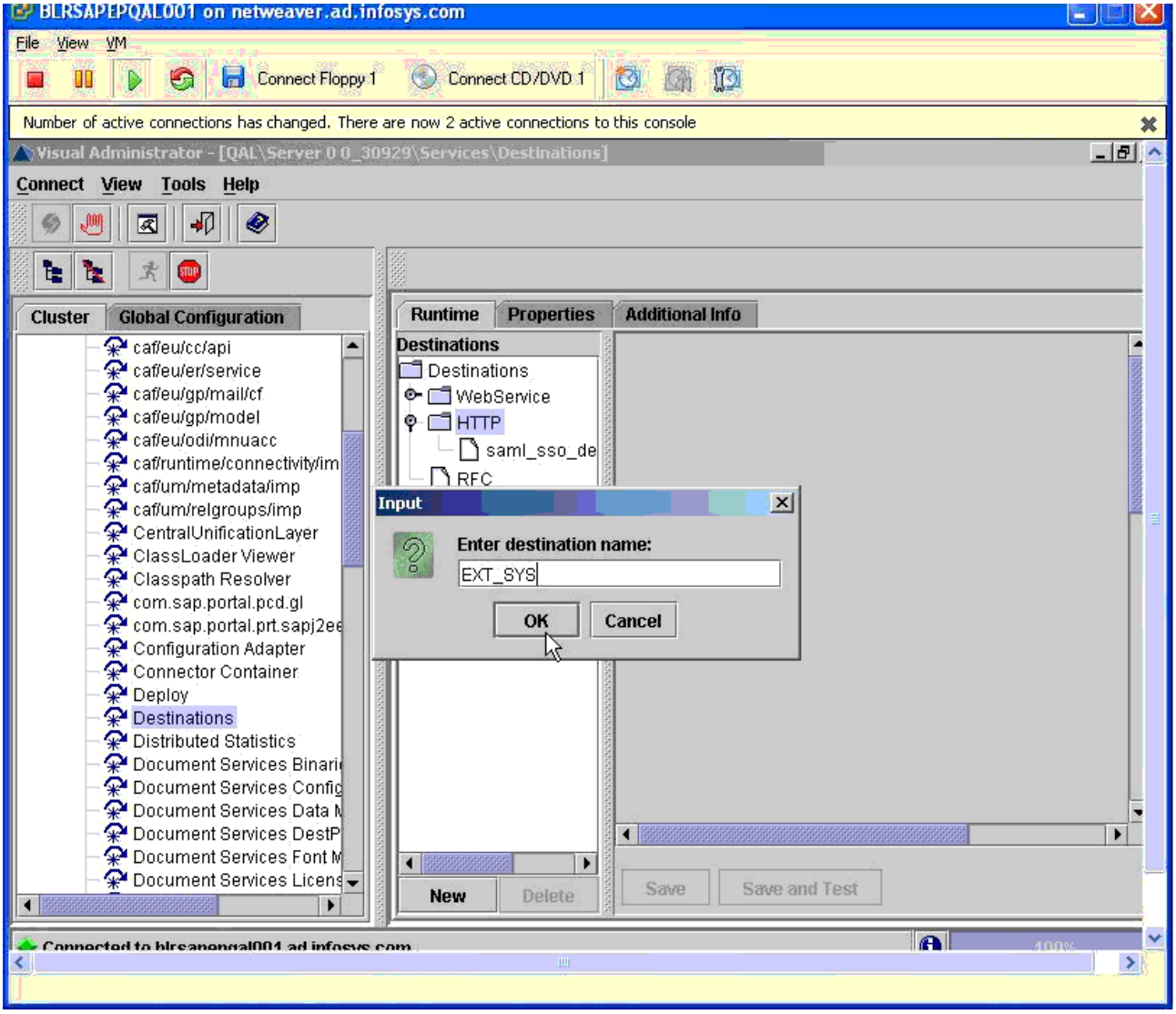


7. Click **OK**.
8. Restart the J2EE™ Engine server process.

Step 2: Creating a Destination

Perform the following steps using **Destinations** in the **Visual Administrator** to create a new destination. The destination defines the parameters in order to connect the external system (Identity Provider).

