GroupID
by imanami

GroupID 10 - Release Notes

Service Release – 2

GroupID
Authenticate

GroupID
Automate

GroupID
Self-Service

GroupID
Password Center

GroupID
Synchronize

GroupID
Insights

GroupID
Reports

Contents

Overview

The document communicates new features introduced in GroupID SR2 and the patches merged in it. The patches are developed against performance-related issues and bugs identified in GroupID 10.0 and GroupID SR1. It also documents known issues in GroupID 10 SR2.

New Features

GroupID as an Identity Provider

GroupID can now provide the services of an identity provider. You can register a third-party application as a service provider in GroupID to authenticate users in that application through GroupID.

QR Code

You can now sign in GroupID by scanning the displayed QR code with the GroupID app installed on your smartphone. This option is available if the QR code feature is enabled for the identity store.

Modern Authentication

GroupID 10 SR2 provides modern authentication support in GroupID 10 SR2. GroupID will use a certificate. The certificate can be generated in IIS or in a third-party application.

In Exchange Online/Office 365, operations are no longer done in the context of a user account (as it used to be), but through a certificate. For example, earlier, GroupID carried out operations in the context of the service account that we specified in identity store settings and messaging provider. For details, see Appendix G.

OAuth notification settings

GroupID now supports OAuth settings for notifications.

Merged Patches

The following sections provides information about the patches merged in GroupID 10 SR2.

Patch #	Description
9469 – Ownership update using group attestation wizard The patch fixes the issue when a user is added as an owner of a group through the Group Attestation wizard and that user is already an Additional owner of the group.	
20597 – STS Same Site Cookie patch Fixes the redirection mechanism to the provided URL after authenticating the user through ADFS or any other SAML provider.	
20832 – Elastic URL(s) from HTTP to HTTPS This patch resolves the issue of converting Elastic URLs from HTTP to HTTPS. Read the ReadmeFirst.txt file in the following path: `[GroupID Installation Drive]:\Program Files\Imanami\GroupID 10.0\ElasticSearch\elasticsearch-6.2.4\` See Appendix A for details.	
20933 – Set-Group with *AdditionalOwners* issue In GroupID Management Shell, *Set-Group* cmdlet is not working for *Replace*, *Remove* and *Clear* parameters for additional owners added via the Self-Service portal.	
20941 – Users unable to change their passwords In the Password Center User portal, when a user tries to change his/her password on the Change Password window, old password does not match issue occurs.	
21475 – Modifying Security Roles policies when adding/removing OUs in the New Object policy The patch fixes the issue of remove restriction on modifying security roles policies when adding/removing OUs from the New Object policy.	
21581 – Typographical error in [*Identity store*].xml file This patch fixes a typographical error in the [*Identity store*].*xml* file located at the following path: `<GroupID Installation Drive>:\Program Files\Imanami\GroupID 10.0\SelfService\Inetpub\[Portal name]\Design\` In the file, *ismandatory* is misspelled as *ismendatory*. Please note it applies to new portals only. In the existing portals, you have to fix the spellings manually.	
27166 – Login screen flash issue when GroupID Authentication is disabled The patch provides a fix for the Authenticate - login screen flash issue. It occurs when GroupID Authentication is disabled and the Self-Service portal is configured with ADFS for SSO.	
27259 – Symbols '<' and '>' issue in fields In the Self-Service portal, if '<' and > signs are used in Group properties name, they get converted into '&lt' and &gt‘. (Parent Patch: 44934)	

