



FORUM SENTRY™ VERSION 9

KERBEROS INTEGRATION GUIDE



Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOS™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™ Forum Sentry™ Web Services Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2024 Forum Systems, Inc. – All Rights Reserved.

Forum Sentry™ Version 9 Kerberos Integration Guide, published May 2024.

D-ASF-SE-029975

Table of Contents

Audience for the Kerberos Integration Guide	4
Conventions Used	4
Kerberos Background	5
Kerberos Service Ticket in SOAP Message	5
Kerberos Support on the System.....	6
Kerberos Concepts and Definitions	6
KERBEROS CONFIGURATION WITH MICROSOFT ACTIVE DIRECTORY	7
KERBEROS CONFIGURATION	9
Configure Kerberos.....	9
Kerberos Policy Creation Screen Terms	10
Kerberos Tokens Examples.....	10
Prerequisites for the User Identity and Access Control Task	10
Add User Identity and Access Control Task for a Kerberos Token.....	11
Step 1: Adding the Identify Document that Includes a Kerberos Token (Optional).....	11
Step 2: Adding the User Identity & Access Control task using a Kerberos Token.....	11
Add SAML Assertion Task Using SAML Custom Attribute from LDAP.....	13
Adding SAML Assertion with SAML Custom Attribute from LDAP.....	14

Audience for the Kerberos Integration Guide

The *Forum Systems Sentry™ Version 9 Kerberos Integration Guide* is for System Administrators who will manage access control policies which use Kerberos tokens for authentication.

Conventions Used

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name: **johnsmith**
Password: *********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.

Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

Kerberos Background

Kerberos is an authentication system that was developed at the Massachusetts Institute of Technology (MIT). Kerberos is designed to enable two parties to exchange private information across an otherwise open network. It works by assigning a unique key, called a ticket, to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

Primarily a centralized network authentication system, Kerberos is designed to verify user's identities and other identities such as, server principal. When configured on the system, Kerberos provides a means of authentication that does not compromise user or server principal passwords by transmitting them over the network in clear text.

The system accepts Kerberos tickets for authentication as it does other Single Sign-on credentials like SAML Assertions or Username tokens. The client passes the Kerberos service ticket as an AP_REQ (ST and Authenticator) to the system via WS Security headers. In this way, Kerberos transitions to a web service which can be used with Forum Systems Sentry.

Sentry adheres to the OASIS Web Service Security group which published the Kerberos Token Profile, defining how to encode Kerberos tickets and attach them to SOAP messages.

The Kerberos Token Profile specification is limited to using the AP-REQ packet (service ticket and authenticator) defined by Kerberos as the Kerberos token. This allows a service to authenticate the ticket and interoperate with existing Kerberos implementations.

Kerberos Service Ticket in SOAP Message

An example of a SOAP message with a Kerberos service ticket is shown below:

```
<S11:Envelope xmlns:S11="...">
  <S11:Header>
    <wsse:Security xmlns:wsse="...">
      <wsse:BinarySecurityToken xmlns:wsse="..." xmlns:wsu="..."
        wsu:Id="myToken" ValueType="...#Kerberosv5_AP_REQ"
        EncodingType="...#Base64Binary">
        MIIIEZzCCA9CgAwIBAgIQEmtJZc0...
      </wsse:BinarySecurityToken>
      ...
    </wsse:Security>
  </S11:Header>
  <S11:Body>
    ...
  </S11:Body>
</S11:Envelope>
```

The Kerberos Service Ticket contains the client's username as part of the encrypted data. For the user to successfully authenticate, the system will decrypt the username.

Kerberos Support on the System

Sentry's WebAdmin manages Kerberos configuration and supports Kerberos tokens. The WebAdmin is a web-based management interface used for monitoring as well as configuring all aspects of the system including server, security and network policies.

