Implementing Forefront Identity Manager 2010

Student Manual

Module 7: Group Management

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

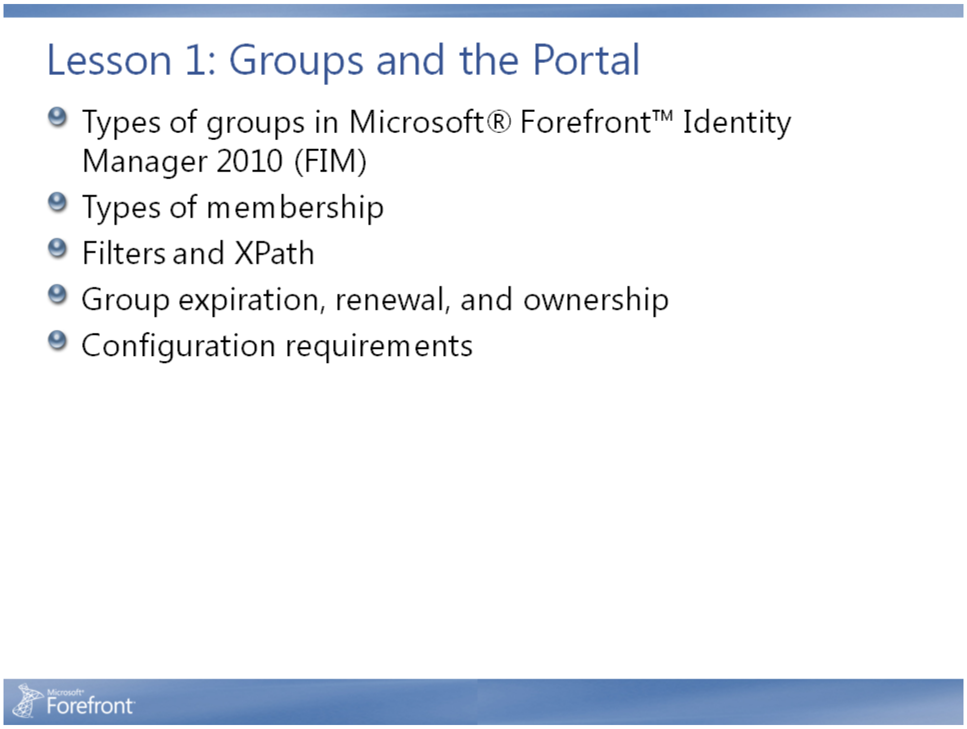
Table of Contents

Module 7: Group Management

Module Overview

This module deals with all the types of groups in Microsoft® Forefront™ Identity Manager (FIM), and some approaches to synchronizing them with Active Directory® (AD).

Lesson 1: Groups and the Portal



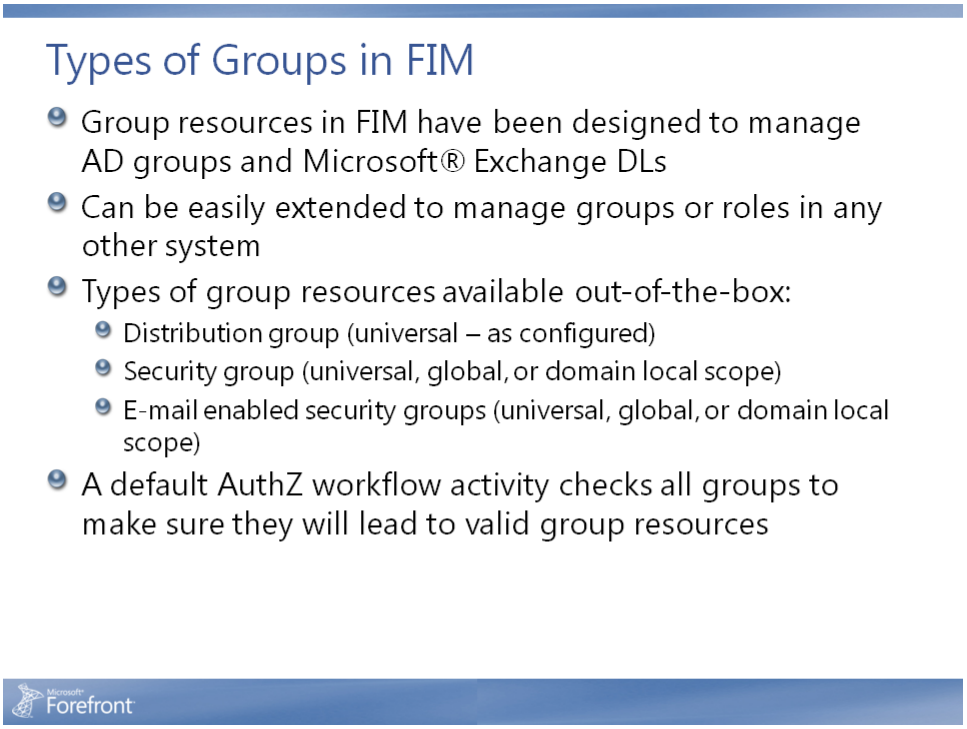
Lesson 1: Groups and the Portal

- Types of groups in Microsoft® Forefront™ Identity Manager 2010 (FIM)
- Types of membership
- Filters and XPath
- Group expiration, renewal, and ownership
- Configuration requirements

In this lesson we discuss the types of groups that the FIM portal provides. Out-of-the-box groups are oriented towards AD, and although it is possible to reconfigure groups to support other directory requirements, this lesson (and indeed, this course) focuses on the out-of-the-box features.

