Oracle® Fusion Middleware

Policy and Assertion Template Reference for Mobile Security Access Server

11*g* Release 2 (11.1.2.3.0)

E58639-01

April 2015

This document describes all of the predefined policies and assertion templates available with Mobile Security Access Server.

ORACLE

Oracle Fusion Middleware Policy and Assertion Template Reference for Mobile Security Access Server, 11*g* Release 2 (11.1.2.3.0)

E58639-01

Primary Author: Jeff Schieli

Contents

2 Predefined Assertion Templates

3 Assertion Template Settings and Configuration Properties

Preface

This section describes the intended audience, how to use this guide, and provides information about documentation accessibility.

Audience

This document is intended for

- System and security administrators who administer web services and manage security
- Application developers who are developing web services and testing the security prior to deployment of the web services
- Security architects who create security policies

How to Use This Guide

It is recommended that you review *Administering Mobile Security Access Server* to gain a better understanding of Mobile Security Access Server (MSAS), a component in the Oracle Mobile Security Suite.

The document is organized as follows:

- Predefined Policies – describes the MSAS predefined security policies.
- Predefined Assertion Templates – describes the MSAS predefined security assertion templates.
- Assertion Template Settings and Configuration Properties – provides details on all the assertion template settings and configuration properties.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Access Management doc set:

- *Installing Oracle Mobile Security Access Server*
- *Administering Oracle Mobile Security Access Server*
- *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*
- *WebLogic Scripting Tool Command Reference for Identity and Access Management*
- *Release Notes for Oracle Identity Management*
- *Installation Guide for Oracle Identity and Access Management*
- *Administering Oracle Mobile Security Suite*
- *Help Reference for Oracle Mobile Security Suite Consoles*
- *High Availability Guide*
- *Administrator's Guide for Oracle Access Management*
- *Securing Applications with Oracle Platform Security Services*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Predefined Policies

This chapter describes the Mobile Security Access Server (MSAS) predefined security and management policies. For more information about attaching policies, see "Attaching and Detaching Policies and Assertions" in *Administering Mobile Security Access Server*.

This chapter includes the following sections:

- Predefined Security Policies
- Predefined Management Policies

> **Note:** Oracle recommends that you do not edit the predefined assertion templates so that you will always have a known set of valid templates. You can, however, create a new assertion template from a predefined assertion template, or configure the attributes in an assertion after you have added it to a policy. For information about managing the assertion templates and adding them to policies, see "Managing Policy Assertion Templates" in *Administering Mobile Security Access Server*.

Predefined Security Policies

This section describes the predefined security policies that are provided with your MSAS installation and which are listed on the **Access Policies** page in the MSAS Console.

The tables in the following sections distinguish how the MSAS security policies are documented in this release:

- MSAS Security Policies – summarizes new MSAS security policies that are documented in this reference.

  Note: Some policies are marked as ***internal*** because they are not available for attachment to URLs in applications.

- Security Polices Supported by MSAS – summarizes additional security policies that are supported by MSAS, but which are documented in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.
- Security Polices Reserved for Future Use – summarizes security policies that appear in the MSAS Console, but which are reserved for future use with MSAS.

MSAS Security Policies

Table 1–1 summarizes the predefined MSAS security policies listed on the **Access Policies** page in the MSAS Console, and which are documented in this reference.

Table 1–1 Predefined MSAS Security Policies

Policy Name	Description
oracle/binding_oes_authorization_policy	Performs user authorization based on the policy defined in Oracle Entitlements Server (OES) and provides fine-grained authorization on any operation on a web service.
oracle/http_action_over_ssl_policy	**Internal** policy that provides SKEK encryption and SKEK decryption.
oracle/http_bmax_jwt_user_token_client_policy	Injects a JWT User Token in the HTTP header when accessing back-end resources.
oracle/http_bmax_oam_client_policy	Injects an OAM access token in the authorization header when accessing OAM protected resources.
oracle/http_bmax_oauth_client_policy	Injects an OAuth access token in the authorization header when accessing OAuth protected resources.
oracle/http_bmax_spnego_client_policy	Creates a SPNEGO token and sends it to the service in the HTTP header.
oracle/http_form_based_auth_over_ssl_service_policy	**Internal** policy that performs HTML form based authentication. This policy can be attached to web applications (URLs).
oracle/http_kinit_over_ssl_policy	**Internal** policy that enables the Kerberos password authentication.
oracle/http_oam_authentication_service_policy	Verifies if the web resource is protected via OAM, and if it is then it authenticates using OAM and establishes the Subject before allowing access to the actual web resource.
oracle/http_oauth2_confidential_client_over_ssl_policy	**Internal** policy that performs OAuth2 confidential client authentication and creates OAuth and OAM tokens. This policy is attached only on internal authentication endpoints.
oracle/http_oauth2_mobile_client_over_ssl_policy	**Internal** policy that performs OAuth2 mobile client authentication and creates OAuth and OAM tokens. This policy is attached only on internal authentication endpoints.
oracle/http_ntlm_token_client_policy	Performs NTLM (NT LAN Manager) authentication with NTLM protected applications. It requires a KINIT or PKINIT-based HTTP session token. This policy can be attached to SOAP/REST services and also to web applications.
oracle/http_pkinit_over_ssl_policy	**Internal** policy enables the Kerberos PKI authentication.
oracle/http_session_token_issue_policy	**Internal** policy that issues a session token with the authenticated user ID.
oracle/http_session_token_verify_policy	Verifies the session token including the timestamp and signature, decrypts the encrypted data and asserts the identity using the user ID from the session token. The request is rejected if the verification fails.
oracle/http_tlp_over_ssl_policy	**Internal** policy that enables the Time Limited Password authentication.

Table 1–1 (Cont.) Predefined MSAS Security Policies

Policy Name	Description
oracle/inject_header_with_bmax_url_policy	**Internal** policy that injects a custom HTTP Header with the BMAX (MSAS) URL. This is required by MSM to know the MSAS URL.
oracle/inject_header_with_client_certificate_policy	**Internal** policy that injects a custom HTTP header with the client certificate received over two-way SSL.
oracle/multi_token_client_policy	An exactly-one policy for creating a SPNEGO, NTLM, or Bearer assertion based on a back-end service policy.

Security Polices Supported by MSAS

Table 1–2 summarizes additional access policies that are supported by Mobile Security Access Server. For detailed descriptions, however, see "Predefined Policies" in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.

Table 1–2 Predefined Security Policies Supported by MSAS

Policy Name	Description
oracle/http_basic_auth_over_ssl_client_policy	Includes credentials in the HTTP header for outbound client requests and verifies that the transport protocol is HTTPS.
oracle/http_basic_auth_over_ssl_service_policy	Uses the credentials in the HTTP header to authenticate users against the Oracle Platform Security Services identity store.
oracle/http_jwt_token_client_policy	Includes a JSON Web Token (JWT) token in the HTTP header. The JWT token is created automatically. The issuer name and subject name are provided either programmatically or declaratively through the policy. You can specify the audience restriction condition for this policy.
oracle/http_jwt_token_over_ssl_client_policy	Includes a JWT token in the HTTP header. The JWT token is created automatically. The issuer name and subject name are provided either programmatically or declaratively through the policy. You can specify the audience restriction condition for this policy.
oracle/http_jwt_token_over_ssl_service_policy	Authenticates users using the username provided in the JWT token in the HTTP header. This policy also verifies that the transport protocol is HTTPS. Requests over a non-HTTPS transport protocol are refused.
oracle/http_jwt_token_service_policy	Authenticates users using the username provided in the JWT token in the HTTP header.
oracle/http_saml20_token_bearer_client_policy	Includes a SAML Bearer V2.0 token in the HTTP header. The SAML token with confirmation method Bearer is created automatically. This policy can be enforced on any HTTP-based client endpoint.
oracle/http_saml20_token_bearer_over_ssl_client_policy	Includes a SAML Bearer v2.0 token in the HTTP header. The SAML token with confirmation method Bearer is created automatically. The policy verifies that the transport protocol provides SSL message protection. This policy can be attached to any HTTP-based client endpoint.
oracle/http_saml20_token_bearer_over_ssl_service_policy	Authenticates users using credentials provided in the SAML v2.0 token with confirmation method Bearer in the HTTP header. The credentials in the SAML token are authenticated against a SAML v2.0 login module. The policy verifies that the transport protocol provides SSL message protection. This policy can be enforced on any HTTP-based endpoint.