Patch #	Description
27296	**Leading space issue in SQL statement** This patch resolves the leading space issue in the SQL statement for Query Designer database key mapping.
28013	**SetDynasty, SetSmartGroup issue** This update fixes the issue of 'Separator* and *'InheritanceBehavior'* parameters in GroupID Management Shell's *Set-Dynasty* cmdlet, it also fixes the *Set-SmartGroup* cmdlet issue when used in the pipeline.
28015	**Entire Directory as 'Start-in' value for Managerial Dynasty** This patch fixes the issue when the value for *Start in* is set to *Entire Directory* in Managerial Dynasty.
28062	**Performance issue connecting to an identity store and creation of objects** This patch fixes the issues that users face while connecting to an identity store and creation of objects. In a multi-domain environment, GroupID takes time to look up the Domain Controllers in a domain. As a result, the creation and update of objects takes considerable time. See Appendix D for details.
28192-2	**G Suite alias normalization issue** Dynasties are not getting mail-enabled in an on-prem AD identity store configured with G suite as a messaging provider.
28192-1	**Mail-enabled child dynasties creation issue** In the absence of the *MailNickName* attribute in Identity Store's Sync attribute list, mail-enabled child dynasties are not created upon parent dynasty update.
28237	**GroupID Management Console loading slow** GroupID Management Console is taking a long time to launch.
28352	**Turkish characters issue in membership** This patch fixes the Turkish characters issue in object names. When these objects are searched, correct results are not fetched.
28469	**Direct Reports' profile picture update** The patch provides a fix for an issue that while using the Self-Service portal, managers cannot update profile picture of their direct reports.
28582	**User Settings failed to reset** In the GroupID portal, when Reset Defaults option in the User Settings is used an error occurs and the user settings are failed to reset.
28684	**Update All Records since last job run** This patch resolves the issue of modifying records in Synchronize. In case of a table destination provider, instead of modifying only those records that have changed since the job's last run, GroupID modifies all records.
28753	**History language issue in SSP** This patch fixes the text localization issues in History for the Danish language.
28790	**Remove the irrelevant users from group membership via *MembershipLifecycle* job** This patch provides a fix to successfully remove the irrelevant users from Elastic and process the temporary membership via the *MembershipLifecycle* job.

Patch #	Description
28821	**– Send email to manager** Notification(s) are not generated even if *Send email notification to manager* option is set on the Transform Password window of a Synchronize job.
28840	**– Leading spaces in SQL statement and Attributes to Inherit issue** This patch provides the followings fixes: • Leading spaces issue in Query Designer's SQL statement • Attributes to inherit option in Smart Group and Dynasties
28841	**– Group Type column issue in Groups' *MemberOf* grid** The patch fixes the issue of the Group Type column appearing blank on the *MemberOf* tab of the Group properties.
28875	**– Resolves object reference error when identity store name is changed** This update fixes the *Object Reference* error which occurs when the name of an identity store is changed.
29073	**– Incorrect error message on SSP Login window** The patch fixes the error that appears on the Self-Service portal's login windows when in the Group policy *MaxPasswordAge* and *MinPasswordAge* are set to zero.
29231	**– German culture support** The patch enables GroupID to run successfully on Windows German version.
29332	**– SSP Smart Group Query Designer filter criteria** The patch fixes the apostrophe sign issue in a Smart Group Query Designer's filter criteria in the Self-Service portal.
29508	**– Bidirectional groups synchronization support** The patch provides cross forest bidirectional Synchronization support for membership and ownership. Having this patch installed, one job group can be created which will provide bi directional support: • Job 1 - Sync from A to B • Job 2 - Sync from B to A

29520	**– Performance Optimization for the count on the *Workflow requests to approve* card and the Workflow Requests listing**
	The patch fixes the issue of loading count on the *workflow requests to approve* card on the Self-Service dashboard. It also optimizes the listing on the Requests page of the Self-Service portal.
	Note:
	After applying the patch, open the *Web.config* file from the following path in a text editor:
	`[GroupID Installation Drive]:\Program Files\Imanami\GroupID 10.0\GroupIDDataService\`
	Change the following key to true:
	`<add key="useWorkflowApproversFromCache" value="false"/>`

