identity-management

Service Description

Abstract
This document provides service description for the **identity-management** service.

Contents

1 Overview

This document describes the **identity-management** service, which enables systems (with operator role or proper permissions) to handle (create, update, remove, query) identities and active sessions (close, query) in bulk. An example of this interaction is when an operator uses the Management Tool to add access to different systems manually.

The **identity-management** service contains the following operations:

- *identity-mgmt-query* lists the identities that match the filtering requirements;
- *identity-mgmt-create* creates the specified identities;
- *identity-mgmt-update* updates the specified existing identities;
- *identity-mgmt-remove* removes the specified identities;
- *identity-mgmt-session-query* lists the active sessions that match the filtering requirements;
- *identity-mgmt-session-close* closes (invalidates) the specified active sessions;

The rest of this document is organized as follows. In Section 2, we describe the abstract message operations provided by the service. In Section 3, we end the document by presenting the data types used by the mentioned operations.

1.1 How This Service Is Meant to Be Used

The service's purpose is to handle the systems' identities and sessions centrally and in bulk. If a Local Cloud supports outsourced authentication, using this service is the only option to make possible for a system to be the part of the Local Cloud.

Application systems should not use this service; only operators (via the Management Tool, for example) or dedicated support systems.

1.2 Important Delimitations

The requester has to identify itself to use any of the operations.

1.3 Access policy

The service is only available for operators, dedicated support systems and those who have the proper authorization rights to consume it.

2 Service Operations

This section describes the abstract signatures of each operation of the service. In particular, each subsection names an operation, an input type, and one or two output types (unsuccessful operations can return different structure), in that order. The input type is named inside parentheses, while the output type is preceded by a colon. If the operation has two output types, they are separated by a slash. Input and output types are only denoted when accepted or returned, respectively, by the operation in question. All abstract data types named in this section are defined in Section 3.

2.1 operation identity-mgmt-query (IdentityQueryRequest) : IdentityListResponse / ErrorResponse

The query data must meet the following criteria:

- The operation returns results in pages. There are default page data settings, but the requester can provide a custom specification.
- If page number is specified, the page size must be specified as well and vice versa.
- In some Local Clouds there is a maximum page size.
- There is an AND relation between different kind of filters.
- If both boundaries about creation time is specified, the resulted time interval cannot be empty.

2.2 operation identity-mgmt-create (IdentityListCreateRequest) : IdentityListResponse / ErrorResponse

The creation data must meet the following criteria:

- Authentication method should come from a predefined set. The content of this set is implementation-specific.
- System names are case insensitive and have to be unique within the Local Cloud.
- System names can contain maximum 63 character of letters (english alphabet), numbers and dash (-), and have to start with a letter (also cannot end with dash).
- The requirements of credential map is based on the authentication method, so the related criteria are implementation-specific.
- Multiple identities can be created at once, but it is forbidden to specify systems with the same name.
- It is forbidden to create an identity that is already registered into the Local Cloud.

2.3 operation identity-mgmt-update (IdentityListUpdateRequest) : IdentityListResponse / ErrorResponse

The update data must meet the following criteria:

- System names are case insensitive and have to be unique within the Local Cloud.
- System names can contain maximum 63 character of letters (english alphabet), numbers and dash (-), and have to start with a letter (also cannot end with dash).
- The requirements of credential map is based on the authentication method, so the related criteria are implementation-specific.
- Multiple identities can be updated at once, but it is forbidden to specify systems with the same name.
- All identities must use the same authentication method.
- It is not possible to update an identity that is not registered into the Local Cloud.

2.4 operation identity-mgmt-remove (IdentityListRemoveRequest) : OperationStatus / ErrorResponse

2.5 operation identity-mgmt-session-query (IdentitySessionQueryRequest) : IdentitySessionListResponse / ErrorResponse

The query data must meet the following criteria:

- The operation returns results in pages. There are default page data settings, but the requester can provide a custom specification.
- If page number is specified, the page size must be specified as well and vice versa.
- In some Local Clouds there is a maximum page size.
- There is an AND relation between different kind of filters.
- If both boundaries about login time is specified, the resulted time interval cannot be empty.

2.6 operation identity-mgmt-session-close (IdentitySessionListCloseRequest) : OperationStatus / ErrorResponse

3 Information Model

Here, all data objects that can be part of the **identity-management** service are listed and must be respected by the hosting System. Note that each subsection, which describes one type of object, begins with the *struct* keyword, which is used to denote a collection of named fields, each with its own data type. As a complement to the explicitly defined types in this section, there is also a list of implicit primitive types in Section 3.15, which are used to represent things like hashes and identifiers.