Table 1–2 (Cont.) Predefined Security Policies Supported by MSAS

Policy Name	Description
oracle/http_saml20_token_bearer_service_policy	Authenticates users using credentials provided in the SAML v2.0 token with confirmation method Bearer in the HTTP header. The credentials in the SAML token are authenticated against a SAML v2.0 login module. This policy can be enforced on any HTTP-based endpoint.
oracle/wss_http_token_client_policy	Includes credentials in the HTTP header for outbound client requests. This policy can be enforced on any HTTP-based client.
oracle/wss_http_token_service_policy	Uses the credentials in the HTTP header to authenticate users against the Oracle Platform Security Services identity store. This policy can be enforced on any HTTP-based endpoint.

Security Polices Reserved for Future Use

Table 1–3 summarizes the predefined MSAS policies that are listed in the **Access Policies** page, but which are reserved for future use.

Table 1–3 Predefined Security Policies that Are Reserved for Future Use

Policy Name	Description
oracle/binding_authorization_denyall_policy	Reserved for future use.
oracle/binding_authorization_permitall_policy	Reserved for future use.
oracle/binding_oes_masking_policy	Reserved for future use.
oracle/binding_permission_authorization_policy	Reserved for future use.
oracle/component_authorization_denyall_policy	Reserved for future use.
oracle/component_authorization_permitall_policy	Reserved for future use.
oracle/component_oes_authorization_policy	Reserved for future use.
oracle/component_permission_authorization_policy	Reserved for future use.
oracle/http_jwt_token_identity_switch_client_policy	Reserved for future use.
oracle/http_oam_token_service_policy	Reserved for future use.
oracle/http_oauth2_token_client_policy	Reserved for future use.
oracle/http_oauth2_token_identity_switch_opc_oauth2_over_ssl_client_policy	Reserved for future use.
oracle/http_oauth2_token_identity_switch_over_ssl_client_policy	Reserved for future use.
oracle/http_oauth2_token_opc_oauth2_client_policy	Reserved for future use.
oracle/http_oauth2_token_opc_oauth2_over_ssl_client_policy	Reserved for future use.
oracle/http_oauth2_token_over_ssl_client_policy	Reserved for future use.
oracle/multi_token_over_ssl_client_policy	Reserved for future use.

Table 1–3 (Cont.) Predefined Security Policies that Are Reserved for Future Use

Policy Name	Description
oracle/multi_token_over_ssl_rest_service_policy	Reserved for future use.
oracle/multi_token_rest_service_policy	Reserved for future use.
oracle/no_authentication_client_policy	Reserved for future use.
oracle/no_authentication_service_policy	Reserved for future use.
oracle/no_authorization_component_policy	Reserved for future use.
oracle/no_authorization_service_policy	Reserved for future use.
oracle/no_messageprotection_client_policy	Reserved for future use.
oracle/no_messageprotection_service_policy	Reserved for future use.
oracle/oauth2_config_client_policy	Reserved for future use.
oracle/pii_security_policy	Reserved for future use.
oracle/sts_trust_config_client_policy	Reserved for future use.
oracle/sts_trust_config_service_policy	Reserved for future use.
oracle/whitelist_authorization_policy	Reserved for future use.
oracle/wss10_message_protection_client_policy	Reserved for future use.
oracle/wss10_message_protection_client_policy	Reserved for future use.
oracle/wss10_saml20_token_client_policy	Reserved for future use.
oracle/wss10_saml20_token_service_policy	Reserved for future use.
oracle/wss10_saml20_token_with_message_protection_client_policy	Reserved for future use.
oracle/wss10_saml20_token_with_message_protection_service_policy	Reserved for future use.
oracle/wss10_saml_hok_with_message_protection_client_policy	Reserved for future use.
oracle/wss10_saml_hok_token_with_message_protection_service_policy	Reserved for future use.
oracle/wss10_saml_token_client_policy	Reserved for future use.
oracle/wss10_saml_token_service_policy	Reserved for future use.
oracle/wss10_saml_token_with_message_integrity_client_policy	Reserved for future use.
oracle/wss10_saml_token_with_message_integrity_service_policy	Reserved for future use.
oracle/wss10_saml_token_with_message_protection_client_policy	Reserved for future use.
oracle/wss10_saml_token_with_message_protection_service_policy	Reserved for future use.
oracle/wss10_saml_token_with_message_protection_ski_basic256_client_policy	Reserved for future use.
oracle/wss10_saml_token_with_message_protection_ski_basic256_service_policy	Reserved for future use.
oracle/wss10_username_id_propagation_with_msg_protection_client_policy	Reserved for future use.

Table 1–3 (Cont.) Predefined Security Policies that Are Reserved for Future Use

Policy Name	Description
oracle/wss10_username_id_propagation_with_msg_protection_service_policy	Reserved for future use.
oracle/wss10_username_token_with_message_protection_client_policy	Reserved for future use.
oracle/wss10_username_token_with_message_protection_service_policy	Reserved for future use.
oracle/wss10_username_token_with_message_protection_ski_basic256_client_policy	Reserved for future use.
oracle/wss10_username_token_with_message_protection_ski_basic256_service_policy	Reserved for future use.
oracle/wss10_x509_token_with_message_protection_client_policy	Reserved for future use.
oracle/wss10_x509_token_with_message_protection_service_policy	Reserved for future use.
oracle/wss11_kerberos_token_client_policy	Reserved for future use.
oracle/wss11_kerberos_token_service_policy	Reserved for future use.
oracle/wss11_kerberos_token_with_message_protection_basic128_client_policy	Reserved for future use.
oracle/wss11_kerberos_token_with_message_protection_basic128__service_policy	Reserved for future use.
oracle/wss11_kerberos_token_with_message_protection_client_policy	Reserved for future use.
oracle/wss11_kerberos_token_with_message_protection_service_policy	Reserved for future use.
oracle/wss11_message_protection_client_policy	Reserved for future use.
oracle/wss11_message_protection_client_policy	Reserved for future use.
oracle/wss11_saml20_token_with_message_protection_client_policy	Reserved for future use.
oracle/wss11_saml20_token_with_message_protection_service_policy	Reserved for future use.
oracle/wss11_saml_or_username_token_with_message_protection_service_policy	Reserved for future use.
oracle/wss11_saml_token_with_identity_switch_message_protection_client_policy	Reserved for future use.
oracle/wss11_saml_token_with_message_protection_client_policy	Reserved for future use.
oracle/wss11_saml_token_with_message_protection_service_policy	Reserved for future use.
oracle/wss11_sts_issued_saml_hok_with_message_protection_client_policy	Reserved for future use.
oracle/wss11_sts_issued_saml_hok_with_message_protection_service_policy	Reserved for future use.
oracle/wss11_sts_issued_saml_with_message_protection_client_policy	Reserved for future use.
oracle/wss11_username_token_with_message_protection_client_policy	Reserved for future use.

