

eHF Authorization

Web Service Documentation

Web Service Documentation

Web Service Documentation Version 1.0 | Status Approved
Security Level Public

Imprint

InterComponentWare AG
Industriestraße 41
69190 Walldorf, Germany
Tel.: +49 (0) 6227 385 0
Fax: +49 (0) 6227 385 199

Document Version: 1.0
Document Language: en (US)
Security Level: Public

Last change on: 9/22/2008
Editorial Staff: BAS

Table of Contents

1	Authorization Web Service Terminology	5
1.1	Permission	5
1.2	Predefined Permission Profile	5
1.3	Target	5
1.4	Principal	6
1.5	Domain	6
1.6	Permission Assignment	6
2	Overview	7
2.1	Web service Description:	7
2.2	Usage Notes:	7
3	Main method parameters:	8
3.1	Impl:Domain	8
3.2	Impl:Principal	8
3.3	Impl:Assignment	8
3.4	Impl:PermissionsReference	10
3.5	Impl:Permission	10
3.6	Impl:DateRange	11
3.7	Impl:Target	11
4	Main Method Description	12
4.1	getAssignmentOverviews	12
4.1.1	getAssignments	12
4.1.2	getAssignment	13
4.1.3	setAssignment	14
4.1.4	addAssignment	15
4.1.5	removeAssignment	16
4.1.6	deleteAssignment	17
4.1.7	deleteAssignments	18
4.1.8	getPermissionsReferences	19

4.1.9	getPermissions	19
4.1.10	getMetadata	20

1 Authorization Web Service Terminology

1.1 Permission

A Permission object represents an access right to a protected system resource. eHF Authorization is specifically designed to support instance-based authorization, where protected resources are typically instances of domain objects. Nevertheless a permission in eHF Authorization can be used to represent any access right to any protected resource.

1.2 Predefined Permission Profile

A predefined permission profile represents a fixed collection of *Permissions* that is given a unique name within a category. Multiple versions of a predefined permission profile can be defined in the system. Hence, a predefined permission profile can be uniquely referenced via a combination of its name, its category along with a version. A version of a predefined permission profile can be in one of two states: active or deprecated. Only one active version of a predefined permission profile can exist in the system at a specific point in time. Also, only the currently active version of a predefined permission profile can be assigned.

1.3 Target

Represents the target resource of a permission. The target provides several descriptors to specify the target resource. It is up to the business application to make sense of the values of the target descriptors.

In the case of instance-based authorization, the descriptors specify the target object's class, the (UML) classifier role, the context of the target object and the target object's identifier. A wildcard string can be assigned to each of these descriptors. Hence, a target is defined in terms of

- a target classifier (a class name, for example)
- a target identifier (a class instance identifier, for example)
- a classifier role (can be thought of a UML classifier role)
- a context (an arbitrary context name)

Each of these descriptors are supporting wildcards. Please note that there is no constraint on the descriptors values. Again, it is the responsibility of the application using eHF Authorization to interpret the descriptors values.

1.4 Principal

Principal is a term defined by Java Security. A *Principal* represents a user or a role for example.

1.5 Domain

The concept of a domain in the context of eHF Authorization is used to indicate, respectively to localize a specific set of protected resources. For example, in the context of instance-based authorization, which is realized by eHF Authorization, the protected resources are instances of objects. To determine a domain in this case, the domain is extracted from the status of these object instances. That way, the status of an object instance binds this object instance to a specific domain.

The domain that is specified in a permission assignment, binds all access rights of this permission assignment to object instances that belong to that domain.

1.6 Permission Assignment

A permission assignment grants one or more permissions to a principal. A permission assignment is bound to the specified domain. eHF Authorization supports permissive and restrictive permission assignments.

2 Overview

2.1 Web service Description:

The Authorization Web Service (aka. Permission Manager Web Service) allows you to create new permission assignments, to manage these permission assignments and to query permission assignments that are persisted in the eHF authorization database.

2.2 Usage Notes:

Creating a new permission assignment

Creating a new permission assignment means to grant access rights to a *Principal*.

To create a new permission assignment, use the *setAssignment* method. The *Assignment* parameter of this method describes which permissions are granted as well as who gets granted these permissions. The granted permissions come in two flavours.