3.1 struct IdentityQueryRequest

Field	Type	Mandatory	Description
authentication	Identity	yes	The requester of the operation.
pageNumber	Number	no (yes)	The number of the requested page. It is mandatory, if page size is specified.
pageSize	Number	no (yes)	The number of entries on the requested page. It is mandatory, if page number is specified.
pageSortField	String	no	The identifier of the field which must be used to sort the entries.
pageDirection	Direction	no	The direction of the sorting.
namePart	String	no	Requester is looking for identities with system names containing the specified text.
isSysop	Boolean	no	Requester is looking for identities that have/do not have higher level administration rights depending of the specified value.
createdBy	Name	no	Requester is looking for identities that have been created by the specified identity.
creationFrom	DateTime	no	Requester is looking for identities that were created after the specified time.
creationTo	DateTime	no	Requester is looking for identities that were created before the specified time.
hasSession	Boolean	no	Requester is looking for identities that have/do not have active session at the moment

3.2 struct Identity

An Object which describes the identity of a system. It also contains whether the identified system has higher level administrative rights.

3.3 struct IdentityListResponse

Field	Type	Description
status	OperationStatus	Status of the operation.
identities	List<IdentityResult>	A page of identities.
count	Number	Total number of identities that match the filters.

3.4 struct IdentityResult

Field	Type	Description
systemName	Name	Unique identifier of the identified system.
authenticationMethod	AuthenticationMethod	The authentication method the identity uses.
sysop	Boolean	Determines whether the identified system has higher level administration rights or not.
createdBy	Name	The identity was created by this identified system.
createdAt	DateTime	Identity was created at this timestamp.
updatedBy	Name	The identity was modified by this identified system.
updatedAt	DateTime	Identity was modified at this timestamp.

3.5 struct ErrorResponse

Field	Type	Description
status	OperationStatus	Status of the operation.
errorMessage	String	Description of the error.
errorCode	Number	Numerical code of the error.
type	ErrorType	Type of the error.
origin	String	Origin of the error.

3.6 struct IdentityListCreateRequest

Field	Type	Mandatory	Description
authentication	Identity	yes	The requester of the operation.
authenticationMethod	AuthenticationMethod	yes	The authentication method all the identities use.
identities	List<IdentityRequest>	yes	A list of identities.

3.7 struct IdentityRequest

Field	Type	Mandatory	Description
systemName	Name	yes	Unique identifier of the identifiable system.
credentials	Credentials	yes	Authentication method-specific credential information of the system.
sysop	Boolean	no	Determines whether the identifiable system has higher level administration rights or not.

3.8 struct Credentials

An Object which maps String keys String values.

3.9 struct IdentityListUpdateRequest

Field	Type	Mandatory	Description
authentication	Identity	yes	The requester of the operation.
identities	List<IdentityRequest>	yes	A list of identities.

3.10 struct IdentityListRemoveRequest

Field	Type	Mandatory	Description
authentication	Identity	yes	The requester of the operation.
names	List<Name>	yes	Names of the identities that need to be removed.

3.11 struct IdentitySessionQueryRequest

Field	Type	Mandatory	Description
authentication	Identity	yes	The requester of the operation.
pageNumber	Number	no (yes)	The number of the requested page. It is mandatory, if page size is specified.
pageSize	Number	no (yes)	The number of entries on the requested page. It is mandatory, if page number is specified.
pageSortField	String	no	The identifier of the field which must be used to sort the entries.
pageDirection	Direction	no	The direction of the sorting.

namePart	String	no	Requester is looking for active sessions of systems with names containing the specified text.
loginFrom	DateTime	no	Requester is looking for active sessions that were created after the specified time.
loginTo	DateTime	no	Requester is looking for active sessions that were created before the specified time.

3.12 struct IdentitySessionListResponse

Field	Type	Description
status	OperationStatus	Status of the operation.
sessions	List<IdentitySessionResult>	A page of sessions.
count	Number	Total number of sessions that match the filters.

3.13 struct IdentitySessionResult

Field	Type	Description
systemName	Name	Unique identifier of the identified system.
loginTime	DateTime	Session was created at this timestamp.
expirationTime	DateTime	Session will expire at this timestamp.

3.14 struct IdentitySessionListCloseRequest

Field	Type	Mandatory	Description
authentication	Identity	yes	The requester of the operation.
names	List<Name>	yes	Names of the identities whose session must be closed.

3.15 Primitives

Types and structures mentioned throughout this document that are assumed to be available to implementations of this service. The concrete interpretations of each of these types and structures must be provided by any IDD document claiming to implement this service.

Type	Description
AuthenticationMethod	A string representation of an authentication method chosen by the implementor of service.
Boolean	One out of true or false.
DateTime	Pinpoints a specific moment in time.
Direction	The direction of a sorting operation. Possible values are the representation of ascending or descending order.
ErrorType	Any suitable type chosen by the implementor of service.
List<A>	An *array* of a known number of items, each having type A.
Name	A string identifier that is intended to be both human and machine-readable.
Number	Decimal number.
Object	Set of primitives and possible further objects.
OperationStatus	Logical, textual or numerical value that indicates whether an operation is a success or a failure. Multiple values can be used for success and error cases to give additional information about the nature of the result.
String	A chain of characters.

4 References

5 Revision History

5.1 Amendments

No.	Date	Version	Subject of Amendments	Author
1	YYYY-MM-DD	5.0.0		Xxx Yyy

5.2 Quality Assurance

No.	Date	Version	Approved by
1	YYYY-MM-DD	5.0.0	