<table>
<tr><th>Patch #</th><th>Description</th></tr>
<tr><td colspan="2"><b>29621 – Fix for Access and Visibility on Prefix field</b>
The patch fixes the issues of Access and Visibility options for the prefix field in the Self-Service portal.</td></tr>
<tr><td colspan="2"><b>29641 – Replication service name issue in event viewer logs</b>
The patch fixes the Imanami Replication service name issue in the event viewer logs.</td></tr>
<tr><td colspan="2"><b>29688 –Users are not able to login via SAML Authentication</b>
This patch provides the fix for users who are not able to login via SAML Authentication if a special character exists in the firstname/lastname/disIpayName/SamAccountName attributes' values.</td></tr>
<tr><td colspan="2"><b>30407 – Incorrect preview results with Double Type attributes</b>
This patch fixes the issue of incorrect Preview results in the Query Designer window when a double type attribute is used in a Smart Group query.</td></tr>
<tr><td colspan="2"><b>30504 – Query syntax not fetching SQL data and generating error message</b>
This update fixes the issue of database Smart Groups query syntax issue. With a minor issue in syntax, the query is not fetching SQL data and generating error message.</td></tr>
<tr><td colspan="2"><b>30528 – Self-Service portal crashes</b>
After applying patch no. 29520, the Self-Service portal stops responding/crashes.
Note:
After applying the patch, open the <i>Web.config</i> file from the following path in a text editor:
<code>[GroupID Installation Drive]:\Program Files\Imanami\GroupID 10.0\GroupIDDataService\</code>
Change the following key to true:
<code>&lt;add key="useWorkflowApproversFromCache" value="false"/&gt;</code></td></tr>
<tr><td colspan="2"><b>30611 – Query mismatch issue in Self-Service and Automate</b>
This patch resolves the query mismatch issue in Self-Service portal and Automate. In Self-Service, in a Smart Group query the attribute <i>userAccountControl</i> with AnyflagOff=2' is showing correct result but in Automate this attribute is showing inconsistent results.</td></tr>
<tr><td colspan="2"><b>30619 – Fixes replication issue of migrated user in AD</b>
Fixes replication issue of migrated user in AD and its direct reports removal from dynasty on update</td></tr>
<tr><td colspan="2"><b>30638 – Smart Group reports not displaying correct results</b>
The patch fixes the issue of the following two reports. The reports are not showing the correct results:
• Smart Groups and number of expected members
• Smart Groups and their expected membership</td></tr>
<tr><td colspan="2"><b>30668 – Resolves the "JOBNAME" tag in subject line of Smart Group notification</b>
The patch fixes the issue of "%JOBNAME%" tag issue in the subject line of the Smart Group Update notification. The tag is not getting resolved.</td></tr>
<tr><td colspan="2"><b>30815 – Reset Filter issue in Request Inbox listing</b>
On the Requests pages in Self-Service portal, the <i>Reset Filters</i> button is not working.</td></tr>
</table>

Patch #	Description
30818	**– Revert AuthOrig value to "not Set"** This update fixes the issue for reverting the value of AuthOrig/UnAuthOrig to default empty value when user tries to update a mail enabled user.

30900	**– Bulk history export and history filters loading issue**
	This patch provides a fix for bulk history export and history filters loading issue. Batch size for history export is set to 100,000 by default and it can be adjusted in Imanami.GroupID.Snapin.dll.config file at:
	`[GroupID Installation Drive]:\Program Files\Imanami\GroupID 10.0\`
	by adding the following line inside <appSettings></appSettings>:
	`<add key=,,HistoryExportLimit" value=200000>`

30933	**– MMC crashes upon setting up portal name as any default navigation link** This patch contains fix for the issue when setting up a Self-Service portal name same as any of the Self-Service portal default navigation links causes GroupID Management Console to crash.
31101	**– Expired/Expiring Group reports generation on changed location Issue** While generating Expired/Expiring Groups report, if a user tries to save the report at any location other than the default location, GroupID gives an error.
31107	**– Portal shows duplicate group name prefixes** If same prefixes are defined for multiple roles, those prefixes are listed as duplicate prefixes to users while creating groups in Self-Service portal.
31110	**– *groupType* Attribute inheritance in Dynasties** This patch provides a fix for the issue where GroupID always inherit the *groupType* attribute to leaf/child dynasties on Parent Dynasty update, even it is present or not present in the selected inherited attributes list of Dynasties configuration.
31111	**– History summary filters not loading** Against the History Summary node in GroupID Management Console, criteria filter boxes do not display list options.
31253	**– *whenChanged* or *whenCreated* columns issue** In GroupID Management Console Automate listing, upon adding *whenCreated* and *whenChcanged* columns, GroupID throws the following exception: *The attribute syntax specified to the directory service is invalid.* This error occurs when a static to Smart Group/Dynasty upgrade is performed.
31372	**– Membership sync issue after deletion of objects from AD** The patch fixes the issue of Smart Group membership after deletion of objects from Active Directory.
31410	**– Additional Owner column in SSP and MMC sorted differently** Additional Owner column in GroupID Management Console and in Self-Service portal is sorted differently.
31413	**– "Unable to search/add Computer object in group" issue.** In a Self-Service portal, computer objects do not appear in searches and are not available to be added as members in a group.