First, you can assign predefined permission profiles. In this case set the *PermissionReference* array attribute of the *Assignment* parameter.

Second, you can assign a custom profile. In this case set the *Permission* array attribute of the *Assignment* parameter. Currently it is not possible to assign predefined profiles and a custom profile at the same time.

Deleting permission assignments

Using the *deleteAssignment* methods you can delete permission assignments from the eHF authorization database.

Querying permission assignments

Various *getAssignment* methods provide the ability to query the eHF authorization database using different search criteria specified by the method parameters.

Updating permission assignments

The authorization web service does not provide an explicit update method. Instead, the *setAssignment* method does override assignments that already exist for this principal/domain.

3 Main method parameters:

Parameter	Description
Impl:Domain	The domain where the permission assignments are granted on.
Impl:Principal	The principal to which the permission assignment is granted.
Impl:Assignment	The permission assignment. Specifies the permission profile(s) that are granted, the <i>Principal</i> which gets granted the permission profiles and the domain.
Impl:PermissionsReference	The predefined permission profile.

3.1 Impl:Domain

Attribute	Description	Type
id	uniquely identifies the <i>Domain</i>	xsd:string

3.2 Impl:Principal

Attribute	Description	Type
id	uniquely identifies the <i>Principal</i>	xsd:string

3.3 Impl:Assignment

Attribute	Description	Type
permissions-References	The predefined profiles of this assignment. Predefined profiles represent a fixed collection of <i>Permissions</i> that are referenced as a whole via a name and a category.	ArrayOfPermissionsReference

permissions	The <i>Permissions</i> of this assignment. A <i>Permission</i> object represents an access right. A <i>Permission</i> consists of a target (e.g. a domain object type or a group of domain object types) and a set of actions that are allowed on these targets (e.g. create, update, delete, etc.)	ArrayOfPermission
domain	The <i>Domain</i> of this assignment. A <i>Domain</i> can be used to specify a group of domain object instances for example. That way, all access rights are bound to domain object instances of this <i>Domain</i> .	impl:Domain
principal	The <i>Principal</i> which has been granted the access rights of this <i>Assignment</i> . A <i>Principal</i> can represent a role or a user of the system for example.	impl:Principal
dateRange	The <i>DateRange</i> of this assignment. The <i>DateRange</i> defines the start date and the end date of the validity of this assignment. The start date as well as the end data can be null respectively. Null values represent assignments that are unlimited in time.	Impl:DateRange
permissionsStale	<i>True</i> if this <i>Assignment</i> is currently in a stale state. Stale means, that at least one <i>PermissionReference</i> in this <i>Assignment</i> has been changed after this <i>Assignment</i> object has been created. An application using eHF can use this information to initiate a re-load of this <i>Assignment</i> object.	xsd:boolean

restriction	<i>True</i> if this <i>Assignment</i> represents a restriction. A restriction defines restrictive permissions. In other words, a restriction specifies that the <i>Principal</i> of this <i>Assignment</i> explicitly does not have the access rights defined by the permissions contained in this <i>Assignment</i> . A restriction cannot be overwritten by another <i>Assignment</i> with permissive access rights. In other words a restrictive <i>Assignment</i> always overrules a permissive <i>Assignment</i> . If this method returns true, then this <i>Assignment</i> represents permissive access rights.	xsd:boolean
locked	<i>True</i> if this <i>Assignment</i> is locked. A locked <i>Assignment</i> is currently not enabled. This locking mechanism can be used to temporarily disable an <i>Assignment</i> .	xsd:boolean

3.4 Impl:PermissionsReference

Attribute	Description	Type	Range
category	The category of this predefined profile.	xsd:string	
name	The name of this predefined profile.	xsd:string	
Version	The version of the predefined profile	xsd:string	
Status	The status of this version of the predefined profile	xsd:string	“ACTIVE” or “DEPRE-CATED”

3.5 Impl:Permission

Attribute	Description	Type	Range
target	The <i>Target</i> object of this <i>Permission</i> .	impl:Target	

actions	The <i>Actions</i> that are granted by this <i>Permission</i> .	ArrayOfAction	
---------	---	---------------	--