Kerberos Concepts and Definitions

The following table defines various Kerberos terms and concepts:

CONCEPT	DEFINITION
Ticket	Kerberos ticket is a set of credentials issued by an authentication server, used to verify the user's identity to any given service.
KDC	Key Distribution Center - a trusted authentication server with which every entity shares a secret key and which issues Kerberos tickets.
Kerberos Realm	Each administrative domain will have its own Kerberos database, which contains information about the users and services for that particular site or administrative domain. This administrative domain is the Kerberos realm.
Principal	A unique identity to which Kerberos can assign tickets. Principals can have an arbitrary number of components. Each component is separated by a component separator, generally `/`. The last component is the realm, separated from the rest of the principal by the realm separator, generally `@`. If there is no realm component in the principal, then it will be assumed that the principal is in the default realm for the context in which it is being used.
TGT	Ticket Granting Ticket - the initial ticket obtained by the Kerberos client, used to prove identity to the KDC to obtain Service Tickets.
Service Ticket	The ticket obtained by the Kerberos client for each Kerberos protected service the user wants to access.
Keytab	A file containing a service's secret keys exported from the KDC.
Authenticator	In encrypted record containing the user's name and a timestamp.

KERBEROS CONFIGURATION WITH MICROSOFT ACTIVE DIRECTORY

1. Web Service client machines must be logged in to the Active Directory Server Domain
2. The Kerberos Service (Sentry) needs a user account created in Active Directory for the Service based on its Service Principal. For Example:

sentry/sentry.forumsys.com@isa2004ee.forumsys.com

The following displays the Properties screen during configuration of the Active Directory user account for the Forum Sentry service:

The screenshot shows the 'sentry Properties' dialog box with the 'Account' tab selected. The 'User logon name' field contains 'sentry/sentry.forumsys.com' and the domain dropdown is set to '@isa2004ee.forumsys.com'. The 'User logon name (pre-Windows 2000)' field contains 'ISA2004EE0\'. Below these fields are 'Logon Hours...' and 'Log On To...' buttons. A checkbox for 'Account is locked out' is unchecked. The 'Account options' section contains four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (unchecked), 'Password never expires' (checked), and 'Store password using reversible encryption' (unchecked). The 'Account expires' section has two radio buttons: 'Never' (selected) and 'End of:' (unchecked). The 'End of:' date is set to 'Sunday, June 19, 2005'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Figure 1: Configuring Kerberos Support with Microsoft Active Directory.

In the Sentry Kerberos Configuration, enter:

- Service Name = sentry
 - Host Name = sentry.forumsys.com
 - Realm = ISA2004EE.FORUMSYS.COM
3. The keytab file is exported using ktpass.exe. ktpass.exe is not installed with the Windows operating system; you must install ktpass separately from the \Support\Tools folder of the Windows operating system CD.

The ktpass command for the above example would look like the following (all on one line):

```
ktpass -out keytab -princ  
sentry/sentry.forumsys.com@ISA2004EE.FORUMSYS.COM -pass * -crypto DES-  
CBC-CRC -mapuser sentry
```

4. Be sure to install "Windows Server 2003 Service Pack 1 32-bit Support Tools". This service pack can be found on Microsoft's Website:

KERBEROS CONFIGURATION

Sentry administrators can create or modify multiple Kerberos policies from the WebAdmin to allow multiple Kerberos configurations to be used within the same Sentry instance.

Administrators need to enter a service principal which is the Kerberos identifier for a service. The service principal is made up of a service name (Sentry firewall name), hostname and Kerberos realm. The following is an example of a service principal:

sentry/sentry.forumsys.com@ISA2004EE.FORUMSYS.COM

Configure Kerberos

Log on to the WebAdmin and confirm that the system is appropriately licensed for Kerberos tickets. For more information, refer to the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.

KERBEROS POLICIES

2 items found. Search max results 1000 [Show](#)

- [KERBEROS POLICY](#)
- [PDC_Customer1](#)
- [PDC1](#)

[Settings](#) [Delete](#) [New](#)

KERBEROS POLICIES > KERBEROS POLICY

KERBEROS POLICY

Name*:

Service Name*:

Host Name*:

Realm*:

Keytab File*: No file chosen

Enabled: ☒

[Save](#)

- On the Navigator, under the Access category, select **Kerberos**.
- Click the **New** button.
- In the Name field, enter your **policy name**.
- In the Service Name field, enter your **service name**.
- In the Host Name field, enter your **host name**.
- In the Realm field, enter your **realm**.
- Accept the default Maximum Clock Skew (secs) field.
- Aligned with Keytab File, click **Browse** to navigate your file system.
- Locate and select the **keytab file** (generated from your KDC), and click **Open**.
- Check the **Enable** checkbox.
- Click **Save**.