Table 1–3 (Cont.) Predefined Security Policies that Are Reserved for Future Use

Policy Name	Description
oracle/wss11_username_token_with_message_protection_service_policy	Reserved for future use.
oracle/wss11_x509_token_with_message_protection_client_policy	Reserved for future use.
oracle/wss11_x509_token_with_message_protection_service_policy	Reserved for future use.
oracle/wss_http_token_over_ssl_client_policy	Reserved for future use.
oracle/wss_http_token_over_ssl_service_policy	Reserved for future use.
oracle/wss_saml20_token_bearer_over_ssl_client_policy	Reserved for future use.
oracle/wss_saml20_token_bearer_over_ssl_service_policy	Reserved for future use.
oracle/wss_saml20_token_over_ssl_client_tpolicy	Reserved for future use.
oracle/wss_saml20_token_over_ssl_service_policy	Reserved for future use.
oracle/wss_saml_bearer_or_username_token_service_policy	Reserved for future use.
oracle/wss_saml_or_username_token_over_ssl_service_policy	Reserved for future use.
oracle/wss_saml_or_username_token_service_policy	Reserved for future use.
oracle/wss_saml_token_bearer_client_policy	Reserved for future use.
oracle/wss_saml_token_bearer_identity_switch_client_policy	Reserved for future use.
oracle/wss_saml_token_bearer_over_ssl_client_policy	Reserved for future use.
oracle/wss_saml_token_bearer_over_ssl_service_policy	Reserved for future use.
oracle/wss_saml_token_over_ssl_client_policy	Reserved for future use.
oracle/wss_saml_token_over_ssl_service_policy	Reserved for future use.
oracle/wss_sts_issued_saml_bearer_token_over_ssl_client_policy	Reserved for future use.
oracle/wss_sts_issued_saml_bearer_token_over_ssl_service_policy	Reserved for future use.
oracle/wss_username_token_client_policy	Reserved for future use.
oracle/wss_username_token_service_policy	Reserved for future use.
oracle/wss_username_token_over_ssl_client_policy	Reserved for future use.
oracle/wss_username_token_over_ssl_service_policy	Reserved for future use.

oracle/binding_oes_authorization_policy

Display Name: Fine-grained authorization using Oracle Entitlements Server

Category: Security

Description

This policy performs user authorization based on the policy defined in Oracle Entitlements Server (OES) and provides fine-grained authorization on any operation on a web service. Authorization is based on attributes, current authenticated subject, and web service actions invoked by the client. This policy should follow an authentication policy where the subject is established, and can be attached to any SOAP-based or REST-based endpoint.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/binding_oes_authorization_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–5, " binding_oes_authorization_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_action_over_ssl_policy

Display Name: HTTP Action Security Policy

Category: Security

Description

This internal policy provides SKEK encryption and SKEK decryption.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_action_over_ssl_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–7, " http_action_over_ssl_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_bmax_jwt_user_token_client_policy

Display Name: HTTP BMAX JWT User Token Client Policy

Category: Security

Description

This policy injects a JWT User Token in the HTTP header when accessing back-end resources.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_bmax_jwt_user_token_client_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–8, " http_bmax_jwt_user_token_client_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_bmax_oam_client_policy

Display Name: HTTP BMAX OAM Token Client Policy

Category: Security

Description

This policy injects an OAM access token in the authorization header when accessing OAM protected resources.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_bmax_oam_client_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–9, " http_bmax_oam_client_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_bmax_oauth_client_policy

Display Name: HTTP BMAX OAUTH Client Policy

Category: Security

Description

This policy injects an OAuth access token in the authorization header when accessing OAuth protected resources.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_bmax_oauth_client_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–10, " http_bmax_oauth_client_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_bmax_spnego_client_policy

Display Name: HTTP BMAX SPNEGO Client Policy

Category: Security

Description

This policy creates a SPNEGO token and sends it to the service in the HTTP header.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_bmax_spnego_client_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–11, " http_bmax_spnego_client_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_form_based_auth_over_ssl_service_policy

Display Name: HTTP Form Based Authentication Service Policy

Category: Security

Description

This internal policy performs HTML form based authentication. This policy can be attached to web applications (URLs).

Assertion

This internal policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_form_based_auth_over_ssl_service_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–13, " http_form_based_auth_over_ssl_service_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_kinit_over_ssl_policy

Display Name: HTTP Kerberos Password Authentication Service Policy

Category: Security

Description

This internal policy enables the Kerberos password authentication.

Assertion

This internal policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_kinit_over_ssl_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–15, " http_kinit_over_ssl_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_oam_authentication_service_policy

Display Name: HTTP OAM Access Service Policy

Category: Security

Description

This policy verifies if the web resource is protected via OAM, and if it is then it authenticates using OAM and establishes the Subject before allowing access to the actual web resource.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_oam_authentication_service_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–18, " http_oam_authentication_service_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_oauth2_confidential_client_over_ssl_policy

Display Name: HTTP OAuth2 Confidential Client Over SSL Policy

Category: Security

Description

This internal policy performs OAuth2 confidential client authentication and creates OAuth and OAM tokens. This policy is attached only on internal authentication endpoints.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_oauth2_confidential_client_over_ssl_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–20, " http_oauth2_confidential_client_over_ssl_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_oauth2_mobile_client_over_ssl_policy

Display Name: HTTP OAuth2 Mobile Client Token Over SSL Service Policy

Category: Security

Description

This internal policy performs OAuth2 mobile client authentication and creates OAuth and OAM tokens. This policy is attached only on internal authentication endpoints.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_oauth2_mobile_client_over_ssl_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–22, " http_oauth2_mobile_client_over_ssl_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_ntlm_token_client_policy

Display Name: HTTP NTLM Authentication Client Policy

Category: Security

Description

This policy performs NTLM (NT LAN Manager) authentication with NTLM protected applications. It requires a KINIT or PKINIT-based HTTP session token. This policy can be attached to SOAP/REST services and also to web applications.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_ntlm_token_client_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–16, " http_ntlm_token_client_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_pkinit_over_ssl_policy

Display Name: HTTP Kerberos PKI Authentication Service Policy

Category: Security

Description

This internal policy enables the Kerberos PKI authentication.

Assertion

This internal policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_pkinit_over_ssl_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–24, " http_pkinit_over_ssl_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_session_token_issue_policy

Display Name: HTTP Session Token Issue Policy

Category: Security

Description

This policy issues a session token with the authenticated user ID.

Assertion

This internal policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_session_token_issue_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–26, " http_session_token_issue_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_session_token_verify_policy

Display Name: HTTP Session Token Verify Policy

Category: Security

Description

This policy verifies the session token including the timestamp and signature, decrypts the encrypted data and asserts the identity using the user ID from the session token. The request is rejected if the verification fails.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_session_token_verify_template

  Note: The `assert.stoken.identity` property's default value is `false` in the `http_session_token_verify_template`. For authorization policy scenarios, this property must be set to `true`.

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–28, " http_session_token_verify_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/http_tlp_over_ssl_policy

Display Name: HTTP TLP Authentication Service Policy

Category: Security

Description

This internal policy enables the Time Limited Password authentication.

Assertion

This internal policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/http_tlp_over_ssl_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–30, " http_tlp_over_ssl_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/inject_header_with_bmax_url_policy

Display Name: Inject Header with BMAX (MSAS) URL

Category: Security

Description

This internal policy injects a custom HTTP header with the BMAX (MSAS) URL. This is required by MSM to know the MSAS URL.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/inject_header_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–31, " inject_header_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/inject_header_with_client_certificate_policy

Display Name: Inject Header with Client Certificate Policy

Category: Security

Description

This internal policy injects a custom HTTP header with the client certificate received over two-way SSL.

Assertion

This policy contains an assertion that is based on the following assertion template, which defines the settings and configuration properties for the policy:

- oracle/inject_header_template

Configuration

To configure the policy:

- Override the configuration properties defined in Table 2–31, " inject_header_template Configuration Properties". For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.

oracle/multi_token_client_policy

Display Name: Multitoken Client Policy for SPNEGO, NTLM, OAM, and OAuth2

Category: Security

Description

This policy is an exactly-one policy for enforcing one of the following authentication policies based on a back-end service policy using transport security.

- SPNEGO over HTTP security—Extracts Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) token from the HTTP header.
- NTLM over HTTP token—Performs NT LAN Manager authentication with NTLM protected applications.
- BMAX OAM Client Policy for OAuth2 authentication SSO—Accesses OAM protected resources.
- BMAX OAuth2 Client Policy for OAuth2 authentication SSO—Accesses OAuth2 protected resources.

