Self service configuration

Last Modified on 03/03/2022 10:53 am EET

Self service temporary account activation validation is done on Centero Agent Gateway. Configuration that specifies users who can use self service temporary account activation are specified to **Modules\Carillon\TemporaryAccountValidityTimes.xml** file located on the Centero Agent Gateway web site.

> **Info**
>
> By default Hybrid devices that are joined to both On-premises AD and Azure AD, use rules for On-premises groups, users and device. This can be changed by Carillon client configuration so that hybrid device will start to use Azure AD based self service rules.

Items root element

XML file contains Items element where you can specify following settings:

- RequireAuthentication: Setting value to 'false' allows self service activation code request to be performed without authentication on Centero Agent Gateway web service. This allows also local user accounts on clients to be used when requesting activation code. If value is 'true' then Centero Agent Gateway web service requires authentication and therefore local user account on clients cannot be used to request activation code. Default and recommended value is 'true'
- AllowCredentials: Setting value to 'false' prevents user from specifying alternative credentials during self service activation code request when using 'Run with local account' activation type. If value is 'true' then user can specify alternative credentials that are used to check if user is allowed to use self servive. Default value is 'true'

Item element

Item element inside Items element allows you to specify following settings:

- Value: 0-11 (see description for the values in User account validity for portal activation)
- AllowSelfService: Setting value to 'true' enable self service feature and setting value to 'false' disables self service feature. Default value is 'true'

Allow element

Allow element inside Item element specifies rules when self service is allowed for users. Allow element can contain several Users elements and if any of the Users elements is matched for the request then self service is allowed (unless Deny rule overrides this). See Users element section for details how to create Users elements.

Deny element

Deny element inside Item element specifies rules when self service is denied for users. Deny element can contain several Users elements and if any of the Users elements is matched for the request then self service is not allowed. See Users element section for details how to create Users elements.

Users element

Users element inside Allow or Deny elements allows you to specify following settings:

- Principal: User or a group to whom self service should be allowed. Following formats accepted:
    - ADDOMAIN\Pre-Win2000 user login name (sAMAccountName attribute): Use for On-premises AD users
    - ADDOMAIN\Pre-Win2000 group name: Use for On-premises AD groups. All users directly or trough nested groups will match the rule
    - GUID: Use for Azure AD groups and users. Always use Azure AD object ID value that can be found from Azure AD management portal. When object ID is for group then all users directly or trough nested groups will match the rule
    - AzureAD\UserProfileName: Can be used for single cloud only Azure AD accounts but preferred method is to use object ID. UserProfileName can be located only on the device after user has logged on to the device and profile is created
- AllowDomainAccountActivation: Setting value to 'true' allows users defined in Principal attribute to use also domain account activation method. Setting value to 'false' allows users defined in Principal attribute to use only local account activation method
- Description: Specify description for the element when needed. For example can be used to document user friendly name for the specified Azure AD object ID in Principal attribute

Users element can contain also Computer elements when rule needs to match only specified computers. If Users element does not contain any Computer elements then rule will match for computers. Any number of Computer elements can be specified to each Users element.

Computer element

Computer element inside Users element allows you to specify following settings:

- Principal: Computer or a group where parent Users rule is valid. Following formats accepted:
    - msDS-PrimaryComputer: On-premises AD device must be included on On-premises AD user accounts msDS-PrimaryComputer attribute to match the rule
    - ADDOMAIN\ComputerName$ (sAMAccountName attribute): Use for On-premises AD computers
    - ADDOMAIN\Pre-Win2000 group name: Use for On-premises AD groups. All computers directly or trough nested groups will match the rule
    - GUID: Use for Azure AD groups and devices. Always use Azure AD object ID value that can be found

from Azure AD management portal. When object ID is for group then all devices directly or trough nested groups will match the rule

- Description: Specify description for the element when needed. For example can be used to document user friendly name for the specified Azure AD object ID in Principal attribute