Patch #	Description
31456 – User is not redirected to Custom URL This patch redirects users to Custom URL when the session is lost with SAML provider.	
31644 – Accept from and Reject from Access Role The patch fixes *Accept from* and *Reject from* Access Role issue on the Delivery Restrictions tab in the Self-Service portal (in GroupID 10 SR1).	
31681 – Computer object addition issue in create wizard for groups This patch fixes the error that occurs while adding computer objects as members on the Members tab of the Group Create wizard in Self-Service portal. Note: This patch will work on those Self-Service portals created after the deployment of this patch.	
31738 – Object Reference Error when selecting *Update only records that have changed* with *whenChanged* attribute This patch solves object reference error in Synchronize. In an AD to AD Synchronize job when selecting the *update only records that have changed* option with *whenChanged* attribute.	
31744 – Inconsistent time format in Automate listings This patch fixes the time format inconsistency w.r.t GroupID machine's time zone in Automate listings columns (*whenchanged*. *when created*, *Modified* attributes).	
31816 – Smart Group Update schedule run with *Memberof* criteria This patch fixes the *MemberOf* criteria issue that occurs after the Smart Group Update schedule run created via GroupID Management Schedule. Note: For users upgraded from a previous GroupID version, user object replication to Elastic from scratch is required after the deployment of this patch.	
31844 – Missing *managedBy/Manager* values in history export The patch provides a fix for exporting new and old attribute (*managedBy*/Manager) values while exporting history which were getting missed earlier.	
31899 – Changing Search Guard user password Issue from Replication node This patch fixes the issue of changing Search Guard's admin user password from the Replication node in GroupID Management Console. See Appendix C for details.	
31915 – Group Properties Update issue in AD identity store with LDAPS This patch fixes the Group properties update issue (groups with # sign in their cn) in an Active Directory identity store that has LDAPS configured.	
31993 – MS365 Groups Properties update issue in Azure identity store This patch fixes the properties update issue with MS365 groups having the *Azure AD roles can be assigned to the group* option enabled.	

32044 – Management Shell command executes successfully even if data is incorrect
The patch fixes the issue of Management Shell cmdlets, New-Group and Set-Group. These cmdlets are getting executed successfully even if the provided data is incorrect for optional parameters. A switch -ValidateData "True" has been added to validate the following attributes:
`Set-Group/SmartGroup/Dynasty Attributes:`
`AcceptMessagesOnlyFrom,`	

Patch #	Description

`AuthOrig .AcceptMessagesOnlyFromGroups .dlmemsubmitprems, RejectMessagesFrom , Unauthorig , RejectMessagesFromGroups, dlmemrejectprems, ownerlnclude, IncludeRecipients, ExcludeRecipients. Member AdditionalOwner New-Group/SmartGroup/Dynasty Attributes:`
`IncludeRecipients, ExcludeRecipients. Members, AdditionalOwner, Top Manager, Owner`	

32137 – Quick Add Button Issue on *Unauthorig* Field on Group Create wizard This patch fixes the Quick Add button issue on *Unauthorig* field on the Group Create wizard, when it is added in the Design node of AD identity store and DNs is selected as its Display Type.	
32179 – Dynasty membership issue This patch fixes the issue of Dynasty Membership. After the deployment of the patch when a parent dynasty is updated (with *Delete empty and orphan dynasty* option unchecked) and a child dynasty gets empty or orphan it will not deleted but kept as an empty dynasty.	
32199 – Search policy set in a security role issue in Automate This patch fixes the Search Policy set in a security role issue in Automate All Group's search scope.	
32277 – Recursive Flat Managerial Dynasty Create/Delete Issue This patch fixes the Create/Delete issue of a Recursive Flat Managerial Dynasty when they are not according to the criteria.	
32346 – Self-service portal dashboard cards issue with azure app proxy This update fixes the Dashboard card error when Self-Service portal is accessed via Azure App Proxy.	
32347 – Computer objects issue in Groups and Members report This patch fixes the issue of computer objects in the *Groups and members* Report. See Appendix B for details.	
32536 – Frist login attempt taking too long after IIS reset This patch provides a fix for the login attempt to take too long after IIS reset, or App Pool recycle. For details, see Appendix E.	
32660 – Quick Add issue in Smart Group Query Designer The patch fixes the issue of Quick Add in Smart Group Query Designer of Self-Service portal.	
32694 – Smart group Preview count issue in Query Designer in Automate and SSP The path resolves Smart Group Preview count issue in Query Designer both in Automate and Self-Service portal.	
32697 – No identity store exists on login attempt on SSP The patch fixes the issue of *No identity stor*e exists error displayed while logging in to Self-Service portal. The error occurs when GroupID App Pool gets crashed or recycled.	