1. Expand Destinations - HTTP.
2. Click New and enter a name for the new destination, for example, EXTSYS.

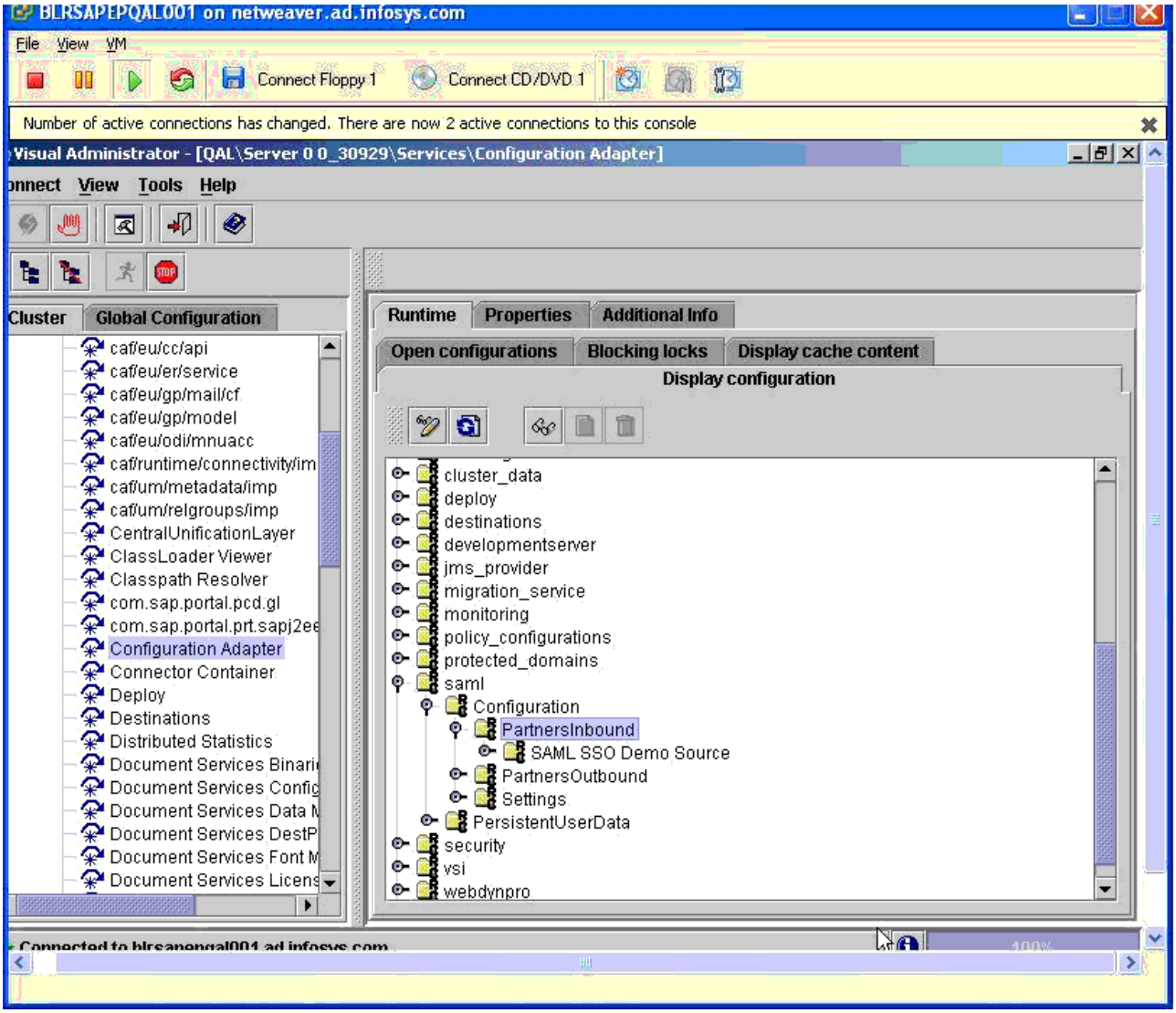


3. Click OK.
4. Enter the URL of the external system (Identity Provider) SOAP Endpoint.
   For example the URL can be something like, `http://ExtSys.abc.com/EXT/xyz/SAP_AS-Java/saml/soap`.
5. Select the appropriate Authentication mechanism such as `BASIC` authentication.
6. Click Save.

