BeyondTrust

AD Bridge Delegate Permissions to Manage License Containers

Table of Contents

Delegate Permissions to Manage License Containers	3
Overview of License Containers and Licenses in AD Bridge	3
Delegate Permissions to a License Container	3

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 2/28/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Delegate Permissions to Manage License Containers

AD Bridge stores licenses for agents in Active Directory (AD). To store the licenses, one or more license containers need to be created using the BeyondTrust Management Console (BMC). Licenses are then imported into the container from the console.

Agents get licenses from the license container they are immediately subordinate to in the AD hierarchy. In most cases, a single license container placed in the hierarchy superordinate to all agents is sufficient. In some cases, additional licensing containers can be created for organizational or administrative reasons.

Overview of License Containers and Licenses in AD Bridge

Each license container and each imported license is stored in AD as an object of class *container*. Appropriate permissions must be defined for a licensing administrator to create and delete license containers and licenses.

In addition to granting permissions to a licensing administrator, AD Bridge computer objects must also be granted **Write all properties** permissions to each license object to write to their claimed license object. These rights will be automatically granted on each imported license when the license container is created, using the default option **Allow Computers to Acquire Licenses Automatically**.

For more information, see Create an AD Bridge License Container at https://www.beyondtrust.com/docs/ad-bridge/getting-started/windows-admin/manage-licenses/create-license-container.htm.

Note: To run the BMC, the user account must be a domain user account and a member of the local Administrators group.

Delegate Permissions to a License Container

This guide shows how to apply the minimum permissions required to manage licensing. In general, if a user has full rights over an OU structure, they can administer all license functions over that OU. The following procedure shows how to add minimum permissions to a security principal (preferably a group) to manage licensing.

The procedure uses the ASDI Edit configuration tool. ADSI Edit exposes the specific permissions required at the minimum level. Active Directory Users and Computers (ADUC) or a command line tool such as DACLS do not expose the permissions to this level of granularity.

Steps might vary slightly between OS versions. Steps provided here are from Windows Server 2012.

1. Using ADSI Edit, connect to the default naming context of the domain and browse to the OU where the license containers will be created.



2. Right-click an OU, and then select Properties.



3. Click the Security tab, and then select Advanced.

OU=PBIS Properties	?	x					
Attribute Editor Security							
Group or user names:							
Administrators (INTECHRALVAdministrators)							
Print Operators (INTECHRAL/Print Operators)							
8 Pre-Windows 2000 Compatible Access (INTECHRAL\Pre-Wind							
ENTERPHISE DUMAIN CUNTRULLERS							
Add	<u>l</u> emove	•					
Permissions for SELF Allow	Deny						
Full control		^					
		≡					
Write							
Delete all child objects							
For special permissions or advanced settings, click Advanced Advanced.							
OK Cancel Apply Help							

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 2/28/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.



4. Click Add.

- _ 🗆 🗙 Advanced Security Settings for PBIS Domain Admins (INTECHRAL\Domain Admins) Chang Owner Permissions Auditing Effective Access For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available). Permission entries: Type Principal & Allow Account Operators (INTECH... erited from Applies to This object only Create/delete InetOrg... None Allow Account Operators (INTECH... Allow Account Operators (INTECH... Create/delete Comput... None This object only This object only Create/delete Group o... None This object only & Allow Print Operators (INTECHRAL... Create/delete Printer o... None SR Allow Account Operators (INTECH... Domain Admins (INTECHRA... Create/delete User obj... None
 Iolow
 Account Operators (INTECHA...
 Creat/A...

 Mallow
 Domain Adminis (INTECHA...
 Full con

 Allow
 ENTERPRISE DOMAIN CONT...
 Special

 Allow
 Authenticated Users
 Special

 Allow
 SYSTEM
 Full con

 Allow
 Pre-Windows 2000 Compatib...
 Special
 None None None Full control Full control Special Special Full control None This object only DC=intechral,DC=local Descendant InetOrgPerson Add Remove View Restore defaults Disable inheritance OK Cancel Apply
- 5. Click **Select a principal**, enter the name of the group to provide permissions to, and then click **OK**.
- _ 🗆 X Permission Entry for PBIS Principal: Select a p Type: Applies to: This object and all descendant objects E Full control Select this object type: User, Group, or Built-in security principal Object Types... From this location Locations... PBISL Check Names eAdmins Modify perm Advanced... 0K Cancel All validated writ All extended righ Create all child obje Create msie Create account object ieee80211-Poli Delete account object Create msImaging-PSPs object aging-PSPs obje OK Cancel
- 6. Select **Allow**, **This object and all descendent objects**, and then select the following permissions from the list and click **OK**:
 - Create Container objects
 - Delete Container objects



7. Repeat steps 4 and 5 to add the group with a new set of permissions.

5

- 8. Select **Allow**, **Descendent Container objects**, and then select the following permissions from the list and click **OK**:
 - List contents
 - · Read all properties
 - · Write all properties
 - Delete
 - Delete subtree
 - Read permissions
 - Modify owner

₿.			Permission Entry for PBIS		x
Prin Typ Ap	ncipal: pe: plies to:	PBISLicenseAdmins (INTECHRAL\PBISLicenseAdmins Allow v Descendant Container objects v) Select a principal		
Ap	mission	Descendant Container abject T T T T T T T T T T T T T	Dekte m/D5-Chim/TendfemationPolicies objects Dekte m/D5-Chim/Types objects Dekte m/D5-Chim/Types objects Dekte m/D5-Chim/Types objects Dekte m/D5-DeviceByprosocGenetic Container objects Dekte m/D5-DeviceByprosocGeneticAccount objects Dekte m/D5-DeviceByprosoCacherological Dekterological Dekterologica		
		Delete aCSPolicy objects	Ureate msUS-Value lype objects	Cancel	

Note: The steps can be performed on an OU, or on the root of the domain. In some cases, especially to manage a licensing container at the domain root, it may not be preferable to grant even these restricted permissions as they allow the manipulation of all container class objects under the target. In these cases, a Domain Admin can create the licensing container first in the BMC and then follow the above steps. However, instead of targeting the parent OU, target the **\$LikewiseEnterpriseLicenses** container created (turn on **Advanced Features** from the ADUC **View** menu to see the created license container).