<table>
<tr><th>Patch #</th><th>Description</th></tr>
<tr><td colspan="2"><b>32807 – 'Get-GroupMember' Command's Return Type issue for Empty Groups</b>
In GroupID Management Shell, the <i>Get-GroupMember</i> cmdlet for empty groups displays the (newline) before and after the message:
"(newline) No members found (newline)"</td></tr>
<tr><td colspan="2"><b>32952 – Smart Group Update job notifications</b>
The Smart Group Update job sends success notification to the specified recipients while the job is configured to send notifications on failure.</td></tr>
<tr><td colspan="2"><b>32963 – log4j Vulnerability</b>
The patch mitigates the CVE-2021-45046 & CVE-2021-44228 vulnerabilities reported for log4j.</td></tr>
<tr><td colspan="2"><b>32968 – Suppress status output of a cmdlet in GroupID Management Shell</b>
The patch resolves the issue of Suppress status output of a command in GroupID Management Shell.</td></tr>
<tr><td colspan="2"><b>33002 – Manager can update attribute replication issue with Preferred DC configuration</b>
The patch fixes the replication issue of the <i>Manager can update</i> attribute with the preferred DC configuration. For details, see Appendix D.</td></tr>
<tr><td colspan="2"><b>33105 – "<i>is unique</i>" field issue with custom display type on the <i>Name</i> attribute</b>
The patch fixes the <i>is unique</i> field issue with custom display type on the <i>Name</i> attribute while creating a group using the Self-Service portal.</td></tr>
<tr><td colspan="2"><b>33106 – Links in the Emails are Different for object update notification from SSP and Shell</b>
Links in the object update emails are different for actions performed from the Self-Service portal and GroupID Management Shell.</td></tr>
<tr><td colspan="2"><b>33469 – Smart Groups and number of expected members Report issue on creation</b>
The patch resolves the issue of the <i>Smart Groups and number of expected members</i> report upon creation and snapshot file empty on downloaded location.</td></tr>
<tr><td colspan="2"><b>33660 - Updates for Azure identity store</b>
The following patches for Azure identity store have been merged into this patch:
• Identity store replication issue when there is a special character in its service account password
• Employeeld attribute replication issue
• Support to manage distribution groups
• Notes field issue</td></tr>
<tr><td colspan="2"><b>33743 – Groups and Members Reports Issue</b>
The patch resolves the issue of membership not displayed in the <i>Groups and members</i> report when the <i>PhysicalDeliveryOfficeName</i> attribute or other attributes under members are removed.</td></tr>
<tr><td colspan="2"><b>34743 – Include/Exclude tab issue while converting a Smart Group into a Static Group</b>
When a Smart Group/Dynasty is converted into a static group, the objects present in Include are removed from membership.</td></tr>
</table>

<table>
<tr><th>Patch #</th><th>Description</th></tr>
<tr><td colspan="2"><b>34747 – Quick search issue with copy and paste text with right click in SSP</b>
The patch resolves the issue of Quick Search with copy and paste with right-click in the Self-Service portal.</td></tr>
<tr><td colspan="2"><b>34749 – IIS crash issue with unhandled exception</b>
Having patch numbers 30528 and 29520 installed, unhandled exception occurs which causes IIS crash.</td></tr>
<tr><td colspan="2"><b>34767 – Null value exception upon Authentication through SAML IDP flow</b>
The patch fixes the null value exception displayed on SSP portal after launching the application through SAML IDP Flow and custom URL redirection by authenticating the user through SAML provider.</td></tr>
<tr><td colspan="2"><b>35053 – Replication attribute removal issue with Automate only license</b>
The patch resolves the issue of replication attributes removal with Automate license only.</td></tr>
<tr><td colspan="2"><b>35458 – SAML authentication issue when GroupID is configured with GMSA</b>
This patch fixes SAML authentication issue when GroupID is configured with gMSA having authentication page disabled.</td></tr>
<tr><td colspan="2"><b>35528 – Error message on Session expiry and multiple triggering of workflow requests on object creation</b>
The patch fixes the session expiry error message and triggering of multiple workflow requests upon object creation.</td></tr>
<tr><td colspan="2"><b>35553 – Exception upon any action on GroupID if session is lost with Azure provider</b>
The patch fixes the exception if the session is expired with Azure provider.</td></tr>
<tr><td colspan="2"><b>35561 – Loading identity store properties issue</b>
The patch resolves the loading issue of identity store properties.</td></tr>
<tr><td colspan="2"><b>35633 – Azure AD identity store replication issue for Group objects</b>
The patch resolves the Azure AD identity store replication issue for Group objects.</td></tr>
<tr><td colspan="2"><b>35755 – Bulk history Export issue from Self-Service portal</b>
The path fixes the issue of bulk history export from SSP.
Add the following key values in the a<i>ppSettings</i> tag in the <i>Applicationconfig/web.config</i> file of MMC GroupID snap-in, Self-Service portals and Password Center portals (User + Helpdesk) respectively:
• To increase/decrease message size length for a single message received on service:
<add key="Services.MaxReceivedMessageSize" value="2147483647" />
• To set the maximum amount of memory allocated for a message:
<add key="Services.MaxBufferPoolSize" value="2147483647" />
NOTE
• In absence of these keys, default value (<i>2147483647; integer value in byte</i>) will be applied.
• <i>MaxReceivedMessageSize</i> should be less than or equal to <i>MaxBufferPoolSize</i>.</td></tr>
</table>