Step 3: Configuring the SAML Parameters

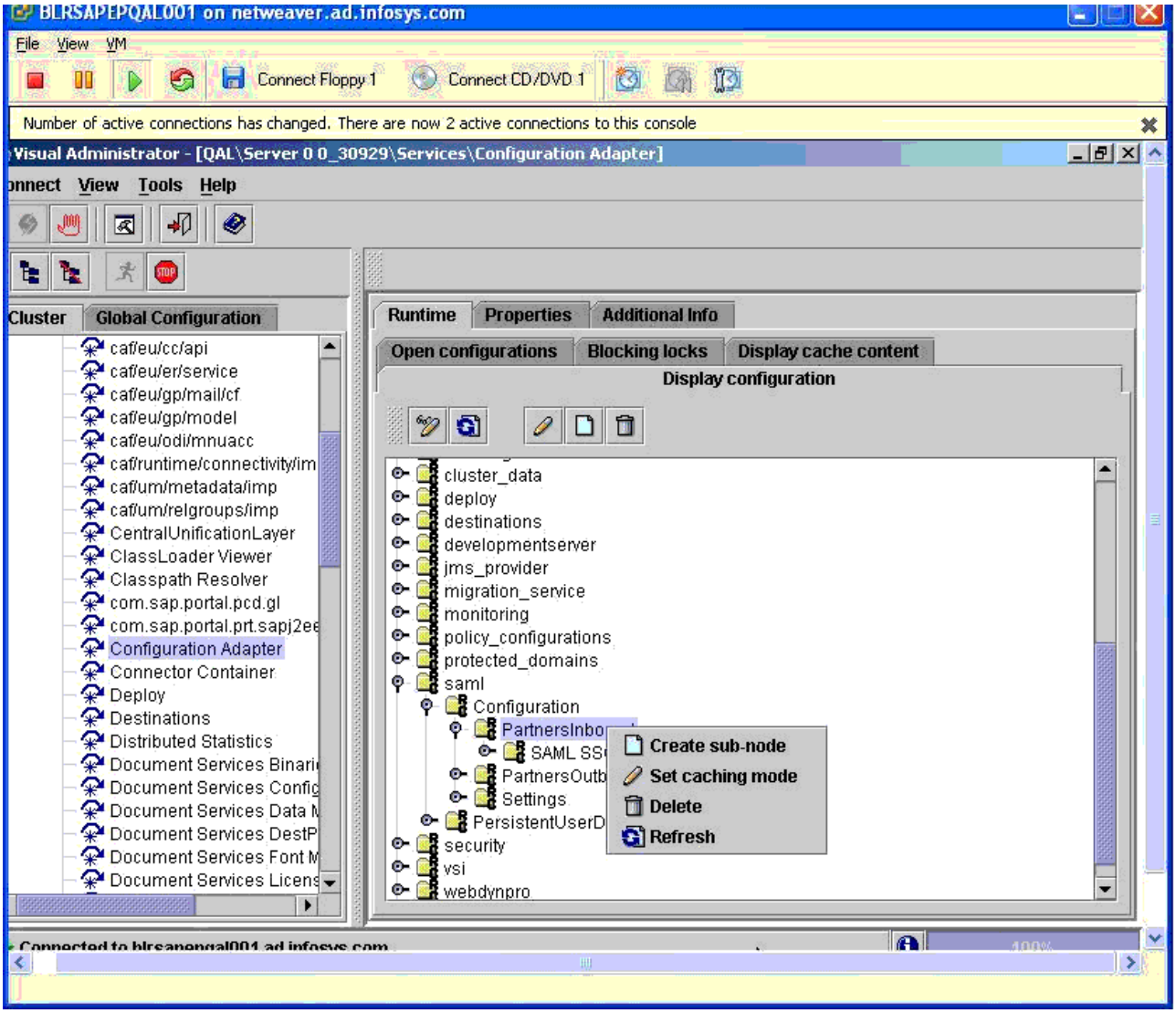
Perform the following steps using the **Configuration Adapter** in the **Visual Administrator** to change the SAML parameters.