Assertions (OR Group)

This policy contains assertions that are based on the following assertion templates as an OR group—meaning any one of the tokens can be sent by the client:

- "oracle/http_spnego_token_client_template" in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.
- oracle/http_ntlm_token_client_template
- oracle/http_bmax_oam_client_template

- oracle/http_bmax_oauth_client_template

Configuration

To configure the policy:

- Override the configuration properties defined in one of the following sections, based on the token sent by the client. For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.
  - "http_spnego_token_client_template Configuration Properties" in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*
  - Table 2–16, " http_ntlm_token_client_template Configuration Properties"
  - Table 2–9, " http_bmax_oam_client_template Configuration Properties"
  - Table 2–10, " http_bmax_oauth_client_template Configuration Properties"

oracle/multi_token_over_ssl_client_policy

Display Name: Multitoken Client Policy for SPNEGO, NTLM, OAM, and OAuth2 Using Transport Security

Category: Security

Note: This policy is reserved for future use.

Reserved for future use.

Description

This policy is an exactly-one policy for enforcing one of the following authentication policies based on a back-end service policy using transport security.

- SPNEGO over HTTP security—Extracts Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) token from the HTTP header.
- NTLM over HTTP token—Performs NT LAN Manager authentication with NTLM protected applications.
- BMAX OAM Client Policy for OAuth2 authentication SSO—Accesses OAM protected resources.
- BMAX OAuth2 Client Policy for OAuth2 authentication SSO—Accesses OAuth2 protected resources.

Assertions (OR Group)

This policy contains assertions that are based on the following assertion templates as an OR group—meaning any one of the tokens can be sent by the client:

- "oracle/http_spnego_token_client_template" in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.
- oracle/http_ntlm_token_client_template
- oracle/http_bmax_oam_client_template
- oracle/http_bmax_oauth_client_template

Configuration

To configure the policy:

- Override the configuration properties defined in one of the following sections, based on the token sent by the client. For more information, see "Configuring Policy Overrides" in *Administering Mobile Security Access Server*.
  - "http_spnego_token_client_template Configuration Properties" in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*
  - Table 2–16, " http_ntlm_token_client_template Configuration Properties"
  - Table 2–9, " http_bmax_oam_client_template Configuration Properties"
  - Table 2–10, " http_bmax_oauth_client_template Configuration Properties"

Predefined Management Policies

This section describes the Oracle Mobile Security Access Server (MSAS) predefined management policies.

Note: This section is reserved for future use.

2

Predefined Assertion Templates

This chapter describes the predefined assertion templates defined for the current release. Use the predefined assertion templates to construct your own policies or clone them to create new policies.

This chapter includes the following sections:

- Predefined Security Assertion Templates
- Predefined Management Assertion Templates

> **Note:** Oracle recommends that you do not edit the predefined assertion templates so that you will always have a known set of valid templates. You can, however, create a new assertion template from a predefined assertion template, or configure the attributes in an assertion after you have added it to a policy. For information about managing the assertion templates and adding them to policies, see "Managing Policy Assertion Templates" in *Administering Mobile Security Access Server*.

For a detailed description of the configuration settings in the tables, see Assertion Template Settings.

For a detailed description of the configuration properties listed in the tables, see Assertion Template Configuration Properties. For details on how to edit the configuration properties, see "Editing the Configuration Properties" in *Administering Oracle Mobile Security Access Server*. For information about overriding policy properties, see "Configuring Policy Overrides" in *Administering Oracle Mobile Security Access Server*.

Predefined Security Assertion Templates

This section describes the predefined security assertion templates that are provided with your MSAS installation and which are listed on the **Assertion Templates** page in the MSAS Console.

The tables in the following sections distinguish how the MSAS security assertion templates are documented in this release:

- MSAS Security Assertion Templates – summarizes new MSAS security assertion templates that are documented in this reference.

  Note: Some assertion templates are marked as ***internal*** because they are not available for attachment to URLs in applications.

- Security Assertion Templates Supported by MSAS – summarizes additional assertion templates that are supported by MSAS, but which are documented in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.
- Security Assertion Templates Reserved for Future Use – summarizes the assertion templates that appear in the MSAS Console, but which are reserved for future use with MSAS.

MSAS Security Assertion Templates

Table 2–1 summarizes the predefined MSAS security assertion templates listed on the **Assertion Templates** page in the MSAS Console, and which are documented in this reference.

Table 2–1 Predefined MSAS Security Assertion Templates

Assertion Template Name	Description
oracle/binding_oes_authorization_template	Performs user authorization based on the policy defined in Oracle Entitlements Server (OES) and provides fine-grained authorization on any operation on a web service.
oracle/http_action_over_ssl_template	Provides SKEK encryption and SKEK decryption.
oracle/http_bmax_jwt_user_token_client_template	Used for accessing JWT user token protected resources.
oracle/http_bmax_oam_client_template	Used for accessing OAM protected resources.
oracle/http_bmax_oauth_client_template	Injects an OAuth access token in the authorization header when accessing OAuth protected resources.
oracle/http_bmax_spnego_client_template	Used for HTTP SPNEGO authentication for negotiating with a back-end Kerberos service.
oracle/http_form_based_auth_over_ssl_service_template	**Internal** assertion template that performs HTML form-based authentication. This assertion can be attached to web applications (URLs).
oracle/http_kinit_over_ssl_template	Used for enabling Kerberos password authentication.
oracle/http_oam_authentication_service_template	Verifies if the web resource is protected via OAM, and if it is protected, then it authenticates using OAM and establishes the Subject before allowing access to the actual web resource.
oracle/http_oauth2_confidential_client_over_ssl_template	Performs OAuth2 confidential client authentication and creates OAuth and OAM tokens. This template is attached only on internal authentication endpoints.
oracle/http_oauth2_mobile_client_over_ssl_template	Performs OAuth2 mobile client authentication and creates OAuth and OAM tokens. This template is attached only on internal authentication endpoints.
oracle/http_ntlm_token_client_template	Performs NTLM (NT LAN Manager) authentication with NTLM protected applications. It requires a KINIT or PKINIT-based HTTP session token. This template can be attached to SOAP/REST services and also to web applications.
oracle/http_pkinit_over_ssl_template	Enables Kerberos PKI password authentication.
oracle/http_session_token_issue_template	**Internal** assertion template that issues a session token with the authenticated user ID.

Table 2–1 (Cont.) Predefined MSAS Security Assertion Templates

Assertion Template Name	Description
oracle/http_session_token_verify_template	Verifies the session token including the timestamp and signature, decrypts the encrypted data and asserts the identity using the user ID from the session token. The request is rejected if the verification fails.
oracle/http_tlp_over_ssl_template	Enables the Time Limited Password authentication.
oracle/inject_header_template	**Internal** assertion template that Injects a custom HTTP header with the client certificate received over two-way SSL.

Security Assertion Templates Supported by MSAS

Table 2–2 summarizes additional assertion templates that are supported by MSAS. For detailed descriptions, however, see "Predefined Assertion Templates" in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.

Table 2–2 Predefined Security Assertion Templates Supported by MSAS

Assertion Template	Description
oracle/http_jwt_token_client_template	Includes a JWT token in the HTTP header. The JWT token is created automatically. The issuer name and subject name are provided either programmatically or declarative through the policy. A policy created using this template can be attached to any HTTP-based client. You can specify the audience restriction condition using the configuration override property.
oracle/http_jwt_token_over_ssl_client_ template	Includes a JWT token in the HTTP header. The JWT token is created automatically. The issuer name and subject name are provided either programmatically or declarative through the policy. A policy created using this template can be attached to any HTTP-based client. You can specify the audience restriction condition using the configuration override property.
oracle/http_jwt_token_service_template	Authenticates users using the credentials provided in the JWT token in the HTTP header.
oracle/http_jwt_token_over_ssl_service_ template	Authenticates users using the username provided in the JWT token in the HTTP header.
oracle/http_saml20_token_bearer_client_ template	Includes SAML 2.0 tokens in outbound SOAP request messages. The SAML token with confirmation method Bearer is created automatically.
oracle/http_saml20_token_bearer_service_ template	Authenticates users using credentials provided in SAML tokens with confirmation method Bearer in the WS-Security SOAP header.
oracle/wss_http_token_client_template	Includes username and password credentials in the HTTP header. You can control whether one-way or two-way authentication is required.
oracle/wss_http_token_over_ssl_client_ template	Includes credentials in the HTTP header for outbound client requests and authenticates users against the Oracle Platform Security Services identity store.
oracle/wss_http_token_service_template	Uses the credentials in the HTTP header to authenticate users against the Oracle Platform Security Services identity store. You can control whether one-way or two-way authentication is required.
oracle/wss_http_token_over_ssl_service_ template	Extracts the credentials in the HTTP header and authenticates users against the Oracle Platform Security Services identity store.