Patch #	Description
Path of MMC GroupID snap-in Applicationconfig file: `[GroupID Installation Drive]:\Program Files\Imanami\GroupID 10.0\imanami.GroupID.snapin.dll.config` **Path of Self-Service web.config file:** [GroupID Installation Drive]:\Program Files\Imanami\GroupID 10.0\SelfService\Inetpub\[*portal name*]\Web\ **Path of Password Center (User portal) web.config file:** C:\Program Files\Imanami\GroupID 10.0\PasswordCenter\Inetpub\[*portal name*]\Web\ **Path of Password Center (Helpdesk portal) web.config file:** C:\Program Files\Imanami\GroupID 10.0\PasswordCenter\Helpdesk\Inetpub\[*portal name*]\Web\	
35804 – Group Attestation of Child Dynasties Child dynasties (Middle/Leaf) will be attested but not renewed. If we are attesting a child Dynasty (middle/leaf) or a Smart Group and if they have Dynasties/child groups in their membership then those groups will not appear in membership during Group Attestation.	
35879 – Start-In issue on updating Parent Dynasty The patch resolves the issue when changing Start-In value while updating the Parent Dynasty.	
35882 – Imanami Management service for AppPool Recycle The patch installs Imanami Management service and resolves the issues related to AppPool recycle and DB cleanup. See Appendix F for details.	
35885 – Extension attribute support for Azure Identity store Extension property attributes and custom extension attributes will be replicated and can be used in Query Designer of Smart Groups.	
36189 – Managerial dynasty issue with "Exclude nested lists of direct report" checked The patch fixes the issue of Managerial dynasty when the *Exclude nested lists of direct report* option is checked.	
36319 – History Export issue for member attribute's old and new value The patch fixes the issue of history export for member attribute's old and new values.	
36367 – History export issue from Self-Service portal Fixes the issue of History export from Self-Service. After deploying patch add following key in web.config file of portal Add the key in web.config file of portal: <addkey="CompressExportHistory" value="true" />	

Patch #	Description
36460	**– Cn\SamAccountName attribute being used as a key attribute** The patch resolves the issue of a Synchronize job, Cn\SamAccountName attribute is being used as a key attribute even if another attribute (e.g. EmployeeID) being configured as a key attribute.
36461	**– SamAccountName attribute update issue on user object properties in Self-Service** The patch fixes the issue of *SamAccountName* attribute update on user object properties in Self- Service portal.
37040	**– Fix for Managerial Dynasty upgrade** This patch fixes the issue of a Managerial Dynasty when upgraded from GroupID 7.
39159	**– Self-Service portal's vulnerability issue fixed** The patch fixes the XSS vulnerability listing issue in Self-Service portal.
39895	**– Insights replication** Insights replication has been optimized.
39899	**– Optimized workflow listings** Workflow listings in Automate and Self-Service have been optimized.
39950	**– Octet String attributes issue in AD** The patch fixes the Octet String Attributes issue in Active Directory. After applying the patch, you must run the replication process.
40028	**– Date Display type issue in Self-Service portal** The patch fixes the issue of the Date Display type in the Self-Service portal.