1. Expand Configurations > SAML > Configuration.



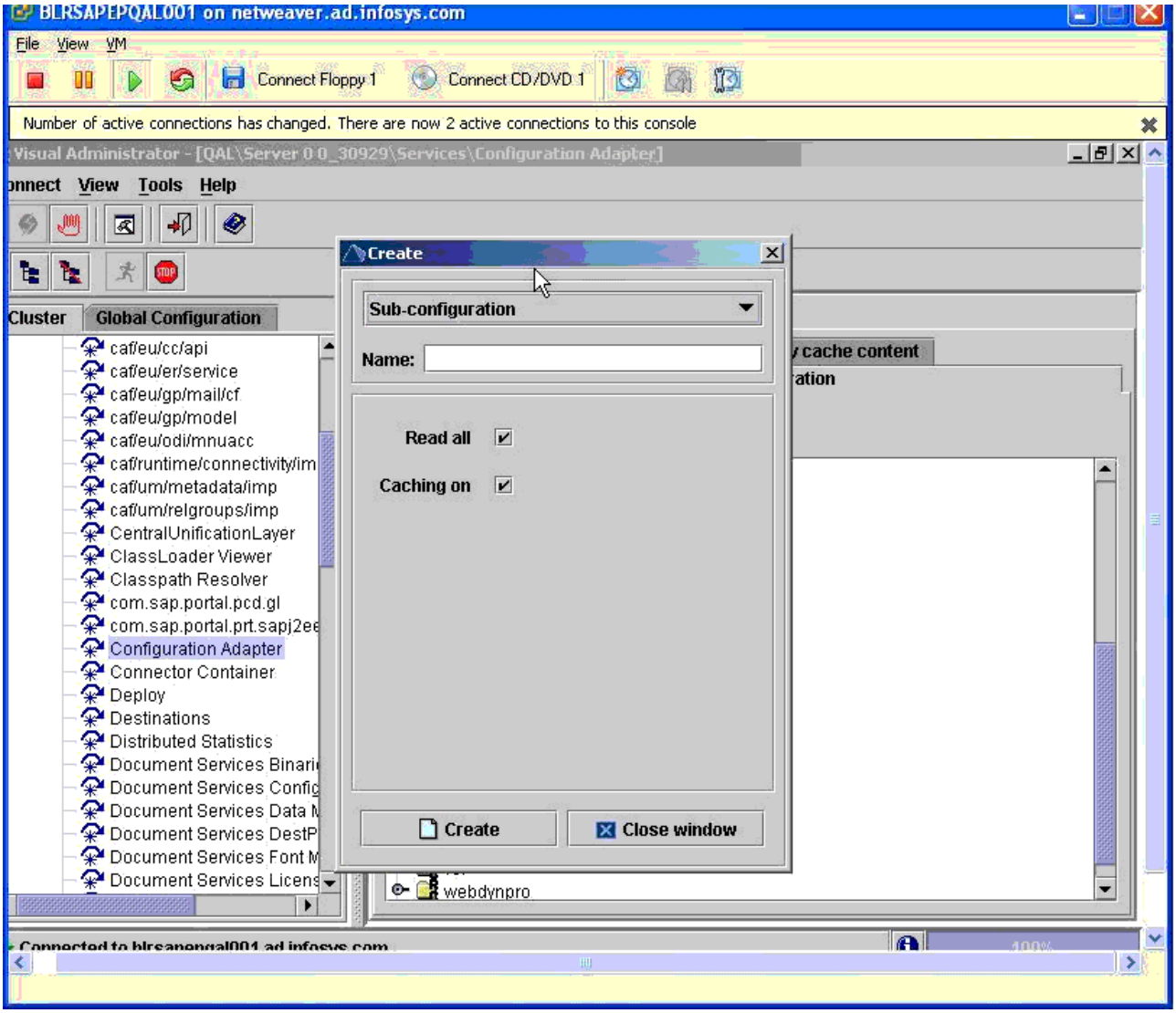
2. Switch to Edit mode. Click Yes.

