Usage Scenario - Azure Active Directory

Last Modified on 08.08.25

Background

The customer has Azure Active Directory tenant and all workstations are Azure AD joined Windows 10 (or later) devices. The customer does not have any Windows servers.

Target

The customer has the following targets that need to be met:

- End users should not have any permanent admin privileges
  - Existing permanent admin privileges must be removed
  - Exceptions can be made (when absolutely needed for performing work tasks) for single workstations by requesting permanent admin privileges from IT support
- All end users should have possibility to get temporary admin privileges when granted by IT support
- End users that currently have permanent admin privileges should have possibility to get temporary local admin privileges as self-service (IT support grant not needed)
- Default permanent admin privileges for Global Admins and Device Administrator Azure AD roles must be removed
- Permanent admin privileges must be allowed for specified Azure AD group to every workstation
- Default local build-in Administrator account on every workstation must have device specific random password with minimum of 12 characters and include special characters also
- Utilize cloud-based resources as much as possible for the platform. When possible, use PaaS resources.
- Get automatic updates to the platform

Platform

The Privilege Manager environment can be deployed to Microsoft's Azure PaaS platform. As the customer only has devices connected to Azure AD there is no need to communicate from PaaS platform to the customer's on-premises environment. So in this scenario Microsoft Azure PaaS platform can be utilized.

Actions for platform:

1. If needed, create new Azure AD group for end users that currently has permanent admin privileges.
2. If needed, create new dynamic Azure AD group for devices that automatically collects all Windows workstations as group members.
3. If needed, create new Azure AD group for users that need to have permanent admin privileges to all workstations.
4. Deploy two Azure App Service resources.

5. Automate platform deployment.
    - Following the instructions, send information that Azure AD group from step 1 needs to have permissions to use self-service with local user account.

Privilege Manager Configuration

Privilege Manager configuration is based on the managed rules created within the Privilege Manager Portal. Managed group rules are used to control local group memberships and managed user rules are used to control local user accounts. Local users can be defined to Privilege Manager to support randomized passwords or temporary admin elevation using local user account.

Local users

1. Create the following local user accounts
2. Temporary Administrator (Example login name: TempAdmin)

Managed group rules

Create the following managed group rules for the Azure AD group (Azure AD group that has all Windows workstations as members) and use group **Administrators** for all rules.

- Built-in Administrator
- Temporary Administrator
- Azure AD group: Users require permanent admin privileges to all workstations as members

> **Info:** As Privilege Manager will start to manage the local group memberships for the groups where managed group rules exist, the existing members in these groups that do not have an active managed group rule will be removed from the local groups. Therefore, target 4 is fulfilled as there are no managed group rules for Azure AD roles.

> **NOTE**: To fulfill targets, additional managed group rules for single devices can be created by IT support.

Managed user rules

Create the following managed group rules for the Azure AD group (Azure AD group that has all Windows workstations as members)

- For built-in Administrator, use **Generate random password and save to database** rule type.
- For Temporary Administrator, use **Generate temporary user account that can be activated** rule type.

Azure AD built-in roles

When you join a Windows device to Azure AD, Azure will automatically add **Global Administrator** and **Azure AD Joined Device Local Administrator** roles the device's local administrators group. Privilege Manager will remove these roles from

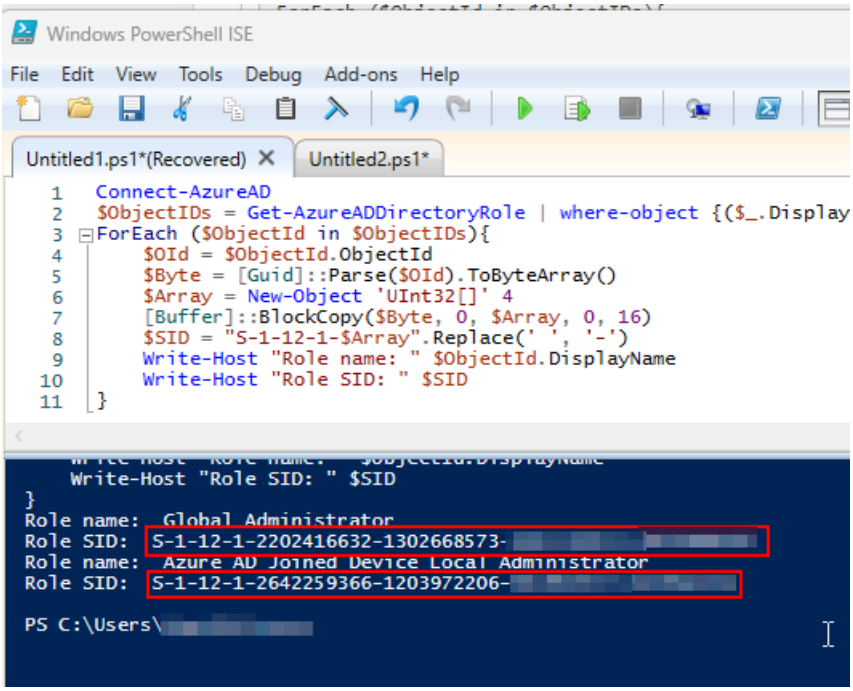
the client device, if you don't specify these roles in Privilege Manager.