Kerberos Policy Creation Screen Terms

The Kerberos configuration screen includes the following terms and definitions:

TERM	DEFINITION
Name	The name this Kerberos policy will be referenced by.
Service Name	The name of the Kerberos protected service.
Host Name	The host name or IP address for the Kerberos service.
Realm	The Kerberos administrative domain.
Maximum Clock Skew	The maximum clock skew allowed between a Kerberos client and Sentry. The client presents a timestamp to the server as part of the Kerberos authenticator. If the difference between the presented timestamp and the current Sentry system time is greater than this value, the client request is invalid.
Keytab File	The keytab file for the Kerberos policy contains the Kerberos service secret key.
Enabled	When checked, the new Kerberos policy will be enabled when saved.

Kerberos Tokens Examples

Examples for working with Kerberos tokens include:

- Add User Identity & Access Control Task for a Kerberos Token.
- Add WSS SAML Assertion Task with SAML Custom Attribute from LDAP.
- Add SAML Assertion Task with SAML Custom Attribute from LDAP.

Prerequisites for the User Identity and Access Control Task

This instruction assumes that the administrator has:

- Loaded a sample document which contains a Kerberos ticket.
- Added an XML Policy.
- Created a task list for the XML Policy using the sample document.

Note: Not all graphics are shown for the above steps. For more information on performing the above actions, refer to the *Forum Systems Sentry™ Version 9 XML Policies Guide* and *Forum Systems Sentry™ Version 9 Access Control Guide*.

Add User Identity and Access Control Task for a Kerberos Token

Step 1: Adding the Identify Document that Includes a Kerberos Token (Optional)

- On the TASK LIST screen, select **New**.
- Enter a name for your task list. Select a sample document with a Kerberos token like he one below. Click **Apply**.



- On the TASK screen, select **New**.
- On the TASK TYPE screen, select the **Identify Document** radio button, and then click **Next**.
- Under the **Document Filter Expression Builder** section select some XML nodes that uniquely identify the document type. The wsse:BinarySecurityToken would be ideal for this. Click **Save**.

Step 2: Adding the User Identity & Access Control task using a Kerberos Token

- On the TASK screen, select **New**.
- On the TASK TYPE screen, select the **User Identity & Access Control** radio button, and then click **Next**.
- On the TASK NAME screen, select a **Task Name** and then click **Next**.
- On the ACCESS CONTROL screen, check the **Map identified user to a known user** checkbox.
- From the ACL Policy drop down list, select **Allow All**, and then click **Next**.

Note: For use cases requiring Kerberos user attributes from LDAP or similar user information, you must map to a known user. Configurations using Kerberos and user attributes without mapping to a known user will fail.

When selecting the Allow All ACL, then no user authorization other than Kerberos is performed.

- On the USER IDENTITY MECHANISM screen, select the **Validate WS-Security & establish identity** radio button, and then click **Next**.

- On the MAXIMUM WS-SECURITY VALIDITY PERIOD screen, click **Next**.
- On the SECURITY TOKEN TYPE screen, select the **Kerberos token** radio button, and then click **Next**.
- On the REMOVE TOKEN screen, determine whether you want to remove the token after processing. Click **Next**.
- On the ERROR TEMPLATE screen, determine if you want to use a different Error Template. Click **Finish**.

Note: Enabling the Remove token option stops the token from being passed beyond the Forum system.

