Infor PLM Accelerate 11

MAC Policies

Important Notices

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials ("Purpose").

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

Trademark Acknowledgements

Publication Information

Publication date: May 31, 2018

Contents

About this guide

This document provides information about how to control permissions and access using MAC Policies in Infor PLM Accelerate.

Intended audience

This guide is intended for system administrators. This document assumes that you have at least some knowledge in:

- System architecture and function for your Infor system
- SQL Server database

For the most up-to-date list of software and hardware requirements for Infor products, see the documentation for your system.

Related documents

You can find the documents in the product documentation section of the Infor Xtreme Support portal, as described in the "Contacting Infor" section below.

Contacting Infor

If you have questions about Infor products, go to the Infor Xtreme Support portal at www.infor.com/inforxtreme.

If we update this document after the product release, we will post the new version on this Web site. We recommend that you check this Web site periodically for updated documentation.

If you have comments about Infor documentation, contact documentation@infor.com.

Chapter 1. Overview

Infor PLM Accelerate provides the flexibility to allow administrators many options when controlling permissions and access within Infor PLM Accelerate. MAC Policies are designed to allow for dynamic control when determining permissions for Items based upon the Properties of the current User and Item being affected. This document focuses on the application MAC Policies along with possible use cases.

Chapter 2. Establishing MAC Policies

Infor PLM Accelerate MAC Policies are created as Items and can be applied across ItemTypes using the individual Permissions type.

Creating a New MAC Policy

You can find MAC Policies in Infor PLM Accelerate by clicking **Administration →Access Control→Mac Policies** in the TOC:

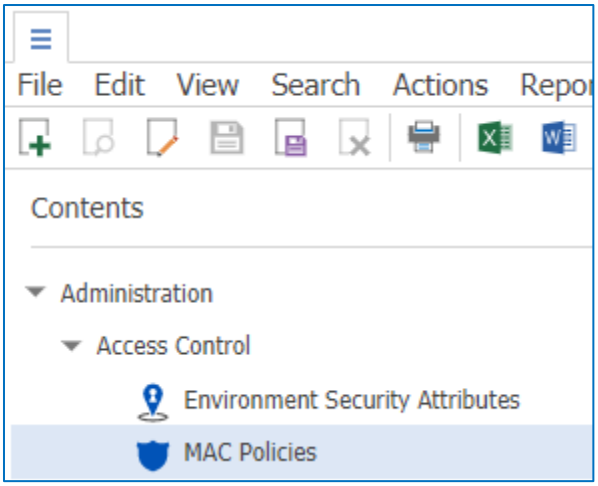

Figure 1.

Only users with Administrative permissions have the ability to create MAC Policies. When you create a new MAC Policy, you need to create and apply Policy Rules.

Creating a Policy Rule

Policy Rules are logic-based conditions which must be true to grant the User permissions to an Item. To create a new Policy Rule, switch to the MAC Policy Editor view by clicking on the MAC Policy Editor icon. Until you create the MAC Policy, this view should not be available. Selecting the **Create New** option makes the lower portion of the window available to enter the logic for the Policy Rule. The following conditions apply to Policy Rules:

- Values are case sensitive.
- String literals text must be enclosed between quotation marks ('text'), quotation escapes with back slash (**\'**).
- A Constant can act as an operand when you use it in a comparison. Otherwise a Constant is a string type.
- Operators and precedence are the same as those used in SQL languages.
- Arithmetic operators are not supported.
- Parentheses can be used to override operator precedence.

- Operators are not case sensitive.
- Comparing two strings follows Transact-SQL rules.

There are also the variables for CurrentUser and CurrentItem, which allow the Policy Rule to pull the Properties of the current User accessing an Item and the current Item being accessed, respectively. Once the logic is complete, the rule can be saved.

Note: If the Policy Rule uses a Property on the User ItemType and a User is able to edit their own User Item, then the User is capable of changing their level of access to any of the ItemTypes that a MAC Policy is applied to. This can also apply if the Edit control is not restricted in a MAC Policy and other Permissions are based on editable Properties.

Defining Environmental Security Attributes

Environmental Security attributes grant a user certain access rights to an Item based on specific circumstances such as the geographical location of the user at the time an access request is made. For example, if the user making the request is located in a country where access is restricted, the request is denied. If the same user changes their physical location to a country where access is not restricted, their request is accepted.

Infor PLM Accelerate uses the “Environment Attribute” item type to define environmental security attributes. Each item that has the “Environment Attribute” ItemType describes one environment security attribute. Each attribute has a specific name and data type as well as a custom method (specified in the “Get Value Method” property) that is called by Infor PLM Accelerate to get the attribute value for each request to Infor PLM Accelerate. The environment security attribute values are taken into account when calculating MAC Policy conditions for determining if an access request should be granted if the conditions use the environment security attribute. An environment security attribute with the name <attr_name> is referenced in a MAC Condition as ‘$<attr_name>’.

Note: It is the responsibility of the system administrator/implementation specialist to create custom server methods that return the environment security attribute values to Infor PLM Accelerate. The custom methods should be created using the EnvironmentAttributeMethod method template.

Exempt Identities

Each MAC Policy includes a list of “Exempt identities.” If the user making an access request has an identity that is included in the “Exempt identities” list, MAC Policy rules are not applicable to the request. The Exempt Identities list is useful when processing is done using GrantIdentity()/RevokeIdentity() to temporarily raise the user access level.

Applying Policy Rules

Once you create the Policy Rules, you must assign them to a MAC Policy view. There are five drop down lists:

- Show Permission Warning – determines if, when permissions are restricted, the User is given a standard permission warning.

- Discover – determines if the User can view an Item within a search grid.
- Get – determines if the User is able to open Forms and view all the Properties of an Item.
- Update – determines if a User is able to lock an Item.
- Delete – determines if a User is able to delete an Item.

Selecting a Policy Rule from the dropdown applies that access right denying the User access if the conditions are not met.

Applying MAC Policies

Once you establish the Policy Rules, you must assign the MAC Policy to the desired ItemTypes and then activate them. Assigning the MAC policy to ItemTypes is done by adding them to the Assigned To Relationship.

To activate a MAC Policy, unlock the policy and select the ‘Activate’ Action. When Activating a MAC Policy, all Users except for the admin activating the MAC Policy should be logged off and prevented from accessing the system until the MAC Policy is activated.

Updating MAC Policies

Once activated, a MAC Policy can be deactivated or versioned. The ‘Deactivate’ action sets a MAC Policy for the ‘Inactive’ state. When a MAC Policy is ‘Inactive,’ the Policy Rules are not applied to control access.

The ‘New Version’ Action increases the Revision of the MAC Policy. The previous revision of the MAC Policy is promoted to the ‘Archived’ state only after the new revision is Activated.

Sample MAC Policy Rule

The following statement is a Policy Rule that is triggered on Update. It assigns a MAC Policy to a Part. The policy rule specifies that only Users with an Employee number beginning with ‘123’ are able to lock Parts with an ‘Assembly’ Classification during working hours. In the following condition, ‘$work_hours’ references an environment security attribute. You would use a custom method associated with the attribute to return the appropriate value.

```
CurrentItem.[Classification] = 'Assembly'
AND
CurrentUser.[Employee #] like '123%'
AND
$work_hours
```