Because Azure AD roles are not regular groups, you need to add the Azure AD roles in Privilege Manager with their SID's. SID can to be created by converting Azure AD role's object id to the correct format. The id can be found by using Azure AD PowerShell module:

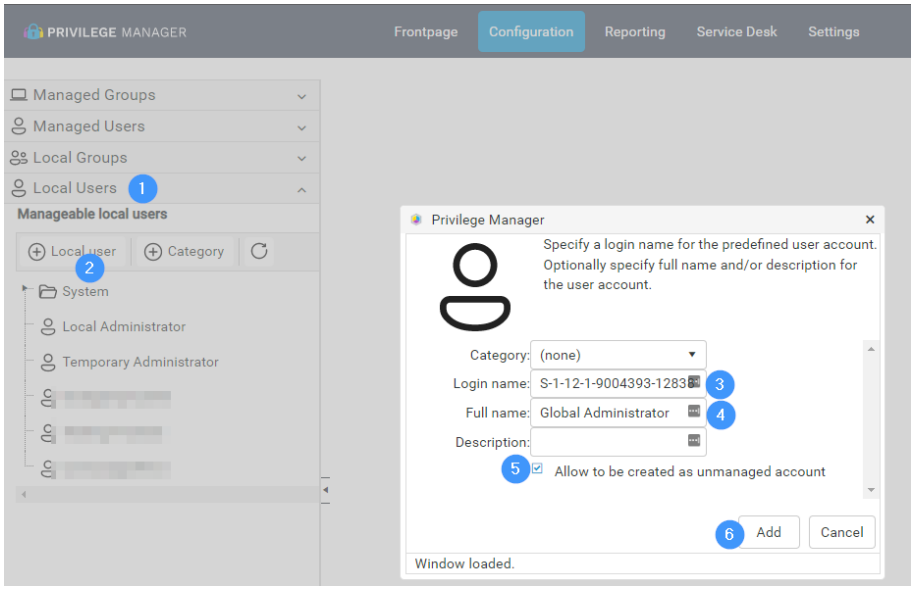
1. Connect to Azure AD via PowerShell with **Connect-AzureAD** command
2. Run the following PowerShell-script to find object id's and convert those to SID format

```
$ObjectIDs = Get-AzureADDirectoryRole | where-object {($_.DisplayName -eq "Global Administrator") -or ($_.DisplayN
ame -eq "Azure AD Joined Device Local Administrator")}
ForEach ($ObjectId in $ObjectIDs){
   $OId = $ObjectId.ObjectId
   $Byte = [Guid]::Parse($OId).ToByteArray()
   $Array = New-Object 'UInt32[]' 4
   [Buffer]::BlockCopy($Byte, 0, $Array, 0, 16)
   $SID = "S-1-12-1-$Array".Replace(' ', '-')
   Write-Host "Role name: " $ObjectId.DisplayName
   Write-Host "Role SID: " $SID
}
```