The lesson considers the different types of membership, and additional portal configuration. It introduces filters, and how XPath can be used for more complicated filters. It also deals with concepts such as group expiration, renewal, and ownership.

Types of Groups in FIM



Types of Groups in FIM

- Group resources in FIM have been designed to manage AD groups and Microsoft® Exchange DLs
- Can be easily extended to manage groups or roles in any other system
- Types of group resources available out-of-the-box:
    - Distribution group (universal – as configured)
    - Security group (universal, global, or domain local scope)
    - E-mail enabled security groups (universal, global, or domain local scope)
- A default AuthZ workflow activity checks all groups to make sure they will lead to valid group resources

By default, group resources are oriented towards AD, and it has been made easy to manage AD groups and Exchange Distribution Lists (DLs) without further modification. However, the schema can easily be extended to provide additional attributes required by other connected systems, or even to create new group-like resource types. The Resource Control Display Configuration (RCDC) of groups could also be modified to allow for different requirements.

There are three types of out-of-the-box group resources and you will have already seen examples of some of these in Module 1:

- Distribution group – The scope is set to Universal, although it is up to you whether you map this to a Universal or Global scope in Active Directory (see next lesson).
- Security groups – Universal, Global, or Domain Local scope.
- E-mail enabled security groups – Universal, Global, or Domain Local scope.

Although distribution groups and security groups are visualized differently in the portal (with the latter including a check box for E-mail Enabled), they are all represented in the same group resource type, with the type attribute being set to either Security, MailenabledSecurity, or Distribution.

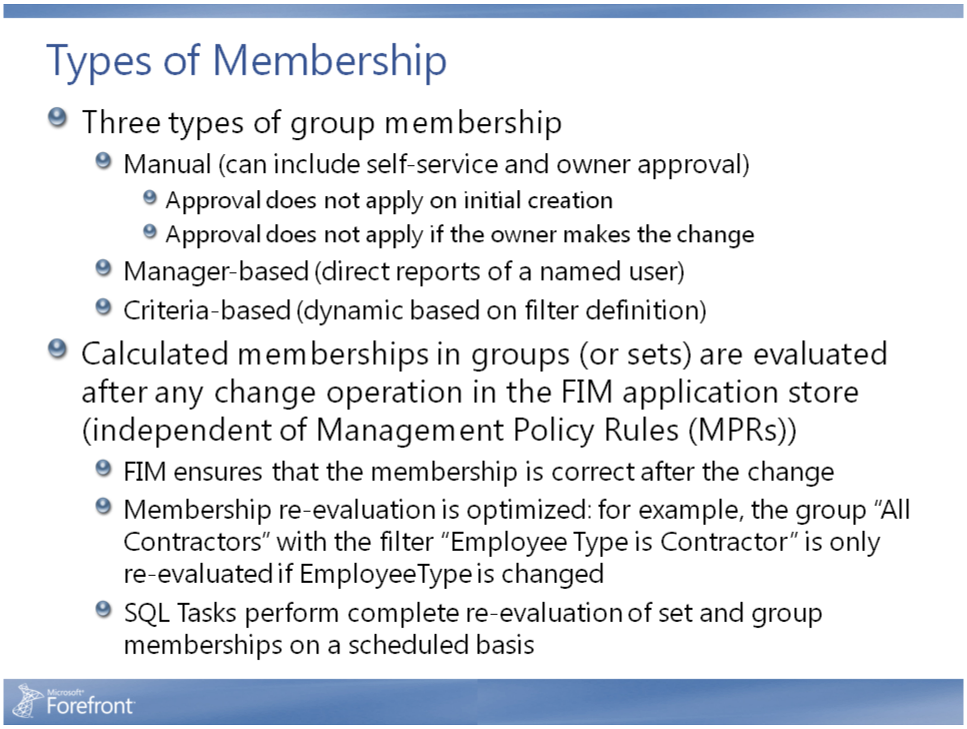
The scope attribute is set to either Domain Local, or Global, or Universal, with the RCDC restricting distribution groups to Universal.

As configured, a default Group Validation workflow activity checks all groups to make sure they will lead to valid group objects. Two Management Policy Rules (MPRs) (one for static groups and the other for dynamic groups) run the workflow whenever anyone modifies certain group attributes (for example, membership, scope, type). The workflow fails (and does not authorize the update) if various checks fail, including:

- Whether an explicit member is being added to a dynamically calculated group.
- Whether the resultant group would not correspond to a valid AD group based on, for example, group type, membership.
- Whether AD rules for multiple forest requirements would be broken.

All of this is configurable in principle (although we do not cover it here as it is a subject for a more advanced course).