Example

TemporaryAccountValidityTimes.xml file:
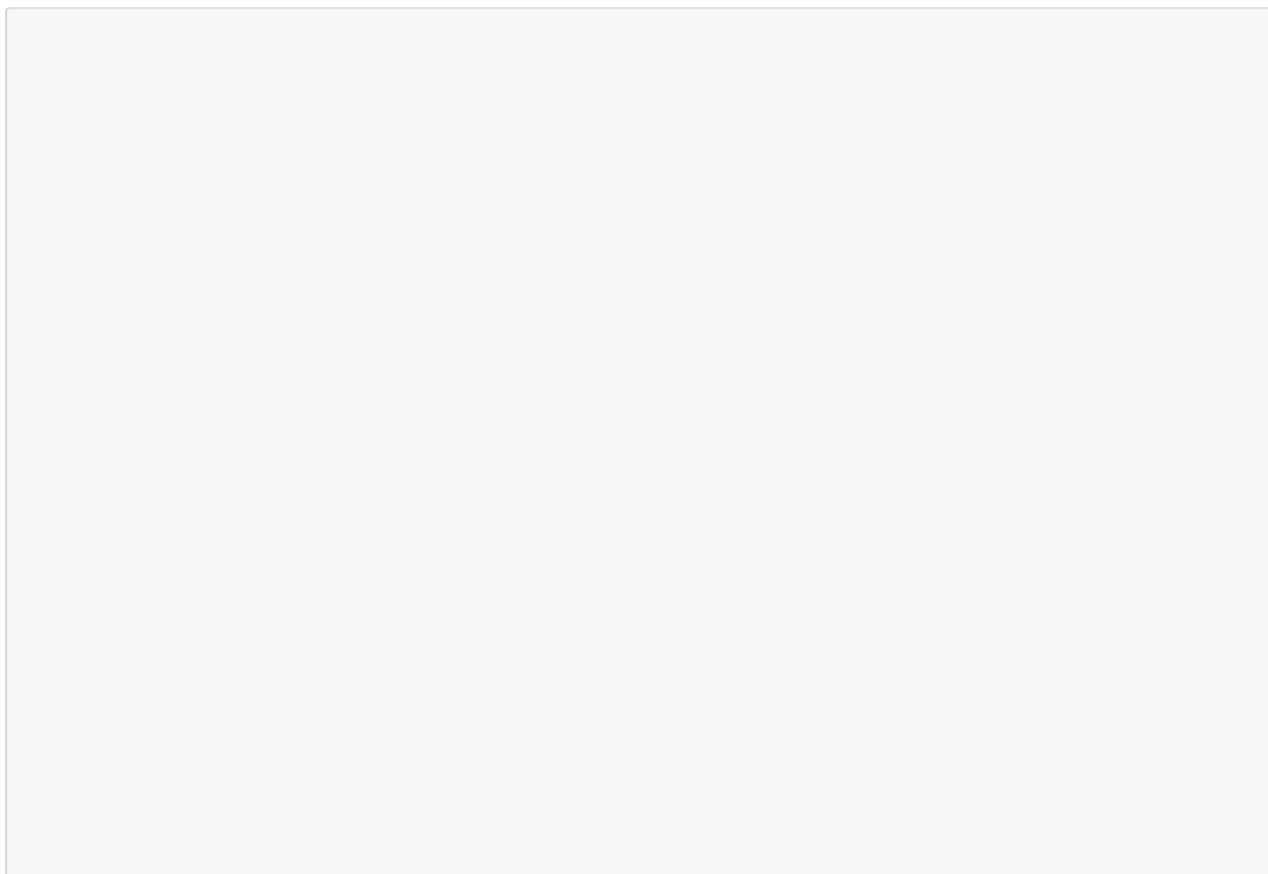
In the example self service feature is enabled and requires user authentication. When using local account activation method, specifying alternative credentials is allowed.

Self service is denied for:

- Members of 'ADDOMAIN\Deny Carillon Self Service' when user is logged on Azure AD device 'LAPTOP1' (96306f5b-489a-460e-9744-61d9b7e332b9) or On-premises AD device that is member of 'ADDOMAIN\All Workstations' On-premises AD group

Self service for local account method is allowed for:

- Members of On-premises AD group 'ADDOMAIN\Allow Carillon Self Service with Local Account' when user is logged on device that is found from users On-premises AD accounts msDS-PrimaryComputer attribute
- Members of 'ADDOMAIN\Allow Carillon Self Service with Domain Account'
- Members of 'ADDOMAIN\Server admins' when user is logged on device that is member of 'ADDOMAIN\All

Servers' On-premises AD group

- Cloud only Azure AD user 'AzureAD\AzureBenefit2MPN' on Azure AD joined device
- Members of 'Allow Carillon Self Service' (8aa297fe-5047-481e-88ca-7b0b741536b7) on Azure AD joined device that is member of 'Windows devices' (5667a674-0a1b-4523-b21b-13d5391d93a9) Azure AD group
- User 'John Doe' (a469f5a2-6f9b-4d1c-beaf-b105ba599acd) on Azure AD joined device 'LAPTOP1' (96306f5b-489a-460e-9744-61d9b7e332b9)

Self service for domain account method is allowed for:

- Members of 'ADDOMAIN\Allow Carillon Self Service with Domain Account'
- Members of 'ADDOMAIN\Server admins' when user is logged on device that is member of 'ADDOMAIN\All Servers' On-premises AD group
- User 'John Doe' (a469f5a2-6f9b-4d1c-beaf-b105ba599acd) on Azure AD joined device 'LAPTOP1' (96306f5b-489a-460e-9744-61d9b7e332b9)