Add WSS SAML Assertion Task Using SAML Custom Attribute from LDAP

Sentry supports the inclusion of custom attributes whose values are retrieved from LDAP in a SAML assertion token within a WS-Security Header. Sentry will pull the LDAP attribute specified in the “Name” field from the authenticated user’s LDAP record. SAML custom attributes can be configured in a WS-Security Header task. Follow these steps to add the WS-Security Header task with SAML custom attribute from LDAP:

Note: This instruction requires that you have an LDAP policy already configured in the WebAdmin. For more information on LDAP policies, refer to the *Forum Systems Sentry™ Version 9 Access Control Guide*.

This instruction generates a WS-Security SAML assertion of the type SAML custom attribute from LDAP.

- On the **TASKS** screen, select **New**.
- On the TASK TYPE screen, select the **WS-Security Header** radio button, and then click **Next**.
- On the TASK NAME screen, click **Next**.
- On the VERSION screen, select the **WSS 1.1** or **WSS 2004** radio button, and then click **Next**.
- On the MUST UNDERSTAND screen, check the **WS-Security processing by the recipient is mandatory** checkbox, and then click **Next**.
- On the TIME TO LIVE screen, check the **Message expires** checkbox.
- Overwrite the Time to live value to **120** minutes, and then click **Next**.
- On the SECURITY TOKEN TYPE screen, select the **SAML token** radio button, and then click **Next**.
- On the SAML VERSION screen, select the **SAML 1.1** or **SAML 2.0** radio button, and then click **Next**.
- On the CONFIRMATION METHOD screen, select **Sender vouches**, and then click **Next**.
- On the SAML ISSUER screen, accept the pre-populated SAML Issuer, and then click **Next**.
- On the SAML AUDIENCE screen, accept the pre-populated SAML Audience, and then click **Next**.
- On the SAML TIME TO START screen, check the **Include a validity** start time checkbox.
- Accept the time to start default value (0), and then click **Next**.
- On the SAML TIME TO EXPIRE screen, check the **Assertion expires** checkbox.
- Overwrite the **value** in the Time to expire field (**120**), and then click **Next**.

Note: The SAML time to start and time to expire may have 1 to 20 numeric characters. The default SAML time to start is 0 minutes, and the default time to expire is 1 minute. A SAML Time to Expire value of 0 minutes is not allowed.

For testing purposes, the SAML Time to Expire header attribute may be increased, allowing time to complete testing and not allowing SAML assertions to expire.

For designing real-time processing tasks, the SAML Time to Expire header attribute should reflect the

smallest window of opportunity which allows SAML requests to pass through the product, as well as maintain the highest level of security.

- On the DISALLOW SAML REUSE screen, check the **Disallow reuse of this assertion** checkbox, and then click **Next**.
- On the USE SAML ADVICE screen, leave the **Use existing SAML assertions as advice** checkbox unchecked, and then click **Next**.
- On the SAML IDENTIFICATION FORMAT screen, select the **Email** radio button, and then click **Next**.
- On the INCLUDE SAML FORMAT URI screen, check the **Include the identifier format URI** checkbox, and then click **Next**.
- On the SAML EMAIL IDENTIFICATION screen, there are two options for configuring the token. Select the **Dynamic**, based on established identity radio button, and then click **Next**.

Note: Selecting the Dynamic, based on established identity radio button applies the email of the user identified earlier in the User Identity and Access Control task to this SAML assertion. Therefore, to select this option, the User Identity and Access Control task must have been added before the WS-Security Header task.

- On the SAML STATEMENT TYPE screen, select the **Attribute** checkbox, and then click **Next**.
- On the SAML AUTHENTICATION screen, leave the **Include the client IP address** checkbox unchecked, and then click **Next**.
- On the SAML ATTRIBUTE screen, accept the value in the Namespace field.
- In the Name field, enter the **name** of a valid LDAP attribute configured on your LDAP server (UID). Multiple values can be separated with comas.
- On the Value Type section of the screen, select the **User attribute** (e.g. LDAP) radio button, and then click **Next**.
- On the SIGN SAML ASSERTION screen, check the **Sign SAML assertion** checkbox, and then click Next.

Note: Signing assertions, or some other form of secure authentication, is strongly recommended for actual deployments.