Security Assertion Templates Reserved for Future Use

Table 2–3 summarizes the predefined MSAS security assertion templates that are listed in the **Assertion Templates** page, but which are reserved for future use.

Table 2–3 Predefined Security Assertion Templates Reserved for Future Use

Assertion Template Name	Description
oracle/binding_authorization_template	Reserved for future use.
oracle/binding_oes_masking_template	Reserved for future use.
oracle/binding_permission_authorization_template	Reserved for future use.
oracle/component_authorization_template	Reserved for future use.
oracle/component_oes_authorization_template	Reserved for future use.
oracle/component_permission_authorization_template	Reserved for future use.
oracle/http_oam_token_service_template	Reserved for future use.
oracle/http_oauth2_token_client_template	Reserved for future use.
oracle/http_oauth2_token_over_ssl_client_template	Reserved for future use.
oracle/http_spnego_token_client_template	Reserved for future use.
oracle/http_spnego_token_service_template	Reserved for future use.
oracle/oauth2_config_client_template	Reserved for future use.
oracle/pii_security_template	Reserved for future use.
oracle/security_log_template	Reserved for future use.
oracle/sts_trust_config_client_template	Reserved for future use.
oracle/sts_trust_config_service_template	Reserved for future use.
oracle/wss10_message_protection_client_template	Reserved for future use.
oracle/wss10_message_protection_client_template	Reserved for future use.
oracle/wss10_saml20_token_client_template	Reserved for future use.
oracle/wss10_saml20_token_service_template	Reserved for future use.
oracle/wss10_saml20_token_with_message_protection_client_template	Reserved for future use.
oracle/wss10_saml20_token_with_message_protection_service_template	Reserved for future use.
oracle/wss10_saml_hok_with_message_protection_client_template	Reserved for future use.
oracle/wss10_saml_hok_token_with_message_protection_service_template	Reserved for future use.
oracle/wss10_saml_token_client_template	Reserved for future use.
oracle/wss10_saml_token_service_template	Reserved for future use.
oracle/wss10_saml_token_with_message_protection_client_template	Reserved for future use.

Table 2–3 (Cont.) Predefined Security Assertion Templates Reserved for Future Use

Assertion Template Name	Description
oracle/wss10_saml_token_with_message_protection_service_template	Reserved for future use.
oracle/wss10_username_token_with_message_protection_client_template	Reserved for future use.
oracle/wss10_username_token_with_message_protection_service_template	Reserved for future use.
oracle/wss10_x509_token_with_message_protection_client_template	Reserved for future use.
oracle/wss10_x509_token_with_message_protection_service_template	Reserved for future use.
oracle/wss11_kerberos_token_client_template	Reserved for future use.
oracle/wss11_kerberos_token_service_template	Reserved for future use.
oracle/wss11_kerberos_token_with_message_protection_client_template	Reserved for future use.
oracle/wss11_kerberos_token_with_message_protection_service_template	Reserved for future use.
oracle/wss11_message_protection_client_template	Reserved for future use.
oracle/wss11_message_protection_client_template	Reserved for future use.
oracle/wss11_saml20_token_with_message_protection_client_template	Reserved for future use.
oracle/wss11_saml20_token_with_message_protection_service_template	Reserved for future use.
oracle/wss11_saml_token_with_message_protection_client_template	Reserved for future use.
oracle/wss11_saml_token_with_message_protection_service_template	Reserved for future use.
oracle/wss11_sts_issued_saml_hok_with_message_protection_client_template	Reserved for future use.
oracle/wss11_sts_issued_saml_hok_with_message_protection_service_template	Reserved for future use.
oracle/wss11_sts_issued_saml_with_message_protection_client_template	Reserved for future use.
oracle/wss11_username_token_with_message_protection_client_template	Reserved for future use.
oracle/wss11_username_token_with_message_protection_service_template	Reserved for future use.
oracle/wss11_x509_token_with_message_protection_client_template	Reserved for future use.
oracle/wss11_x509_token_with_message_protection_service_template	Reserved for future use.
oracle/wss_saml20_token_bearer_over_ssl_client_template	Reserved for future use.
oracle/wss_saml20_token_bearer_over_ssl_service_template	Reserved for future use.

Table 2–3 (Cont.) Predefined Security Assertion Templates Reserved for Future Use

Assertion Template Name	Description
oracle/wss_saml20_token_over_ssl_client_tpolicy	Reserved for future use.
oracle/wss_saml20_token_over_ssl_service_template	Reserved for future use.
oracle/wss_saml_token_bearer_client_template	Reserved for future use.
oracle/wss_saml_token_bearer_over_ssl_client_template	Reserved for future use.
oracle/wss_saml_token_bearer_over_ssl_service_template	Reserved for future use.
oracle/wss_saml_token_bearer_service_template	Reserved for future use.
oracle/wss_saml_token_over_ssl_client_template	Reserved for future use.
oracle/wss_saml_token_over_ssl_service_template	Reserved for future use.
oracle/wss_sts_issued_saml_bearer_token_over_ssl_client_template	Reserved for future use.
oracle/wss_sts_issued_saml_bearer_token_over_ssl_service_template	Reserved for future use.
oracle/wss_username_token_client_template	Reserved for future use.
oracle/wss_username_token_over_ssl_client_template	Reserved for future use.
oracle/wss_username_token_over_ssl_service_template	Reserved for future use.
oracle/wss_username_token_service_template	Reserved for future use.
oracle/xpath_token_auth_service_template	Reserved for future use.
oracle/xpath_username_auth_service_template	Reserved for future use.

oracle/binding_oes_authorization_template

Display Name: Binding OES Authorization Template

Category: Security

Type: oes-authorization

Description

The `binding_oes_authorization_template` assertion template performs user authorization based on the policy defined in Oracle Entitlements Server (OES) and provides fine-grained authorization on any operation on a web service. Authorization is based on attributes, current authenticated subject, and web service actions invoked by the client. This policy should follow an authentication policy where the subject is established, and can be attached to any SOAP-based or REST-based endpoint.

Settings

Table 2–4 lists the settings for the `binding_oes_authorization_template` assertion template.

Table 2–4 binding_oes_authorization_template Settings

Name	Default Value
OES Based Authorization	
Action Match	*
Constraint Match	
Resource Match	*

Configuration

Table 2–5 lists the default configuration properties and the default settings for the `binding_oes_authorization_template` assertion template.

Table 2–5 binding_oes_authorization_template Configuration Properties

Name	Default Value	Type
application.name	None	Optional
resource.type	None	Optional
resource.name	None	Optional
lookup.action	None	Optional
execute.action	None	Optional
use.single.step	None	Optional
reference.priority	None	Reserved for future use.

oracle/http_action_over_ssl_template

Display Name: HTTP Action Security Over SSL Template

Category: Security / Message Protection

Type: http-action-security

Description

The `http_action_over_ssl_template` assertion template provides SKEK encryption and SKEK decryption.

Settings

Table 2–6 lists the settings for the `http_action_over_ssl_template` assertion template.