3. Select PartnersInbound and click Create a node below the selected node. The Create page appears.



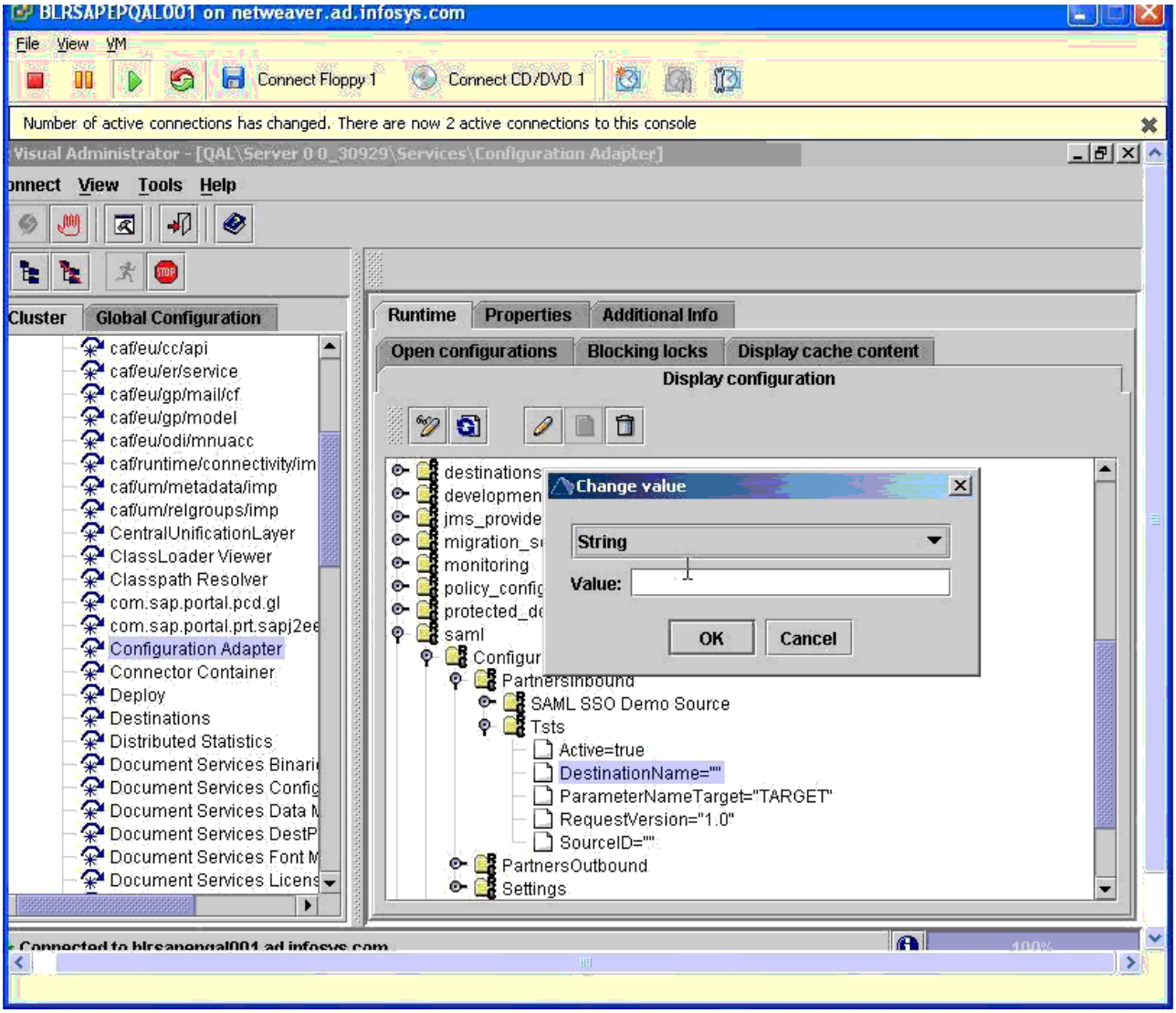
4. Enter a Name for the partner, for example, EXTSYS.

5. Click Create. A new node is created.



6. Expand the new node.

7. Double-click DestinationName. Enter the name of the destination created in the previous step.



8. Double-click SourceID. Enter the value of the External System (Identity Provider) Source ID prefixed with B64: or Hex:.

   Use the prefix Hex: or B64: to specify the format of the source ID as follows:

   - Hex: Specify the source ID as a 40 character sequence in hexadecimal form.
   - B64: Specify the source ID as a base 64- encoded string (28 character sequence that ends with an equal sign (=)).