- On the SIGNATURE POLICY screen, from the Signature Policy drop down, select a **Signature Policy** name, and then click **Next**.
- On the INCLUDE CERTIFICATES screen, check the **Include certificates** checkbox, and then click **Next**.
- On the SIGN KEY INFO screen, check the **Sign key info** checkbox, and then click **Finish**.

Add SAML Assertion Task Using SAML Custom Attribute from LDAP

Sentry supports the inclusion of custom attributes whose values are retrieved from LDAP in a SAML assertion. Sentry will pull the LDAP attribute specified in the "Name" field from the authenticated user's LDAP record. SAML custom attributes can be configured in a SAML Assertion Task.

Note: This instruction requires that you have a dynamic LDAP policy already configured in the WebAdmin. For more information on LDAP policies, refer to the *Forum Systems Sentry™ Version 9 Access Control Guide*.

This example generates a SAML attribute assertion that uses the LDAP UUID attribute. Before performing this operation, the WS-Security Header task from the previous example must be disabled.

Adding SAML Assertion with SAML Custom Attribute from LDAP

- On the TASKS screen, select **New**.
- On the TASK TYPE screen, select the **SAML Assertion** radio button, and then click **Next**.
- Accept the Task Name in the TASK NAME screen, and then click **Next**.
- On the VERSION screen, select the **SAML 1.1** or **SAML 2.0** radio button, and then click **Next**.
- On the CONFIRMATION METHOD screen, select **Sender vouches**, and then click **Next**.
- On the ISSUER screen, the Issuer name is pre-populated in the Issuer field. Click **Next**.
- On the SAML AUDIENCE screen, accept the pre-populated SAML Audience, and then click **Next**.
- On the TIME TO START screen, check the **Include a validity start time** checkbox.
- Accept the time to start default value (0), and then click **Next**.

Note: The Time to start and time to expire may have 1 to 20 numeric characters. The default Time to start is 0 minutes, and the default Time to expire is 1 minute.

For designing real-time processing tasks, the Time to expire should reflect the smallest window of opportunity which allows SAML requests to pass through the product, as well as maintain the highest level of security.

For testing purposes, the Time to expire attribute may be increased, allowing time to complete testing and not allowing SAML assertions to expire.

- On the TIME TO EXPIRE screen, check the **Assertion expires** checkbox.
- In the Time to expire field, enter a **value** as the time to expire after issued, and then click **Next**.
- On the DISALLOW REUSE screen, leave the **Disallow reuse of this assertion** checkbox unchecked, and then click **Next**.
- On the USE SAML ADVICE screen, leave the **Use existing SAML assertions as advice** checkbox unchecked, and then click **Next**.
- On the IDENTIFICATION FORMAT screen, check the **Email** radio button, and then click **Next**.
- On the INCLUDE FORMAT URI screen, check the **Include the identifier format URI** checkbox, and then click **Next**.
- On the EMAIL IDENTIFICATION screen, click the **Dynamic, based on established identity** radio button, and then click **Next**.

Note: Selecting the Dynamic, based on established identity radio button applies the email of the user identified earlier during the User Identity and Access Control task to this SAML assertion.

- On the STATEMENT TYPE screen, select the **Attribute** checkbox, and then click **Next**.
- On the AUTHENTICATION screen, leave the **Include the client IP address** checkbox unchecked, and then click **Next**.
- On the ATTRIBUTE screen, accept the value in the Namespace field.
- In the Name field, enter the **name** of a valid LDAP attribute configured on your LDAP server. This instruction uses UID. Multiple values can be separated with commas.
- In the Value Type section of the screen, select the **User attribute (e.g. LDAP)** radio button, and then click **Next**.
- On the SIGN ASSERTION screen, check the **Sign assertion** checkbox, and then click **Next**.

Note: Signing assertions, or some other form of secure authentication, is strongly recommended for actual deployments.

- On the SIGNATURE POLICY screen, in the Signature Policy drop down list, select a **Signature policy name**, and then click **Next**.
- On the INCLUDE CERTIFICATES screen, check the **Include certificates** checkbox, and then click **Next**.

- On the SIGN KEY INFO screen, check the **Sign key info** checkbox, and then click **Finish**.