Types of Membership



Types of Membership

- Three types of group membership
  - Manual (can include self-service and owner approval)
    - Approval does not apply on initial creation
    - Approval does not apply if the owner makes the change
  - Manager-based (direct reports of a named user)
  - Criteria-based (dynamic based on filter definition)
- Calculated memberships in groups (or sets) are evaluated after any change operation in the FIM application store (independent of Management Policy Rules (MPRs))
  - FIM ensures that the membership is correct after the change
  - Membership re-evaluation is optimized: for example, the group "All Contractors" with the filter "Employee Type is Contractor" is only re-evaluated if EmployeeType is changed
  - SQL Tasks perform complete re-evaluation of set and group memberships on a scheduled basis

There are three types of out-of-the-box group membership:

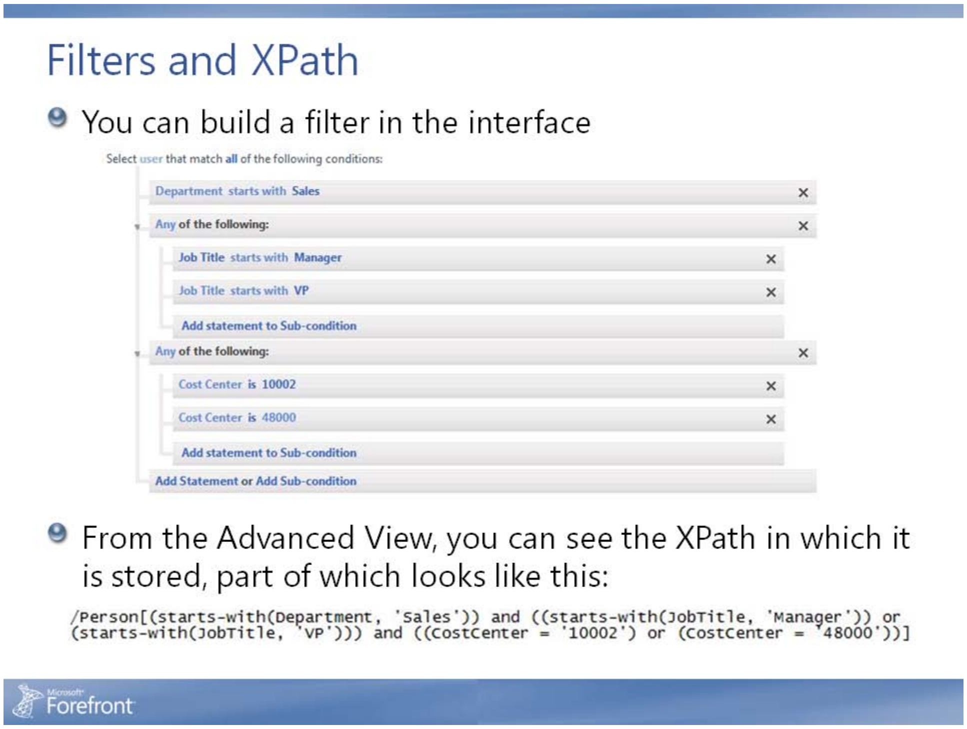
- Manual – As you have seen, members can be selected in the portal, or via Microsoft® Office Outlook® 2007, and may require owner approval.
- Manager-based – Automatic membership of all those reporting to a particular manager (including the manager).
- Criteria-based – Automatic membership based on a filter condition.

Calculated memberships of groups (or sets) are evaluated after any change operation in the FIM application store (independent of MPRs). FIM ensures that the membership is correct after the change.

FIM optimizes the membership re-evaluation by only recalculating the groups' memberships affected by the change, for example, the group All Contractors with the filter Employee Type is Contractor is not going to be re-evaluated every time a telephone number is changed, but will be if Employee Type is changed.

In case of any logical nesting or timing issues that might cause inconsistencies in group memberships, there is a scheduled SQL task (FIM_MaintainGroupsJob) which runs twice a day at 9:00 A.M. and 5:00 P.M. (by default) to recalculate all group memberships. (A similar task, FIM_MaintainSetsJob, runs much more often to check that Sets are appropriately populated).

Filters and XPath



Filters and XPath

- You can build a filter in the interface

Select user that match all of the following conditions:

- Department starts with Sales ×
- Any of the following: ×
  - Job Title starts with Manager ×
  - Job Title starts with VP ×
  - Add statement to Sub-condition
- Any of the following: ×
  - Cost Center is 10002 ×
  - Cost Center is 48000 ×
  - Add statement to Sub-condition
- Add Statement or Add Sub-condition