Table 2–6 http_action_over_ssl_template Settings

Name	Default Value
Authentication Token	
Algorithm Suite	`Basic128`
Action Token	
Algorithm Suite	`Basic128`
Transport Layer Security	

Table 2–6 (Cont.) http_action_over_ssl_template Settings

Name	Default Value
Transport Layer Security	Disabled
Transport Layer Security—Include Timestamp	Disabled
Transport Layer Security—Mutual Authentication Required	Disabled

Configuration

Table 2–7 lists the default configuration properties and the default settings for the `http_action_over_ssl_template` assertion template.

Table 2–7 http_action_over_ssl_template Configuration Properties

Name	Default Value	Type
reference.priority	None	Reserved for future use.

oracle/http_bmax_jwt_user_token_client_template

Display Name: HTTP BMAX JWT User Token Client Template

Category: Security

Type: http-jwt-user-token-security

Description

The `http_bmax_jwt_user_token_client_template` assertion template is used for accessing JWT user token protected resources.

Settings

This assertion template does not have settings.

Configuration

Table 2–8 lists the default configuration properties and the default settings for the `http_bmax_jwt_user_token_client_template` assertion template.

Table 2–8 http_bmax_jwt_user_token_client_template Configuration Properties

Name	Default Value	Type
reference.priority	None	Reserved for future use

oracle/http_bmax_oam_client_template

Display Name: HTTP BMAX OAM Token Client Template

Category: Security

Type: http-oam-token-security

Description

The `http_bmax_oam_client_template` assertion template is used for accessing OAM protected resources.

Settings

This assertion template does not have settings.

Configuration

Table 2–9 lists the default configuration properties and the default settings for the `http_bmax_oam_client_template` assertion template.

Table 2–9 http_bmax_oam_client_template Configuration Properties

Name	Default Value	Type
reference.priority	None	Reserved for future use

oracle/http_bmax_oauth_client_template

Display Name: HTTP BMAX OAUTH Client Template

Category: Security

Type: http-oauth-token-security

Description

The `http_bmax_oauth_client_template` assertion injects an OAuth access token in the authorization header when accessing OAuth protected resources.

Settings

This assertion template does not have settings.

Configuration

Table 2–10 lists the default configuration properties and the default settings for the `http_bmax_oauth_client_template` assertion template.

Table 2–10 http_bmax_oauth_client_template Configuration Properties

Name	Default Value	Type
oauth2.client.csf.key	oauth2.confidential.client.credentials	Optional
oauth2.mobile.client.csf.key	oauth2.mobile.client.id	Optional
scopes	UserProfile.me UserProfile.users. UserProfile.groups	Required
reference.priority	None	Reserved for future use

oracle/http_bmax_spnego_client_template

Display Name: HTTP BMAX Spnego Client Template

Category: Security

Type: http-spnego-security

Description

The `http_bmax_spnego_client_template` assertion template is used for HTTP SPNEGO authentication for negotiating with a back-end Kerberos service.

Settings

This assertion template does not have settings.

Configuration

Table 2–11 lists the default configuration properties and the default settings for the `http_bmax_spnego_client_template` assertion template.

Table 2–11 http_bmax_spnego_client_template Configuration Properties

Name	Default Value	Type
service.principal.name	None	Optional
preemptive.auth	True	Optional
credential.delegation	None	Optional
reference.priority	None	Reserved for future use

oracle/http_form_based_auth_over_ssl_service_template

Display Name: HTTP Form Based Authentication Service Assertion Template

Category: Security

Type: form-based-auth

Description

The internal `http_form_based_auth_over_ssl_service_template` assertion template performs HTML form based authentication. This assertion can be attached to web applications (URLs).

Settings

Table 2–14 lists the settings for the `http_form_based_auth_over_ssl_service_template` assertion template.

Table 2–12 http_form_based_auth_over_ssl_service_template Settings

Name	Default Value
Transport Layer Security	
Transport Layer Security	Enabled
Transport Layer Security—Include Timestamp	Disabled
Transport Layer Security—Mutual Authentication Required	Disabled

Configuration

Table 2–15 lists the default configuration properties and the default settings for the `http_form_based_auth_over_ssl_service_template` assertion template.

Table 2–13 http_form_based_auth_over_ssl_service_template Configuration Properties

Name	Default Value	Type
username.field.name	j_username	Optional
password.field.name	j_username	Optional
login.error.page.url	None	Optional
login.page.url	None	Optional

oracle/http_kinit_over_ssl_template

Display Name: HTTP Kerberos Authentication Service Assertion Template

Category: Security

Type: http-kinit-security

Description

The `http_kinit_over_ssl_template` assertion template is used for enabling Kerberos password authentication.

Settings

Table 2–14 lists the settings for the `http_kinit_over_ssl_template` assertion template.

Table 2–14 http_kinit_over_ssl_template Settings

Name	Default Value
Authentication Token	
Algorithm Suite	`Basic128`
Transport Layer Security	
Transport Layer Security	Disabled
Transport Layer Security—Include Timestamp	Disabled
Transport Layer Security—Mutual Authentication Required	Disabled

Configuration

Table 2–15 lists the default configuration properties and the default settings for the `http_kinit_over_ssl_template` assertion template.

Table 2–15 http_kinit_over_ssl_template Configuration Properties

Name	Default Value	Type
keystore.sig.csf.key	None	Optional
reference.priority	None	Reserved for future use

oracle/http_ntlm_token_client_template

Display Name: HTTP NTLM Authentication Client Template

Category: Security

Type: http-ntlm-security

Description

The `http_ntlm_token_client_template` assertion template performs NTLM (NT LAN Manager) authentication with NTLM protected applications. It requires a KINIT or PKINIT-based HTTP session token. This template can be attached to SOAP/REST services and also to web applications.

Settings

This assertion template does not have settings.

Configuration

Table 2–16 lists the default configuration properties and the default settings for the `http_ntlm_token_client_template` assertion template.

Table 2–16 http_ntlm_token_client_template Configuration Properties

Name	Default Value	Type
service.principal.name	None	Optional
reference.priority	None	Reserved for future use

oracle/http_oam_authentication_service_template

Display Name: HTTP OAM Access Service Assertion Template

Category: Security

Type: http-oam-authentication-security

Description

The `http_oam_authentication_service_template` assertion template verifies if the web resource is protected via OAM, and if it is protected, then it authenticates using OAM and establishes the Subject before allowing access to the actual web resource.

Settings

Table 2–17 lists the settings for the `http_oam_authenication_service_template` assertion template.

Table 2–17 http_oam_authentication_service_template Settings

Name	Default Value
Authentication Header	
Authentication Header—Mechanism	`basic`

Configuration

Table 2–18 lists the default configuration properties and the default settings for the `http_oam_authentication_service_template` assertion template.

Table 2–18 http_oam_authentication_service_template Configuration Properties

Name	Default Value	Type
reference.priority	None	Reserved for future use

oracle/http_oauth2_confidential_client_over_ssl_template

Display Name: HTTP OAth2 Confidential Client Over SSL Template

Category: Security

Type: http-oauth2-confidential-client-security

Description

The `http_oauth2_confidential_client_over_ssl_template` assertion template performs OAuth2 confidential client authentication and creates OAuth and OAM tokens. This template is attached only on internal authentication endpoints.

Settings

Table 2–19 lists the settings for the `http_oauth2_mobile_client_over_ssl_template` assertion template.

Table 2–19 http_oauth2_confidential_client_over_ssl_template Settings

Name	Default Value
Authentication Token	
Algorithm Suite	`Basic128`
Transport Layer Security	
Transport Layer Security	Disabled
Transport Layer Security—Include Timestamp	Disabled
Transport Layer Security—Mutual Authentication Required	Disabled

Configuration

Table 2–20 lists the default configuration properties and the default settings for the `http_oauth2_confidential_client_over_ssl_template` assertion template.