40029	**– Prefix enforcement in Automate**
	The patch enables prefix enforcement on Group update event in Automate.
	Steps:
	1. Close GroupID Management Console
	2. From the following path:
	`[GroupID Installation Drive]:\Program Files\Imanami\GroupID 10.0\`
	3. Open Imanami.GroupID.Snapin.dll in a text editor. Add the following key under appSettings:
	`<add key="EnforcePrefixOnUpdate" value="False7>`
	4. Save the file and launch GroupID again.

40955	**– Exchange Advanced and Exchange General tabs in Automate for AD and MS365** The patch enables the *Exchange Advanced* and *Exchange General* tabs in Automate for Active Directory and MS365 environments.
40956	**– All Requests option not visible in GroupID Management Console** With a Self-Service license, the All Request option in GroupID Management Console is not shown. Steps: 1. Close GroupID Management Console. 2. Extend Active Directory schema.

<table>
<tr><th>Patch #</th><th>Description</th></tr>
<tr><td colspan="2">3. Synchronize attributes in Exchange Advanced and Exchange General tabs using AAD Connect.</td></tr>
<tr><td colspan="2"><b>43922 – <i>PasswordNeverExpires</i> checkbox in Self-Service portal</b>
After the deployment of this patch, the <i>PasswordNeverExpire</i> field can be displayed on User property page in the Self-Service portal.</td></tr>
<tr><td colspan="2"><b>43937 – Smart Group Schedule listing</b>
Smart Group bind to a schedule having OU as target scope is not shown in Self-Service portal’s listing.</td></tr>
<tr><td colspan="2"><b>44145 – Unique values for object attributes</b>
The patch ensures every object's attributes have unique values.</td></tr>
<tr><td colspan="2"><b>44152 – Convert-Group cmdlet populates all domain objects in Include list</b>
Convert-Group cmdlet of GroupID Management Shell populates all domain objects in the include list of a Smart Group although the Include column is empty in the imported CSV file.</td></tr>
<tr><td colspan="2"><b>44198 – Smart Group Membership issue</b>
Upon Smart Group membership update, all users' attribute <i>memberof</i> is not handled correctly.</td></tr>
<tr><td colspan="2"><b>44201 – Multiple issues fixed</b>
The patch fixes the following issues:
• OOB notification in case of Flat Recursive dynasty
• Nest workflow support while group creation
• Schedule listing in Self-Service Smart Group properties
• Real-time field validation for the Contact object type
• Query crashes while a Smart Group updates Include/Exclude info</td></tr>
<tr><td colspan="2"><b>44385 – Smart Group scheduler name missing when jobs run simultaneously</b>
When multiple scheduled jobs are executed simultaneously, Smart Group scheduler name is missing in the notification email.</td></tr>
<tr><td colspan="2"><b>44458 – Groups are getting extended</b>
The patch fixes the issue of groups getting extended when no notification is sent by GLM.</td></tr>
<tr><td colspan="2"><b>44526 – Multiple issues fixed</b>
The patch fixes the following issues:
• Performance optimization in Request Inbox listing
• DL and Security Group Expansion issue in Notification
• Request not listing if objects are added in <i>msExchCoManagedßyünk</i> attribute
• Request not listing if Disabled mailbox is set as an approver
• Additional owner Do Notify issue</td></tr>
<tr><td colspan="2"><b>44758 – Allow objects with leading/trailing spaces in their attributes values as group members</b>
The patch enables users to be added to a group membership that has specified attributes values' with leading/trailing spaces. They can be modified as follows:</td></tr>
</table>

Patch #	Description
1. From the file path: [GroupID Installation Drive]:\Program Files\Imanami\GroupID 10.0\ Open the *attribute-no-trim.dat* file in a text editor. 2. Add the required attributes that need to be replicated with leading/trailing spaces. Each line must contain only one attribute and there must not be any empty line in the file. 3. Whenever the data file is updated, restart IIS and Imanami Replication Service.	
44834 – Password Center Helpdesk portal reset password issue in restricted mode The patch fixes the issue in Password Center Helpdesk portal (restricted mode) when the *Don't allow Helpdesk to reset password without user's interaction* option is unchecked.	
44934 – Ampersand sign '&' issue in Group Name When a group is created using the Self-Service portal and a special character is used in its Name field, the special character is converted to &amp.	
45166 – Cryptographic error on Self-Service This patch fixes the cryptographic error in the Self-Service portal. This error occurs when the portal's session times out or when a user is rerouted to another GroupID server in a load-balanced scenario.	
45197 – Smart Group note addition when group is created via GroupID Management Shell When a Smart Group is created using GroupID Management Console, the following note appears in the Note field of Group properties: *This is an automated group, please do not modify membership. Membership is controlled by GroupID.* But when a group is created via GroupID Management Shell, this note does not appear. This patch fixes this issue.	
45466 – Attribute *imsgquickfilter* value set to 3 issue This patch provides fix for the *imsgquickfilter* attribute value set to 3 issue in Automate. After the deployment of the patch, open file *imsgquickfilter.ps1* placed at the following path: `[GroupID Installation Drive]:\Program Files\Imanami\GroupID 10.0\` After executing this file in GroupID Management Shell, the issue will be fixed.	