3.6 Impl:DateRange

Attribute	Description	Type	Range
fromDate	The start date of this time interval. The start date is included in the interval.	xsd:dateTime	
toDate	The end date of this time interval. The end date is included in the interval	xsd:dateTime	

3.7 Impl:Target

Attribute	Description	Type	Range
type	The type classifier of this <i>Target</i> object. The type classifier is typically (but not necessarily) a fully qualified class name or a package name.	xsd:string	
role	The role classifier of this <i>Target</i> . The role classifier is typically (but not necessarily) an UML role.	xsd:string	
context	The context classifier of this <i>Target</i> object. If it is necessary to distinguish targets of the same type in different business use cases (or contexts) then the context classifier can be used for this purpose.	xsd:string	
identifier	The identifier classifier of this <i>Target</i> object. The identifier classifier is typically (but not necessarily) the identifier value of an object instance.	xsd:string	

4 Main Method Description

4.1 getAssignmentOverviews

Description:

Finds all permission assignments granted to principals of the specified type on the specified domain. The method returns only assignments overviews. That means the permission arrays of the returned assignment objects are empty.

Arguments:

Parameter	Description	Data Type	Usage	Default
domain	The domain where the permission assignments are granted on.	impl:Domain	R	
principal- Qualifier	The qualified name of the principal type to which permission assignments are granted.	xsd:QName	R	

Returns:

Description	Data Type
An array containing the found permission assignment overviews. If no permission assignments are found, then an empty array is returned.	impl:Assignment

4.1.1 getAssignments

Description:

Finds all permission assignments granted to principals of the specified type on the specified domain.

Arguments:

Parameter	Description	Data Type	Usage	Default
domain	The domain where the permission assignments are granted on.	impl:Domain	R	
principal-Qualifier	The qualified name of the principal type to which permission assignments are granted.	xsd:QName	R	

Returns:

Description	Data Type
An array containing the found permission assignments.	impl:Assignment

4.1.2 getAssignment

Description:

Finds the permission assignment granted to the specified principal on the specified domain.

Arguments:

Parameter	Description	Data Type	Usage	Default
domain	The domain where the permission assignment is granted on.	impl:Domain	R	
principal	The principal to which the permission assignment is granted.	impl:Principal	R	

Returns:

Description	Data Type
The found permission assignment.	impl:Assignment

4.1.3 setAssignment

Description:

Creates a new permission assignment. Existing assignments for the same *Principal* on the same domain are overwritten by this method. Mixing custom permissions and predefined profiles in one assignment is not allowed. Only active versions of predefined profiles are allowed.

Arguments:

Parameter	Description	Data Type	Usage	Default
assignment	The permission assignment. Specifies the permission profile(s) that are granted, the <i>Principal</i> which/who gets granted the permission profiles and the domain.	impl:Assignment	R	

Error codes/Exceptions:

Besides the common errors and exception, the following errors may occur:

Error code/Exception	Reason
IllegalArgumentException	The principal is null in the Assignment parameter
IllegalArgumentException	The assignment contains a custom profile and predefined profiles. Mixing a custom profile with predefined profiles in one assignment is not allowed.
IllegalArgumentException	Start date is not before end date
IllegalArgumentException	The version of the predefined profile is deprecated

AccessControlException	Assignment is already expired (can be configured)
AccessControlException	Assignment contains more than one predefined profile (can be configured)
AccessControlException	Current user is not allowed to grant one ore more of the permissions in the predefined profile
AccessControlException	Current user is not allowed to grant a permission in a custom profile
AccessControlException	Unknown predefined profile
AccessControlException	Empty predefined profiles

4.1.4 addAssignment

Description:

Adds a permission assignment to an existing assignment for the principal and the domain. Predefined profiles of the given assignment are added to the set of predefined profiles of the existing assignment. Custom permissions of the given assignment are added to the set of custom permissions of the existing assignment. Mixing custom permissions and predefined profiles in one assignment is not allowed. Only active versions of predefined profiles are allowed.

If no assignment exists for the principal and the domain, then a new assignment is created.