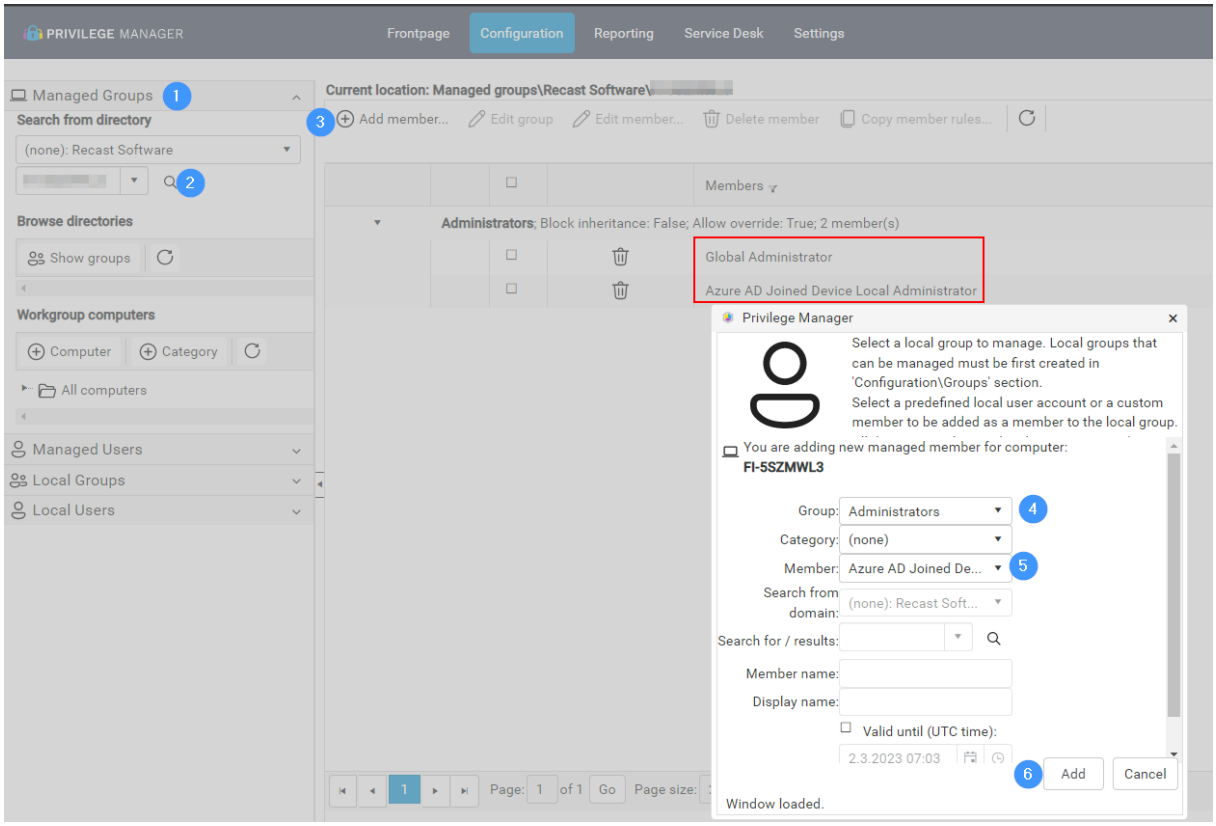
Example:



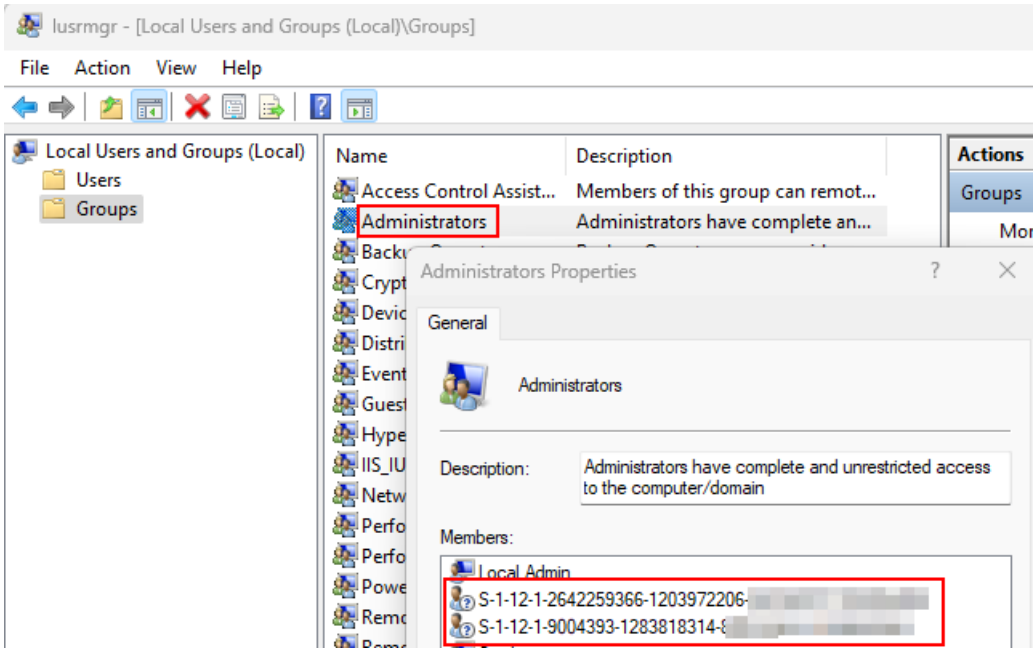
1. Create a new local user in Privilege Manager
2. Copy the SID from PowerShell script's output, and add it to "Login name" field
3.



4. Add roles to client devices Administrators group in Manage Groups page:



5. Azure AD roles can now be found from client device's Administrators group



It might take up to 4 hours until users with the specified Azure AD role have administrator access to the device

Copyright © 2025 Recast Software Inc. All rights reserved.