Table 2–20 http_oauth2_confidential_client_over_ssl_template Configuration Properties

Name	Default Value	Type
oauth2.client.csf.key	oauth2.confidential.client.credentials	Required
reference.priority	None	Reserved for future use

oracle/http_oauth2_mobile_client_over_ssl_template

Display Name: HTTP OAMMS Mobile Client Token Over SSL Service Template

Category: Security

Type: http-oauth2-mobile-client-security

Description

The `http_oauth2_mobile_client_over_ssl_template` assertion template performs OAuth2 mobile client authentication and creates OAuth and OAM tokens. This template is attached only on internal authentication endpoints.

Settings

Table 2–21 lists the settings for the `http_oauth2_mobile_client_over_ssl_template` assertion template.

Table 2–21 http_oauth2_mobile_client_over_ssl_template Settings

Name	Default Value
Authentication Token	
Algorithm Suite	`Basic128`
Transport Layer Security	

Table 2–21 (Cont.) http_oauth2_mobile_client_over_ssl_template Settings

Name	Default Value
Transport Layer Security	Disabled
Transport Layer Security—Include Timestamp	Disabled
Transport Layer Security—Mutual Authentication Required	Disabled

Configuration

Table 2–22 lists the default configuration properties and the default settings for the `http_oauth2_mobile_client_over_ssl_template` assertion template.

Table 2–22 http_oauth2_mobile_client_over_ssl_template Configuration Properties

Name	Default Value	Type
oauth2.mobile.client.csf.key	oauth2.mobile.client.id	Required
reference.priority	None	Reserved for future use

oracle/http_pkinit_over_ssl_template

Display Name: HTTP Kerberos PKI Authentication Service Assertion Template

Category: Security

Type: http-pkinit-security

Description

The `http_pkinit_over_ssl_template` assertion template enables Kerberos PKI password authentication.

Settings

Table 2–23 lists the settings for the `http_pkinit_over_ssl_template` assertion template.

Table 2–23 http_pkinit_over_ssl_template Settings

Name	Default Value
Authentication Token	
Algorithm Suite	`Basic128`
Transport Layer Security	
Transport Layer Security	Disabled
Transport Layer Security—Include Timestamp	Disabled
Transport Layer Security—Mutual Authentication Required	Disabled

Configuration

Table 2–24 lists the default configuration properties and the default settings for the `http_pkinit_over_ssl_template` assertion template.

Table 2–24 http_pkinit_over_ssl_template Configuration Properties

Name	Default Value	Type
keystore.sig.csf.key	None	Optional
reference.priority	None	Reserved for future use

oracle/http_session_token_issue_template

Display Name: HTTP Session Token Issuance Template

Category: Security

Type: http-stoken-issue

Description

The `http_session_token_issue_template` assertion template issues a session token with the authenticated user ID.

Settings

Table 2–25 lists the settings for the `http_session_token_issue_template` assertion template.

Table 2–25 http_session_token_issue_template Settings

Name	Default Value
Session Token	
Algorithm Suite	`Basic128`

Configuration

Table 2–26 lists the default configuration properties and the default settings for the `http_session_token_issue_template` assertion template.

Table 2–26 http_session_token_issue_template Configuration Properties

Name	Default Value	Type
csf.map	None	Optional
keystore.sig.csf.key	None	Optional
keystore.enc.csf.key	None	Optional
reference.priority	None	Reserved for future use

oracle/http_session_token_verify_template

Display Name: HTTP Session Token Verification Template

Category: Security

Type: http-stoken-verify

Description

The `http_session_token_verify_template` assertion template verifies the session token including the timestamp and signature, decrypts the encrypted data and asserts the identity using the `userID` from the session token. The request is rejected if the verification fails.

Settings

Table 2–27 lists the settings for the `http_session_token_verify_template` assertion template.

Table 2–27 http_session_token_verify_template Settings

Name	Default Value
Session Token	
Algorithm Suite	`Basic128`

Configuration

Table 2–28 lists the default configuration properties and the default settings for the `http_session_token_verify_template` assertion template.

Table 2–28 http_session_token_verify_template Configuration Properties

Name	Default Value	Type
csf.map	None	Optional
keystore.sig.csf.key	None	Optional
keystore.enc.csf.key	None	Optional
assert.stoken.identity	false	Required

Note: For authorization policy scenarios, this property must be set to `true`. For information about overriding policy properties, see "Configuring Policy Overrides" in *Administering Oracle Mobile Security Access Server*.

oracle/http_tlp_over_ssl_template

Display Name: HTTP TLP Authentication Service Assertion Template

Category: Security

Type: http-tlp-security

Description

The `http_tlp_over_ssl_template` assertion template enables the Time Limited Password authentication.

Settings

Table 2–29 lists the settings for the `http_tlp_over_ssl_template` assertion template.

Table 2–29 http_tlp_over_ssl_template Settings

Name	Default Value
Authentication Token	
Algorithm Suite	`Basic128`
Transport Layer Security	
Transport Layer Security	Disabled
Transport Layer Security—Include Timestamp	Disabled
Transport Layer Security—Mutual Authentication Required	Disabled

Configuration

Table 2–30 lists the default configuration properties and the default settings for the `http_tlp_over_ssl_template` assertion template.

Table 2–30 http_tlp_over_ssl_template Configuration Properties

Name	Default Value	Type
reference.priority	None	Reserved for future use

oracle/inject_header_template

Display Name: Inject Header Template

Category: Security

Type: inject-header

Description

The `inject_header_template` assertion template injects a custom HTTP header with the client certificate received over two-way SSL.

Settings

This assertion template does not have settings.

Configuration

Table 2–31 lists the default configuration properties and the default settings for the `inject_header_template` assertion template.

Table 2–31 inject_header_template Configuration Properties

Name	Default Value	Type
http.header.name	None	Optional
http.header.value	None	Optional
reference.priority	None	Reserved for future use

oracle/xpath_token_auth_service_template

Display Name: XPath Based Token Authentication Assertion Template

Category: Security

Type: xpath-token-auth

> **Note:** This assertion template is reserved for future use.

Description

The `xpath_token_auth_service_template` assertion template provides XPath based token authentication service.

Settings

Table 2–32 lists the settings for the `xpath_token_auth_service_template` assertion template.

Table 2–32 xpath_token_auth_service_template Settings

Name	Default Value
Authentication Header	
Authentication Header—Mechanism	jwt
Is Signed	Enabled
Algorithm Suite	`Basic128Sha256Rsa15`
Is Encrypted	Disabled
Token Location XPath	
XPath Expression	
XPath Namespaces (comma separated)	

Configuration

Table 2–33 lists the default configuration properties and the default settings for the `xpath_token_auth_service_template` assertion template.

Table 2–33 xpath_token_auth_service_template Configuration Properties

Name	Default Value	Type
trusted.issuers	None	Optional
keystore.sig.csf.key	None	Optional
propagate.identity.context	None	Optional
reference.priority	None	Reserved for future use

oracle/xpath_username_auth_service_template

Display Name: XPath Based Username/Password Authentication Assertion Template

Category: Security

Type: xpath-username-auth

> **Note:** This assertion template is reserved for future use.

Description

The `xpath_username_auth_service_template` assertion template provides XPath based username/password authentication service.

Settings

Table 2–34 lists the settings for the `xpath_token_username_service_template` assertion template.

Table 2–34 xpath_username_auth_service_template Settings

Name	Default Value
XPath to Username	
XPath Expression	None
XPath Namespaces (comma separated)	None

Table 2–34 (Cont.) xpath_username_auth_service_template Settings

Name	Default Value
XPath to Password	
XPath Expression	None
XPath Namespaces (comma separated)	None

Configuration

Table 2–35 lists the default configuration properties and the default settings for the `xpath_username_auth_service_template` assertion template.

Table 2–35 xpath_username_auth_service_template Configuration Properties

Name	Default Value	Type
reference.priority	None	Reserved for future use

Predefined Management Assertion Templates

This section describes the predefined management assertion templates defined for the current release.

Table 2–36 summarizes the management assertion templates.

Table 2–36 Management Assertion Templates

Name	Description
oracle/security_log_template	Provides a logging assertion template that can be attached to any binding or component.

oracle/security_log_template

Display Name: Security Log Assertion Template

Category: Security

Type: Logging

> **Note:** This assertion template is reserved for future use.