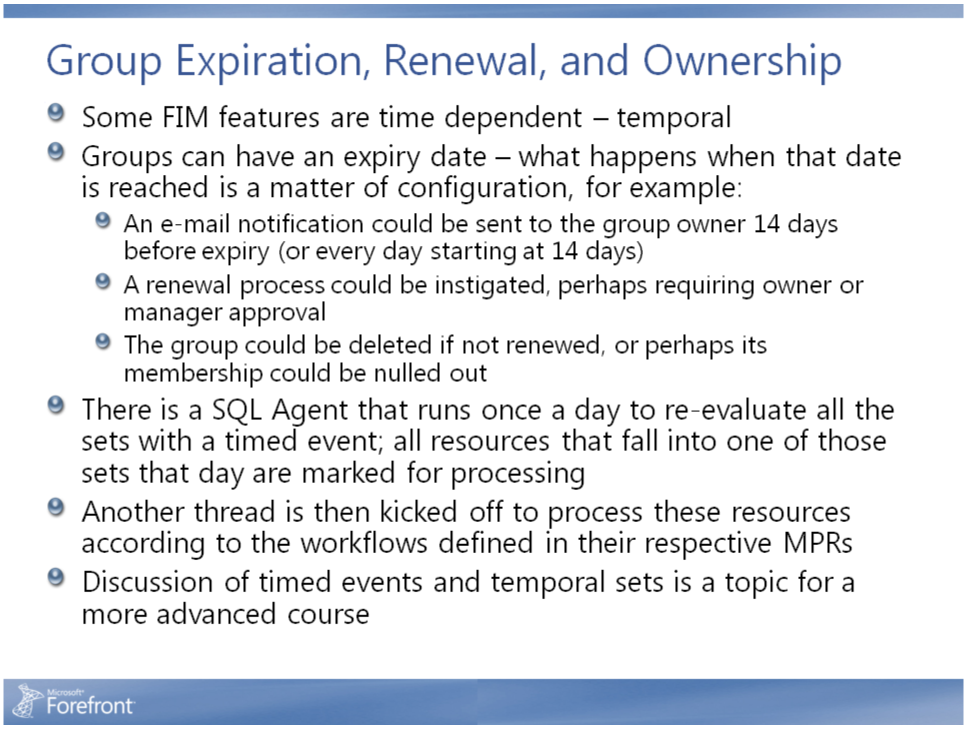
- From the Advanced View, you can see the XPath in which it is stored, part of which looks like this:

```
/Person[(starts-with(Department, 'Sales')) and ((starts-with(JobTitle, 'Manager')) or
(starts-with(JobTitle, 'VP'))) and ((CostCenter = '10002') or (CostCenter = '48000'))]
```

You can build a filter using the Query Builder in the UI. This allows reasonably sophisticated filters to be built by power users. Such filters are actually stored as XPath, which can then be viewed using the Advanced View.

The filter shown in the picture above results in XPath, which (minus some general stuff) looks like that also shown above. This is pretty easy to follow in this case, and you could extend it if you like (with care!). You can use this idea as a way of learning a little about XPath. Much more sophisticated filters can be built using XPath directly. See the XPath Filter Language Reference in http://msdn.microsoft.com/en-us/library/ee652287(VS.100).aspx.

Group Expiration, Renewal, and Ownership



Group Expiration, Renewal, and Ownership

- Some FIM features are time dependent – temporal
- Groups can have an expiry date – what happens when that date is reached is a matter of configuration, for example:
  - An e-mail notification could be sent to the group owner 14 days before expiry (or every day starting at 14 days)
  - A renewal process could be instigated, perhaps requiring owner or manager approval
  - The group could be deleted if not renewed, or perhaps its membership could be nulled out
- There is a SQL Agent that runs once a day to re-evaluate all the sets with a timed event; all resources that fall into one of those sets that day are marked for processing
- Another thread is then kicked off to process these resources according to the workflows defined in their respective MPRs
- Discussion of timed events and temporal sets is a topic for a more advanced course

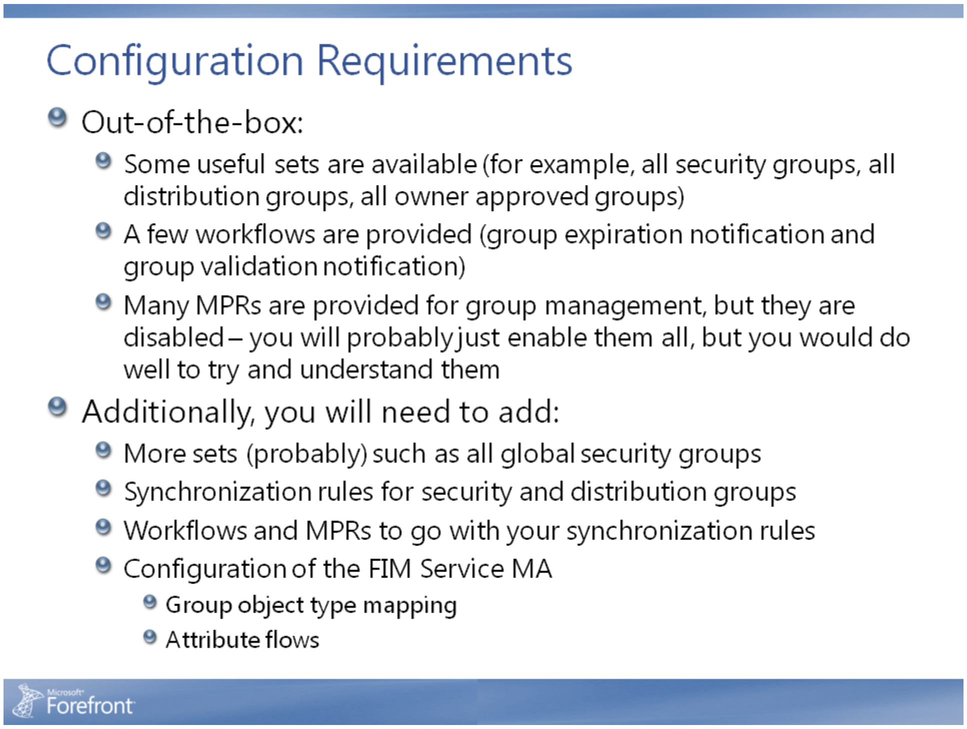
Some FIM features are time-dependent (temporal). For example, groups can have an expiry date and what happens when that date is reached is a matter of configuration:

- An e-mail notification could be sent to the group owner 14 days before expiry.
- A renewal process could be instigated, perhaps requiring owner or manager approval.
- The group could be deleted if not renewed, or perhaps its membership could be nulled out.