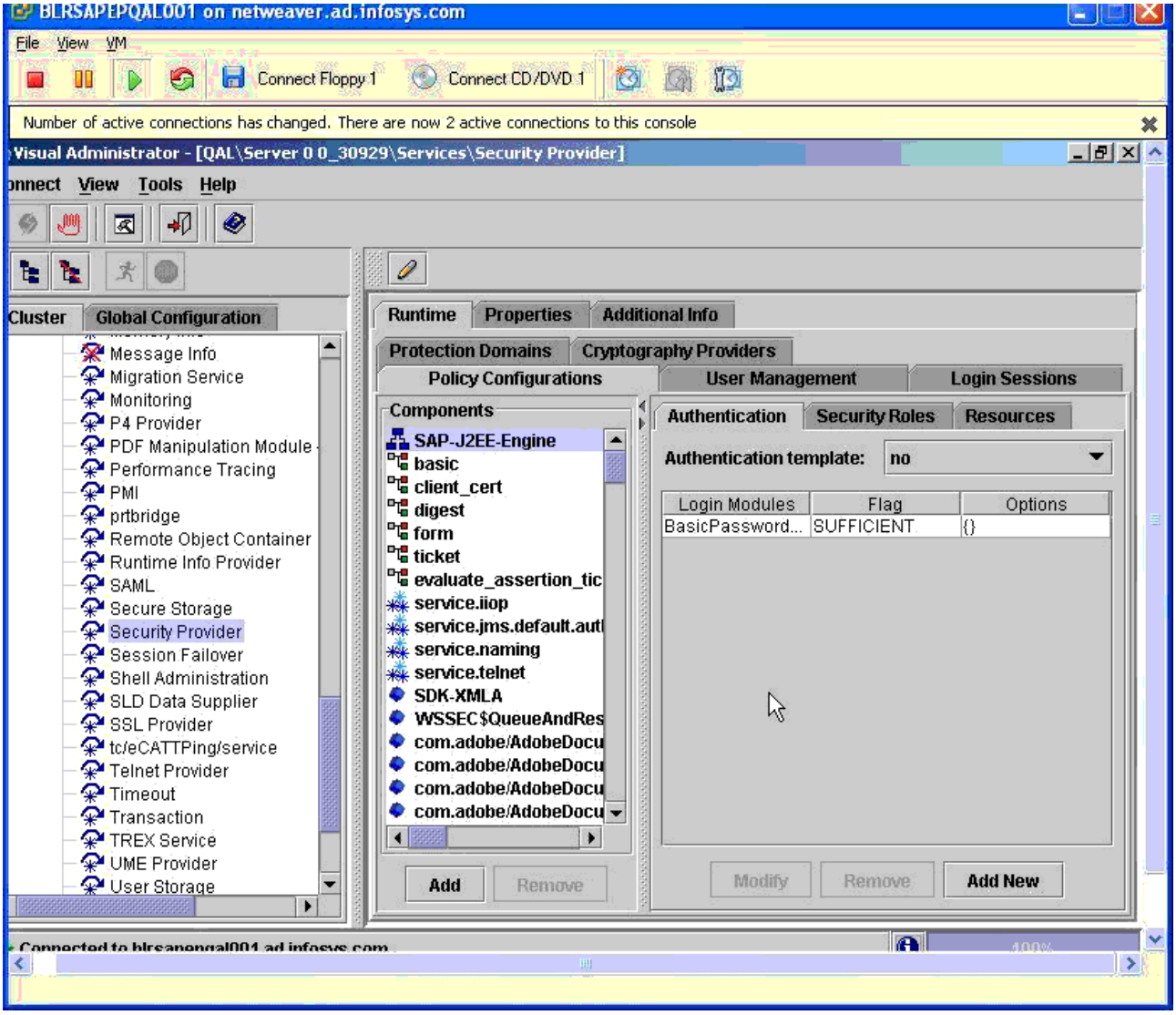
   This is the Source ID that is noted when configuring the identity provider on the external system.

9. For testing purposes, the **PermitInsecureConnections** parameter, located under **Configurations > SAML > Configuration - Settings** can be set to ‘true’. In a production environment, this value should be set to ‘false’.