Arguments:

Parameter	Description	Data Type	Usage	Default
Assignment	the permission assignment. Specifies the permission profile(s) or the custom permissions that are added to an existing assignment for the principal and the domain.	impl:Assignment	R	

Error codes/Exceptions:

Besides the common errors and exception, the following errors may occur:

Error code/Exception	Reason
IllegalArgumentException	The principal is null in the Assignment parameter
IllegalArgumentException	The assignment contains a custom profile and predefined profiles. Mixing a custom profile with predefined profiles in one assignment is not allowed.
IllegalArgumentException	Start date is not before end date
IllegalArgumentException	The version of the predefined profile is deprecated
AccessControlException	Assignment is already expired (can be configured)
AccessControlException	Assignment contains more than one predefined profile (can be configured)
AccessControlException	Current user is not allowed to grant one ore more of the permissions in the predefined profile
AccessControlException	Current user is not allowed to grant a permission in a custom profile
AccessControlException	Unknown predefined profile
AccessControlException	Empty predefined profiles
IllegalStateException	Adding a predefined profile to an assignment with a custom profile is not allowed (and vice versa)

4.1.5 removeAssignment

Description:

Removes a permission assignment from an existing assignment for the principal and the domain. Predefined profiles of the given assignment are removed from the set of predefined profiles of the existing assignment. Custom permissions of the given assignment are removed from the set of custom permissions of the existing assignment. Removing custom permissions from predefined profiles is not allowed (and vice versa).

If no predefined profile and no custom permission remains after the remove operation, then assignment is deleted.

Arguments:

Parameter	Description	Data Type	Usage	Default
Assignment	the permission assignment. Specifies the permission profile(s) or the custom permissions that are removed from an existing assignment for the principal and the domain.	impl:Assignment	R	

Error codes/Exceptions:

Besides the common errors and exception, the following errors may occur:

Error code/Exception	Reason
IllegalArgumentException	The principal is null in the Assignment parameter
IllegalArgumentException	The assignment contains a custom profile and predefined profiles. Mixing a custom profile with predefined profiles in one assignment is not allowed.
IllegalArgumentException	Start date is not before end date
AccessControlException	Current user is not allowed to revoke one or more of the permissions in the predefined profile
AccessControlException	Current user is not allowed to revoke a permission in a custom profile
IllegalStateException	Removing a predefined profile from an assignment with a custom profile is not allowed (and vice versa)

4.1.6 deleteAssignment

Description:

Deletes the permission assignment that is granted to the specified principal on the specified domain.

Arguments:

Parameter	Description	Data Type	Usage	Default
domain	The domain where the permission assignment is granted on.	impl:Domain	R	
principal	The principal to which the permission assignment is granted.	impl:Principal	R	

Error codes/Exceptions:

Besides the common errors and exception, the following errors may occur:

Error code/Exception	Reason
AccessControlException	Current user is not allowed to delete the assignment

4.1.7 deleteAssignments

Description:

Deletes all permission assignments that are granted to the specified principal.

Arguments:

Parameter	Description	Data Type	Usage	Default
principal	The principal to which the permission assignments are granted.	impl:Principal	R	

Error codes/Exceptions:

Besides the common errors and exception, the following errors may occur:

Error code/Exception	Reason
AccessControlException	Current user is not allowed to delete the assignment

4.1.8 getPermissionsReferences

Description:

Finds all predefined permission references in the eHF authorization database.

Returns:

Description	Data Type
An array containing all predefined permission profiles.	impl:PermissionsReference

4.1.9 getPermissions

Description:

Returns all permissions defined in the predefined profile that matches the given profile reference parameter. If the profile contains no permissions or if no profile matches the given reference parameter, then an empty array is returned.

Arguments:

Parameter	Description	Data Type	Usage	Default
reference	The predefined permission profile.	impl:PermissionsReference	R	

Returns:

Description	Data Type
An array with all permissions that the predefined profile contains.	impl:Permission

Error codes/Exceptions:

Besides the common errors and exception, the following errors may occur:

Error code/Exception	Reason
----------------------	--------

IllegalArgumentException	the reference parameter is ambiguously defined, which means that the given reference parameter matches to more than one predefined profile
--------------------------	--

4.1.10 getMetadata

Description:

Returns the meta data for the type specified by the given qualified name.

Arguments:

Parameter	Description	Data Type	Usage	Default
classQualifier	The qualified name of the type.	xsd:QName	R	

Returns:

Description	Data Type
The meta data of the type.	impl:ClassMetaData