There is an SQL Agent Job (FIM_TemporalEventsJob) that runs once a day at 1:00 A.M. (by default) to re-evaluate all the sets with a timed event. All objects that fall into one of those sets that day are marked for processing. Another thread is then kicked off to process these objects according to the workflows defined in their respective MPRs.

Further discussion of timed events and temporal sets is a topic for a more advanced course.

Configuration Requirements



Configuration Requirements

- Out-of-the-box:
  - Some useful sets are available (for example, all security groups, all distribution groups, all owner approved groups)
  - A few workflows are provided (group expiration notification and group validation notification)
  - Many MPRs are provided for group management, but they are disabled – you will probably just enable them all, but you would do well to try and understand them
- Additionally, you will need to add:
  - More sets (probably) such as all global security groups
  - Synchronization rules for security and distribution groups
  - Workflows and MPRs to go with your synchronization rules
  - Configuration of the FIM Service MA
    - Group object type mapping
    - Attribute flows

Out-of-the-box Sets, Workflows, and MPRs for Managing Groups

You will find around 20 sets relating to groups, including All Security Groups, All Distribution Groups, All Owner Approved Groups, and All Expiring Groups (this last one has the criterion Expiration Time prior to 14 days from today).

Several workflows are also related to groups. For example:

- Group Expiration Notification – Sends an e-mail message to the owner of the target of an MPR (presumably a group!)
- Group Validation – Checks all groups to make sure they will lead to valid group objects.
- Requestor Validation With/Without Owner Authorization – A pair of workflows that allow an owner to make updates (without having to go through an authorization process).

Many MPRs are provided for group management, but they are disabled. You will probably just enable them all, but you would do well to try and understand them as you do so:

- Most of them grant permissions to owners, users, and administrators, and do not run workflows.
- A few of them trigger the workflows above.

Example:

The MPR **Temporal policy workflow: Impending group resource expiry notification** triggers the **Group Expiration Notification** workflow when a resource gets added to the **Expiring Group Resources** set. Groups join the set when they are within 14 days of expiring, and that is tested at 1:00 A.M. every day by a Microsoft® SQL Server® Agent. Thus a group owner is sent an e-mail message 14 days before the group expires. What happens when the group actually expires is another matter. You could include the expiration time in the definition of the set to decide which groups should be synchronized, and so deprovision the expired groups.

Additional Configuration

Synchronization Rules

You will probably need more sets, such as All Global Security Groups, All Universal Groups. You will also need synchronization rules, associated workflows, and MPRs for each MA that will be involved in provisioning.

Configuration of the FIM Service MA

You will need to select **Group** as one of your object types, and include attributes such as **Member**. You will map the CS object type group to a suitable metaverse (MV) object (group, presumably). You will need some import and export attribute flows.

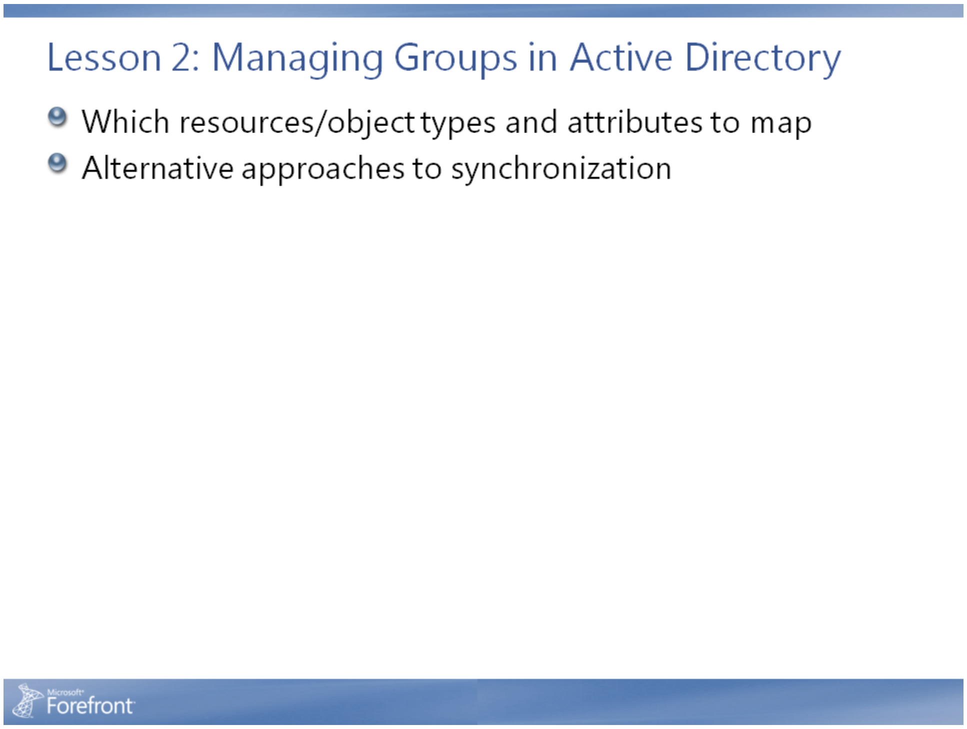
Typical Import Attribute Flows are:

Data Source Attribute	Metaverse Attribute
AccountName	accountName
DisplayedOwner	displayedOwner
DisplayName	displayName
ExpectedRulesList	expectedRulesList
MailNickname	mailNickname
Member	member

Typical Export Attribute Flows are:

Data Source Attribute	Metaverse Attribute
email	mail
DetectedRulesList	DetectedRulesList

Lesson 2: Managing Groups in Active Directory

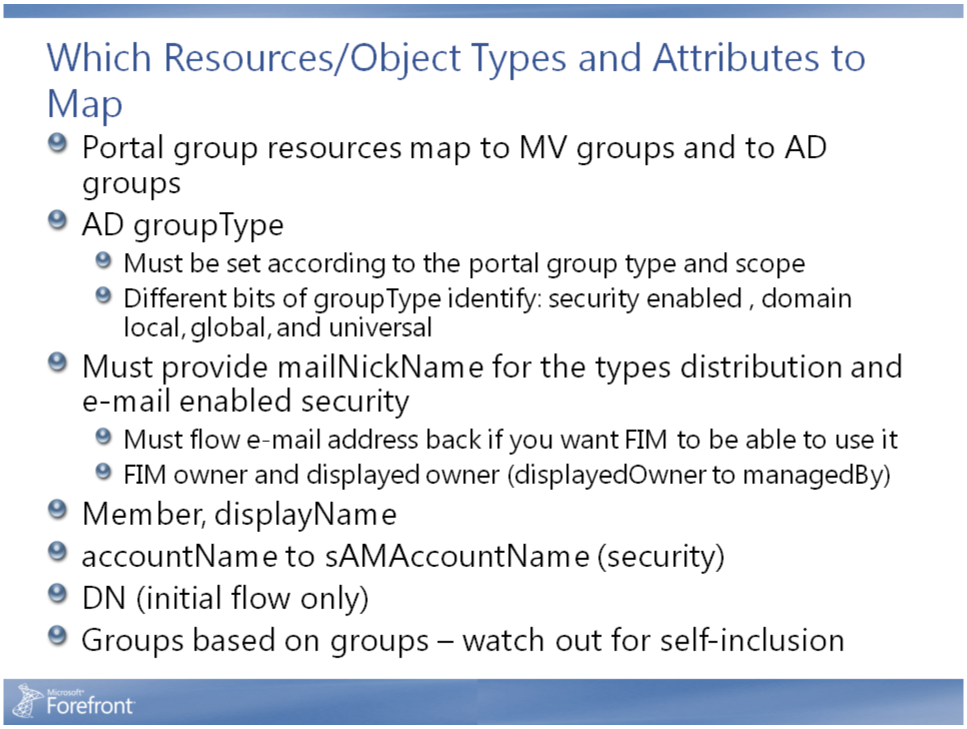


Lesson 2: Managing Groups in Active Directory

- Which resources/object types and attributes to map
- Alternative approaches to synchronization

The most likely reason for having groups in the portal is that you wish to manage groups in AD. This lesson explores the issues and approaches.

Which Resources/Object Types and Attributes to Map



Which Resources/Object Types and Attributes to Map

- Portal group resources map to MV groups and to AD groups
- AD groupType
  - Must be set according to the portal group type and scope
  - Different bits of groupType identify: security enabled , domain local, global, and universal
- Must provide mailNickName for the types distribution and e-mail enabled security
  - Must flow e-mail address back if you want FIM to be able to use it
  - FIM owner and displayed owner (displayedOwner to managedBy)
- Member, displayName
- accountName to sAMAccountName (security)
- DN (initial flow only)
- Groups based on groups – watch out for self-inclusion

Object Types

In the FIM Service MA you will presumably have mapped the CS object type Group to the MV object type Group. When you define your synchronization rule(s) for the AD MA, you will map the MV object type Group to the CS object type Group.

The GroupType Attribute

The different bits of this number attribute correspond to different properties of an AD group:

Meaning	Binary	Hexadecimal	Decimal interpretation
Security Enabled	01000000000000000000000000000000	80000000	-2147483648
Domain Local	00000000000000000000000000000100	00000004	4
Global Group	00000000000000000000000000000010	00000002	2
Universal Group	00000000000000000000000000001000	00000008	8

For example, it follows that we flow 2 for a global distribution group, but -2147483646 for a global security group (they are ANDed together, which just happens to produce the same result as adding them in this case). The numbers we actually need are as follows:

Synchronization Rule	Attribute Flow to groupType
Domain Local Security group	-2147483644
Global Security group	-2147483646
Universal Security group	-2147483640
Universal Distribution group	8

Distribution groups should be universal if they are to be handled correctly in the global address List. You can use global scope in single domain systems (in which case you would flow a 2).

So you must somehow arrange that the correct value flows to groupType depending on the scope and type of the group (see next topic).

The mailNickName Attribute

Just as for users, you will need to flow this attribute if you want the group to be e-mail enabled (so definitely for distribution groups). If you flow null, then no harm is done. Note that if you create a group, and then flow mailNickName, the group will become e-mail Enabled, but the reverse is not true (mailNickName is used to create an e-mail address, then it is no longer required).