Step 4: Adjusting the Login Module Stack for Using SAML

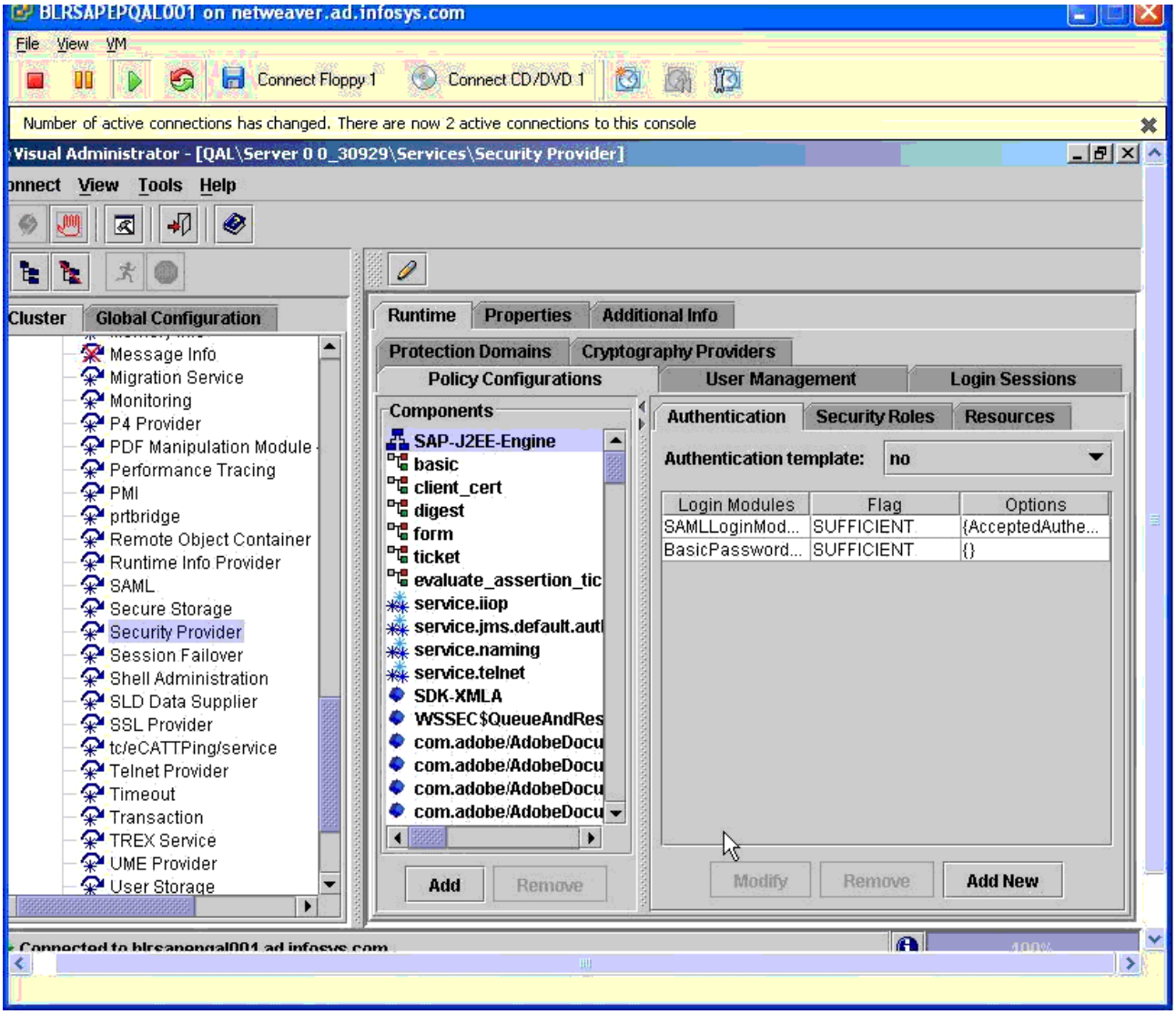
Perform the following steps using the **Security Provider** service in the **Visual Administrator** to adjust the login modules that apply to the application that is to be configured for SAML assertions. Perform these steps for each template or application that is to support SAML assertions, e.g. the `basic` template.

1. Select the **Authentication** tab.



2. Click **Add New**. The *Available Login Modules* page appears.
3. Select **SAMLLoginModule**. Click **OK**. The SAML Login Module is added to the end of the list of Login Modules.
4. Select SAMLLoginModule and click **Modify**. The *Edit Login Module* page is page is displayed.
5. Set the **Position** to `1`.

6. Ensure the **Flag** is set to `SUFFICIENT`.



7. Click **OK**.

Reference/Related Content

Peter Tuton, “Configuring Single Sign-on for SAP NetWeaver Application Server Java™ with IBM Tivoli Federated Identity Manager using SAML 1.0 “ (SAP Article on SDN **Created on:** 21 March 2006)

Using SAML Assertions for Single Sign-On on help.sap.com

For more information, visit the Identity and Access Management homepage.

Disclaimer and Liability Notice

This document may discuss sample coding or other information that does not include SAP official interfaces and therefore is not supported by SAP. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing the information, code or methods suggested in this document, and anyone using these methods does so at his/her own risk.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of this technical article or code sample, including any liability resulting from incompatibility between the content within this document and the materials and services offered by SAP. You agree that you will not hold, or seek to hold, SAP responsible or liable with respect to the content of this document.