Projection Policy

This feature was called "Account Synchronization Settings" in midPoint versions 2.1 and earlier.

Assignment Policy Enforcement

There are several ways how accounts can be provisioned and managed:

- Link accounts to users (link)
- Assign accounts to user directly or using roles. (assignment)

There is a major difference between these two approaches from the policy point of view. The **links** describe actual situation (what *is*) while **assignments** describe the policy (what *should be*). This is discussed in detail in Assigning vs Linking.

There are many ways how to resolve the difference between the policy (assignments) and reality. Assignment enforcement modes are used to control this part of midPoint behaviour. The goal of enforcement modes is to determine account *legality* of projections. I.e. midPoint computes whether the specific account (or any other *projection*) is legal or illegal. An account is legal if there is a valid assignment for it or if an enforcement mode allows it. E.g. in FULL enforcement mode the account is legal only if there is a valid assignment. In NONE enforcement mode the account is legal anytime it exists regardless of the assignments.

The legality of the account is then used by the activation mechanism to determine what to do with the account. The activation usually deals with illegal accounts and determines whether to delete the account, disable it or do any other action.

Operation and Migration

The questionable part is what to do in reality (links) do not conform to the policy (assignments). Maybe the most obvious answer to that question would be to fix the reality: create missing accounts, delete surplus accounts, correct the links. That is usually expected from a working IDM system. But the IDM system that is just being deployed is quite different. The "business first" mantra usually applies when the system is being deployed. It means that the impact of the IDM deployment on the business should be minimized. Therefore the IDM system usually tolerates policy violations during its deployment and early life. Especially if the policies are just beginning to form and there are a lot of violations that need to be addressed manually one by one. In such early phases the system usually only reports the current situation, allows to fix it but it is not enforcing the policies.

Enforcement Options

The enforcement of assignments can be managed in system global configuration. This applies to the whole system (all resources and accounts). The individual enforcement options for resources will be provided later.

The options are:

- **none**: No enforcement of assignments. The assignments will be ignored.
- **positive**: Assignments will be enforced only in a positive manner. Unassigning of account will not remove it. If a non-existing account is assigned it will be created. If existing account is not assigned it will NOT be removed.
- **relative** (default): The same as "positive", with one exception: if an account is assigned and user request unassignment of the account, it will be deleted. Existing accounts that are not assigned will NOT be removed.
- **full**: Full enforcement of assignments. Non-existent assigned accounts will be created, existent unassigned accounts will be deleted, etc.
- **mark**: Policy violations will be marked for manual processing. **NOT YET IMPLEMENTED**

Legalization

If "legalize" is set to true then the illegal resource objects (e.g. accounts) will be made legal. Illegal resource object is a linked resource object for which there is no assignment. If this option is set to true then it will automatically add a (direct) assignment for this object. Default is false.

Configuration

The projection policy can be configured at several layers:

- System configuration: the setting applies to all objects and all cases unless they are overridden
- Resource: the setting applies to all objects in that specific resource. Overrides system configuration
- Resource Schema Handling per objectType definition. Overrides resource and system configuration.

The options can be set in System Configuration object as illustrated by following example:

```
<systemConfiguration oid="00000000-0000-0000-0000-000000000001">
    <name>SystemConfiguration</name>
        <metadata>...</metadata>
    <globalAccountSynchronizationSettings>
        <assignmentPolicyEnforcement>full</assignmentPolicyEnforcement>
    </globalAccountSynchronizationSettings>
</systemConfiguration>
```

The option can be set in resource definition:

```
<resource>
    ...
    <projection>
        <assignmentPolicyEnforcement>positive</assignmentPolicyEnforcement>
        <legalize>true</legalize>
    </projection>
    ...
</resource>
```