Other Attributes

You will obviously want to flow member and displayName.

Security groups will need an sAMAccountName. Distribution groups do not, but neither would it do any harm to flow one.

There are two types of ownership for a group in the portal:

- Owner – This is used by FIM internally.
- DisplayedOwner – What you would like to be seen in other systems.

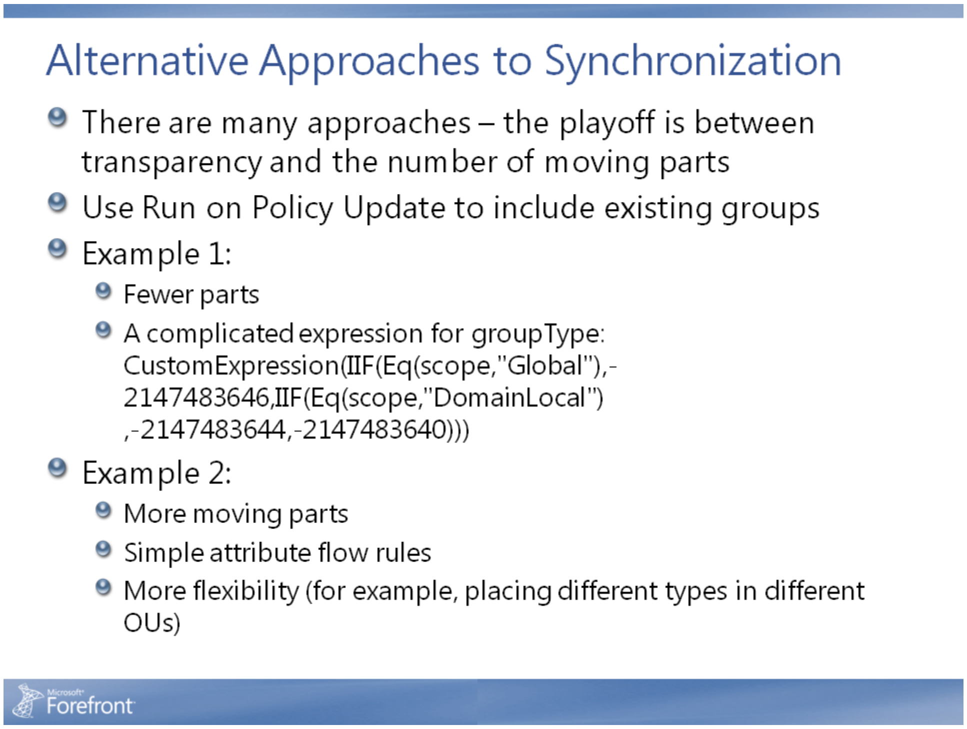
You can map any attribute to any attribute, but a normal usage would be to flow **DisplayedOwner** to **displayedOwner** in the MV, and then out to **managedBy** in AD (this will then be available in Office Outlook 2007, for example).

You will need to build up a DN, and you must have an **Initial Flow Only** flow. You may not need a persistent flow, unless the container could change.

Groups Based on Groups

You can certainly have groups that contain groups, but note that you must take care not to include a group in itself. FIM will not stop you, but AD will not like it!

Alternative Approaches to Synchronization



Alternative Approaches to Synchronization

- There are many approaches – the playoff is between transparency and the number of moving parts
- Use Run on Policy Update to include existing groups
- Example 1:
  - Fewer parts
  - A complicated expression for groupType: CustomExpression(IIF(Eq(scope,"Global"),-2147483646,IIF(Eq(scope,"DomainLocal") ,-2147483644,-2147483640)))
- Example 2:
  - More moving parts
  - Simple attribute flow rules
  - More flexibility (for example, placing different types in different OUs)

There are many valid approaches to synchronizing portal groups with AD groups. At one extreme, you may be able to get away with one synchronization rule, with some awkward expressions for working out what to flow to which attributes. At the other extreme, you can have many simple synchronization rules.

In all cases, when you create a workflow to add a synchronization rule, make it Run on Policy Update so that it applies to your existing groups.

Example Configuration 1

One outbound synchronization rule for distribution groups flowing all the expected attributes (such as DN, member, mailNickname, etc.) and flowing an 8 (or a 2) to groupType, and a workflow to add it and a set transition MPR to trigger the workflow for groups joining all distribution lists (deprovisioning happens when a distribution group is deleted in the portal).

Another outbound synchronization rule for security groups flowing all the expected attributes (such as DN, member, mailNickname, etc.), plus sAMAccountName (if it is not e-mail enabled, there is no mailNickname, and so none flows), and groupType is handled by:

```
CustomExpression(IIF(Eq(scope,"Global"),-2147483646,IIF(Eq(scope,"DomainLocal"),-
2147483644,-2147483640)))
```

This relies on scope having been flowed into the MV. Again, deprovisioning happens when a group is deleted in the portal.

Inbound synchronization can either be done by a separate rule, or you could make the above into inbound and outbound rules. The path of least resistance here is one rule to flow mail back into the MV (if there isn't an e-mail address, no harm is done).

You can probably see that with some extra work these two rules could be collapsed into one, however the custom expression becomes more opaque, and we will need the groupType to be flowed into the MV (so that we can make a decision on whether it is a security group).