Description

The `security_log_template` assertion template provides a logging assertion template that can be attached to any binding or component.

Settings

Table 2–37 lists the settings for the `security_log_template` assertion template.

Table 2–37 security_log_template Settings

Name	Default Value
Logging	
Request	all
Response	soap_body
Fault	Not set

Configuration

Table 2–38 lists the configuration properties and the default settings for the `security_log_template` assertion template.

Table 2–38 security_log_template Properties

Name	Default Value	Type
reference.priority	None	Reserved for future use

3

Assertion Template Settings and Configuration Properties

This chapter provides details on all the assertion template settings and configuration properties.

This chapter includes the following sections:

Assertion Template Settings

The following sections summarize the settings that can be set for the predefined assertion templates; settings are listed alphabetically.

> **Note:** Not all settings apply to all assertion templates.

Action Match

Action or web service operation for which authorization checks are performed. This value can be a comma-separated list of values. This field accepts wildcards.For example, `validate,amountAvailable`.

Algorithm Suite

Algorithm suite used for message protection. See "Supported Algorithm Suites" in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.

Authentication Header—Header Name

Name of the authentication header.

Authentication Header—Mechanism

Authentication mechanism.

Valid values include:

- `basic`—Client authenticates itself by transmitting the username and password.

  Note: It is recommended that you configure SSL when using basic authentication. For more information, see "Configuring the SSL Keystore and Truststore" in *Administering Oracle Mobile Security Access Server*.

- `cert`—**Not supported in this release**. Client authenticates itself by transmitting a certificate.
- `custom`—**Not supported in this release**. Custom authentication mechanism.
- `digest`— **Not supported in this release**. Client authenticates itself by transmitting an encrypted password through the use of an MD5 digest.
- `jwt`—Client authenticates itself using JWT token.
- `oam`—Client authenticates itself using OAM agent.
- `oauth2`—Client authenticates itself using OAuth2 agent.
- `saml20-bearer`—Client authenticates itself using SAML 2.0 Bearer token.
- `spnego`—Client authenticates itself using Kerberos SPNEGO.

Constraint Match

Expression that represents the constraints against which authorization checks are performed. The constraints expression is specified using the following two `messageContext` properties:

- `messageContext.authenticationMethod`—Determines the authentication method used to authenticate the user. Valid value is SAML_SV.
- `messageContext.requestOrigin`—Determines whether the request originated from an internal or external network. This property is valid only when using Oracle HTTP Server and the Oracle HTTP server administrator has added a custom VIRTUAL_HOST_TYPE header to the request.

The constraint pattern properties and their values are case sensitive.

The constraint expression uses the following standard supported operators: ==, !=, &&, || and !.

Is Encrypted

Flag that specifies whether the SAML token is encrypted.

Is Signed

Flag that specifies whether the SAML token is signed.

Resource Match

Name of the resource for which authorization checks are performed. This field accepts wildcards.For example, if the namespace of the web service is `http://project11` and the service name is `CreditValidation`, the resource name is `http://project11/CreditValidation`.

Transport Layer Security

Flag that specifies whether Secure Socket Layer (SSL), otherwise known as Transport Layer Security (TLS), is enabled.

Transport Layer Security—Include Timestamp

Flag that specifies whether to include a timestamp. A timestamp can be used to prevent replay attacks by identifying an expiration time after which the message is no longer valid.

Transport Layer Security—Mutual Authentication Required

Flag that specifies whether two-way authentication is required.

Valid values include:

- Enabled—The service must authenticate itself to the client, and the client must authenticate itself to the service.
- Disabled—One-way authentication is required. The service must authenticate itself to the client, but the client is not required to authenticate itself to the service.

XPath Expression

Reserved for future use.

XPath Namespaces (comma separated)

Reserved for future use.

Assertion Template Configuration Properties

The following sections summarize the configuration properties that can be set for the predefined assertion templates; settings are listed alphabetically.

> **Note:** Not all configuration properties apply to all assertion templates.

application.name

The application name defined in OES. Value can be static or dynamic that uses ${} notation.

assert.stoken.identity

Flag that specifies whether to assert the user against the identity store. The default value is `false`, which means the user is not asserted against the identity store during STOKEN verification. This flag must be set it to `true` if the authorization policy is attached after the STOKEN verification policy.

credential.delegation

Flag that specifies whether Credential Delegation with Forwarded TGT is supported. This value is false by default.

csf.map

Reserved for future use.

execute.action

Optional property. Action that will be used during real authorization. Value can be static or dynamic that uses ${} notation.

Fault

Requirements for logging fault messages. The valid values are:

- all—Log the entire SOAP message.
- header—Log SOAP header information only.
- soap_body—Log SOAP body information only.
- soap_envelope—Log SOAP envelope information only.

http.header.name

Name of the HTTP header to be inserted into outgoing HTTP headers to back-end resources.

http.header.value

Value of the HTTP header to be inserted into outgoing HTTP headers to back-end resources.

keystore.enc.csf.key

The alias and password used for storing the decryption key password in the keystore.

If you set this value you then can override `keystore.enc.csf.key`, as described in "Configuring Policy Overrides" in *Administering Oracle Mobile Security Access Server*.

If you do override this value, the key for the new value must be in the keystore. That is, overriding the value does not free you from the requirement of configuring the key in the keystores.

keystore.sig.csf.key

The alias and password used for storing the signature key password in the keystore. This property allows you to specify the signature key on a per-attachment level instead of at the domain level. This key is used when generating the enveloping signature, as specified using `saml.envelope.signature.required` flag.

login.error.page.url

Name of the login error page file for example: `login_error.html`. This is required to display an error message when authentication failed.

login.page.url

Login page relative URL.

lookup.action

Optional property. Action that will be used during attributes lookup. Value can be static or dynamic that uses ${} notation.

oauth2.client.csf.key

The OAuth2 confidential client ID and secret used for performing OAuth2 confidential client authentication with the OAM Mobile and Social Service.

If you set this value, you can override the `oauth2.client.csf.key`, as described in "Configuring Policy Overrides" in *Administering Oracle Mobile Security Access Server*.

If you override this value, the OAuth2 confidential client ID and secret for the new value must be in the client profile. That is, even if you override the value, you still need to configure the required OAuth2 confidential client profile in the OAM Mobile and Social Service.

oauth2.mobile.client.csf.key

The OAuth2 mobile client ID used for performing OAuth2 mobile client authentication with the OAM Mobile and Social Service.

If you set this value, you can override the `oauth2.mobile.client.csf.key`, as described in "Configuring Policy Overrides" in *Administering Oracle Mobile Security Access Server*.

If you override this value, the OAuth2 mobile client for the new value must be in the client profile. That is, even if you override the value, you still need to configure the required OAuth2 mobile client profile in the OAM Mobile and Social Service.

password.field.name

Name of the password field in login HTML page.

preemptive.auth

Flag that specifies whether to perform preemptive authentication with back-end resources. The default value is `true` in the `http_bmax_spnego_client_policy`. This property is not supported in multitoken client policies.

propagate.identity.context

Reserved for future use.

reference.priority

Reserved for future use.

Request

Requirements for logging request messages.

The valid values are:

- all—Log the entire SOAP message.
- header—Log SOAP header information only.
- soap_body—Log SOAP body information only.
- soap_envelope—Log SOAP envelope information only.

Response

Requirements for logging response messages. The valid values are the same as for Request.

resource.name

Optional property. Resource name defined in OES. Value can be static or dynamic that uses ${} notation.

resource.type

Optional property. Resource type defined in OES. Value can be static or dynamic that uses ${} notation.

scopes

OAuth scopes is a way to control access to resources. The value of **scopes** is expressed as a list of space-delimited, case sensitive strings.

service.principal.name

Kerberos principal name that identifies the service.

trusted.issuers

Reserved for future use.

username.field.name

Name of the username field in login HTML page.

use.single.step

Optional property. Set value to `true` to skip lookup phase. Does not apply to masking policy.