Directory schema

OID hierarchy used in the core schema:

`1.3.6.1.4.1.43192.1.1 - Core schema`
`1.3.6.1.4.1.43192.1 - LDAP`
`1.3.6.1.4.1.43192 - Enterprise OID (AIGSG)`

AIGSG-Object (object.ldif)

Abstract class containing common object attributes. All directory entries processed by the Event Server should either subclass AIGSG-Object or use one of its subclasses as an auxiliary class.

AIGSG-ObjectId

Attribute containing hex-encoded 64-bit object ID in the following format: "{0123456789abcdef}".

Event Server automatically generates ID for each newly created object within the directory tree, so this attribute is optional and shouldn't be set manually.

AIGSG-ObjectClass

Class name of the object, e.g. "device.access.MagneticLock". This attribute is mandatory.

AIGSG-ObjectOwner

DN of the object's owner, which can be an user or a group. Permission check is bypassed for owners of the object. This attribute is optional.

AIGSG-ObjectPolicy

DN of the policy object associated with this object. Object can have multiple policies associated with it. See AIGSG-Policy for details.

AIGSG-ObjectDisabled

Allows to temporarily exclude object from the processing without deleting it. Note that value of the attribute is never checked, so object is considered to be disabled once it has this attribute assigned, regardless of its actual value.

If some client had active session with the server at the time its object was disabled, the session will be aborted and further authentication attempts will be rejected until client's object is enabled again.

Setting "AIGSG-ObjectDisabled" attribute for top-level object disables all lower-level objects as well.

AIGSG-ObjectArea

Client-specific text data describing object position on a location plan (see AIGSG-LocationPlan).

AIGSG-User (user.ldif)

Auxiliary class describing user objects. This class should be added to existent user entries within the LDAP tree, such as 'user' objects in Active Directory.

System attributes User-Principal-Name and SAM-Account-Name are queried to get system name of the user. User entry should be bindable for client to be authenticated against LDAP by the Event Server.

AIGSG-Settings

User settings in the following format:

```
param_1 = value_1;
param_2 = value_2;
...
```

Settings are parsed by the Event Server and delivered to its clients as typed name-value pairs (see devapi.Obj and userapi.Obj in the protocol definition).

AIGSG-Group (user.ldif)

Auxiliary class describing user group objects. This class should be added to existent group entries within the directory tree, such as *group* objects in Active Directory.

System attribute *member* is queried by the Event Server to get member entries of the group. Nested groups are supported.

AIGSG-Device (device.ldif)

Structural class describing device objects.

AIGSG-SerialNumber

Device serial number. This attribute is mandatory.

AIGSG-Settings

Device settings. See AIGSG-User for the format details.

AIGSG-Service (service.ldif)

Structural class describing service objects.

AIGSG-Settings

Service settings. See AIGSG-User for the format details.

AIGSG-Sensor, AIGSG-Actuator (sensor.ldif)

Structural classes describing sensors and actuators (i.e. "writable" sensors) respectively. All sensors should be subobjects of their devices or services.

AIGSG-SerialNumber

Sensor's serial number. This attribute is optional.

AIGSG-Settings

Sensor settings. See AIGSG-User for the format details.

AIGSG-Script (script.ldif)

Structural class describing scripts. Scripts can be device or service-local, i.e. represented as subobjects of devices or services.

AIGSG-ScriptSource

Source code of the script in Lua language.

AIGSG-Settings

Script settings. Settings are parsed by the Event Server and provided to the script as regular Lua table, accessible via `script.this()` function. See AIGSG-User for the format details.

AIGSG-Location (location.ldif)

Auxiliary class describing units of the organization or georgraphical locations. This class should be added to existent organizational unit entries within the directory tree.

AIGSG-LocationPlan

Client-specific binary data containing location plan.

AIGSG-Policy (policy.ldif)

Object policy. All user permissions and event handling settings are policy-based, where policies applied to top-level objects have priority over policies applied to lower-level objects. For example, consider the following organization structure:

```
Organization (location object, class: location.Organization)
  Office (location object, class: location.Building)
    John Doe (user object, class: User)
    Entrance Door (device object, class: device.door.Entrance)
    Vault Door (device object, class: device.door.Vault)
    ...
```

If some permission is explicitly denied for user John Doe at "Organization" level (via policy object associated with this location object), it remains denied for this user regardless of all lower-level policies, even if the same permission is explicitly allowed at the "Office" level; and vice-versa: explicitly allowed permissions cannot be withdrawn by another policies applied to lower-level objects.

AIGSG-PolicyMember

DN of the policy member, which can be an user or a group. Policy can have multiple members. All users of policy's member groups are considered to be members of the respective policy.

AIGSG-PolicyAllowObject, AIGSG-PolicyDenyObject

White- (AIGSG-PolicyAllowObject) and blacklist (AIGSG-PolicyDenyObject) of object class names to which the policy can be applied. Wildcard matching is supported, for example:

```
AIGSG-PolicyAllowObject:
   device.door.*
AIGSG-PolicyDenyObject:
   device.door.Vault
```

Applies policy to all "door" devices except vault doors.

AIGSG-PolicyAllowEvent, AIGSG-PolicyDenyEvent

White- (AIGSG-PolicyAllowEvent) and blacklist (AIGSG-PolicyDenyEvent) of event class names processed by the policy. Wildcard matching is supported.

Consider following policy settings are applied to `ou=Organization` entry in the above example:

```
AIGSG-PolicyAllowObject:
   device.door.*
AIGSG-PolicyDenyObject:
   device.door.Vault
AIGSG-PolicyAllowEvent:
   event.door.Open
   event.door.Close
   event.door.Opened
   event.door.Closed
AIGSG-PolicyMember:
   cn=John Doe,ou=Office,ou=Organization
```

User John Doe is allowed to send event.door.Open and event.door.Close control events directly to all door devices in the office except vault doors. He's also allowed to receive event.door.Opened and event.door.Closed signal events from the same devices (i.e. excluding vault doors).

AIGSG-PolicyScript

DN of the script which should be executed when signal event passes through the policy filters. Multiple scripts can be associated with the policy.