Example Configuration 2

This configuration has more moving parts, but with careful naming it can be made more transparent and it has a lot of flexibility (for example, it would be easy to put differently scoped groups into different OUs).

It is the example that is used in the lab that follows, not because it is necessarily the best way, but because it is a better demonstration of sets, workflows, MPRs, EREs, and so on.

Create sets for everything: all global security groups, all local security groups, and all domain local security groups.

Create two base synchronization rules, one for distribution groups and one for security groups as above, but without flowing groupType.

Create three more synchronization rules, one each for the three scopes, each based on (dependent on) the base security group synchronization rule, each flowing a different value to groupType (appropriate to the scope).

Create workflows to add the distribution group synchronization rule as before, and then three pairs of workflows as follows:

Workflow Name	Synchronization Rule	Action
Add AD SG Domain Local Flow	Domain Local Security Group	Add
Remove AD SG Domain Local Flow	Domain Local Security Group	Remove
Add AD SG Global Flow	Global Security Group	Add
Remove AD SG Global Flow	Global Security Group	Remove
Add AD SG Universal Flow	Universal Security Group	Add
Remove AD SG Universal Flow	Universal Security Group	Remove

Create a transition set MPR to trigger the distribution group workflow as before, and three pairs of transition set MPRs to trigger the workflows as follows:

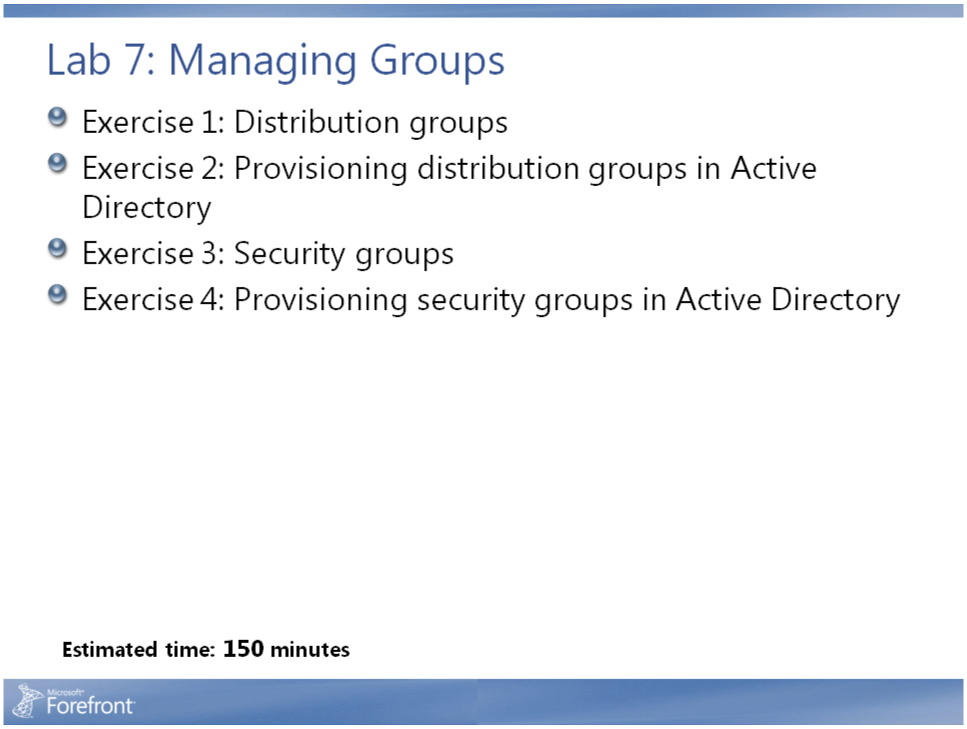
Display Name	Transition Set	Transition Type	Action Workflow
Sync Rules: Add Domain Local SG Flow	All Domain Local SGs	Transition In	Add AD SG Domain Local Flow
Sync Rules: Remove Domain Local SG Flow	All Domain Local SGs	Transition Out	Remove AD SG Domain Local Flow
Sync Rules: Add Global SG Flow	All Global SGs	Transition In	Add AD SG Global Flow
Sync Rules: Remove Global SG Flow	All Global SGs	Transition Out	Remove AD SG Global Flow
Sync Rules: Add Universal SG Flow	All Universal SGs	Transition In	Add AD SG Universal Flow
Sync Rules: Remove Universal SG Flow	All Universal SGs	Transition Out	Remove AD SG Universal Flow

Now when you create a security group, it will get two synchronization rules, one to handle most of the work, and the second to flow the correct value for groupType.

If the scope changes, one rule is removed and another is added.

You will also find that flow fails on exporting to AD, if a domain local group is changed to a global group or vice versa. This is entirely consistent with the way the AD users and computers (ADUC) management console behaves (try it!). In the last module we will make the portal interface behavior consistent with ADUC behavior. Meanwhile the fix is to make a group universal, after which you can do what you like with it.

Lab 7: Managing Groups



Lab 7: Managing Groups

- Exercise 1: Distribution groups
- Exercise 2: Provisioning distribution groups in Active Directory
- Exercise 3: Security groups
- Exercise 4: Provisioning security groups in Active Directory

Estimated time: 150 minutes