Self Service Configuration

Last Modified on 01.27.23

Self service temporary account activation validation is done via the Recast Agent Gateway. You can configure users who can use self service temporary account activation in the **Modules\x\TemporaryAccountValidityTimes.xml** file located on the Recast Agent Gateway website.

> 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 Privilege Manager client configuration so that the 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 this value to 'false' allows self service activation code request to be performed without authentication on the Recast Agent Gateway web service. This allows also local user accounts on clients to be used when requesting activation codes. If the value is 'true', then Recast Agent Gateway web service requires authentication and therefore local user accounts on clients cannot be used to request activation codes. The default and recommended value is 'true'
- **AllowCredentials**: Setting this value to 'false' prevents users from specifying alternative credentials during self service activation code requests when using the 'Run with local account' activation type. If this value is set to 'true' then users can specify alternative credentials that are used to check if a user is allowed to use self service. The 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 are matched for the request then self service is allowed (unless Deny rule overrides this). See Users element section for details on 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 match for the request then self service is not allowed. See the Users element section for details on how to create Users elements.

Users element

The 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. The following formats are 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 through nested groups will match the rule
  - GUID: Use for Azure AD groups and users. Always use the Azure AD object ID value that can be found from the Azure AD management portal. When object ID is for group then all users directly or through nested groups will match the rule
  - AzureAD\UserProfileName: This can be used for single cloud only Azure AD accounts but the preferred method is to use object ID. UserProfileName can be located only on the device after the user has logged on to the device and the profile is created
- **AllowDomainAccountActivation**: Setting this value to 'true' allows users defined in the Principal attribute to also use the domain account activation method. Setting this value to 'false' allows the users defined in the Principal attribute to use only the local account activation method
- **Description**: Add a description for the element when needed. For example, this can be used to document a user-friendly name for the specified Azure AD object ID in Principal attribute

Users element can also contain Computer elements when the rule needs to match only specified computers. If Users element does not contain any Computer elements then the 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:

```
<?xml version="1.0" encoding="utf-8" ?>
<Items RequireAuthentication="false" AllowCredentials="true">
  <Item Value="0" AllowSelfService="true">
    <Allow>
      <Users Principal="ADDOMAIN\Allow Carillon Self Service with Local Account" AllowDomainAccountActivation="fal
se">
        <Computer Principal="msDS-PrimaryComputer"/>
      </Users>
      <Users Principal="ADDOMAIN\Allow Carillon Self Service with Domain Account" AllowDomainAccountActivation="t
rue">
      </Users>
      <Users Principal="ADDOMAIN\Server admins" AllowDomainAccountActivation="true">
        <Computer Principal="ADDOMAIN\All Servers"/>
      </Users>
      <Users Principal="AzureAD\AzureBenefit2MPN" AllowDomainAccountActivation="false">
      </Users>
      <Users Principal="8aa297fe-5047-481e-88ca-7b0b741536b7" Description="Allow Carillon Self Service AAD object
ID" AllowDomainAccountActivation="false">
        <Computer Principal="5667a674-0a1b-4523-b21b-13d5391d93a9" Description="Windows devices AAD object I
D"/>
      </Users>
      <Users Principal="a469f5a2-6f9b-4d1c-beaf-b105ba599acd" Description="John Doe user account AAD object ID"
AllowDomainAccountActivation="true">
        <Computer Principal="96306f5b-489a-460e-9744-61d9b7e332b9" Description="John Doe's device LAPTOP1 AAD
object ID"/>
      </Users>
    </Allow>
    <Deny>
      <Users Principal="ADDOMAIN\Deny Carillon Self Service">
        <Computer Principal="96306f5b-489a-460e-9744-61d9b7e332b9" Description="John Doe's device LAPTOP1 AAD
object ID"/>
        <Computer Principal="ADDOMAIN\All Workstations"/>
      </Users>
    </Deny>
  </Item>
</Items>
```

In the example the 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 a user is logged on to the 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 the 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)