45486 – Removal of Include/Exclude list with invalid value
In GroupID Management Shell cmdlets:
`Set-Group -Add @{lncludes=Muser.name"}`
and
`Set-Group -Remove @{lncludes=Muser.name"}, for Smartgroup/Dynasty,`
Include/Exclude list gets removed when a user enters an invalid value for username (*Muser.name*).	

45537 – SmartGroup Update history issue Upon bulk membership update of a Smart Group, history is not logged.	

Patch #	Description
45661 – CPU spikes optimization for concurrent sessions	The patch fixes the issue of CPU consumption for concurrent sessions of Self-Service portal.
45745 – Temporary membership status after upgrade	This patch fixes the temporary membership status issue after running the upgrade from a previous version. After applying the patch, run the following GroupID Management Shell cmdlet: `Fix-MembershipType -IdentityStoreId 1 -Verbose` Specify the correct identity store ID to fix the invalid membership types. The cmdlet also writes the logs to *%temp%\logManagementShell.gid.log* file.

45748 –Performance of GUS scheduler	This patch fixes the performance issues of GUS scheduler.
	1. Open the *web.config* file from the following path:
	`[GroupID Installation Drive]:\Program Files\Imanami\GroupID 10.0\GroupIDDataService\`
	2. Add the following lines inside <appSettings> </appSettings> tags:
	`<add key="batchsize" value="500" />`
	`<add key="usegus" value="true" />`
	`<add key=historyparaller value=false" />`
	Batch size can be adjusted also, by setting *usegus* to false.
	Note: By doing this, optimized performance of this patch will be opted out and old implementation of GUS will be in action.

45859 – Helpdesk user account lockout status when GPO set to 0	Fixes the issue of user account lockout status on Helpdesk portal, either user is locked or not, when Account lockout (GPO) settings is set to 0 minutes.
IGU2020-0001 — Query results different in ADUC and Query Designer window	ADUC and the Preview option in the Query Designer window display different results for the same LDAP query.
IGU2020-0002 — Parenthesis in an SQL data source column gives error	In the Query Designer window, if SQL data source is used with a column name having a parenthesis, an error is displayed.
IGU2020-0003 – Identity store for a child domain	If GroupID is connected with a domain that has a child domain and identity store for that child domain is not created then GroupID reports are not generated.
IGU2020-0004 – Automate issues and exception notification in Target column of a scheduled job	In this patch, multiple Automate issues in Query Designer when an external data source is used in a Smart Group query. • Column name is not properly ordered with CSV data source • External data source key mapping drop down does not work if an external database contains a single column

Patch #	Description
• Database Smart Group not executing the query properly if it has Enter key/New Line key character The patch also fixes issue of exception notification in the *Target* column of a scheduled job.	
IGU2020-0005 – Smart Group Update job is failing Smart Group Update job fails if objects in the job are not resolved.	
OOB002 – OOB (Threshold) values for Flat/Recursive Flat Managerial dynasty If Out of Bound (threshold) values are specified for a Flat Managerial or Recursive Flat Managerial dynasty, an error occurs while updating the dynasty.	
Replication002 – Replication time-out Replication time-out session issue has been fixed.	
SelfService0001 – Multiple Self-Service portal issues fixed This patch fixes multiple Self Service portal issues: • Export option does not export Additional Group • Ownership Nullable object must have a value • Error on SSP vulnerabilities in Self-Service portal • Group advanced search based on smart query/criteria is not working properly. Group type is not showing in Members grid	

Upgrade Notes

1. When you upgrade from GroupID 10 SR1 to GroupID SR2 on a different machine then you must run restore replication after upgrade.

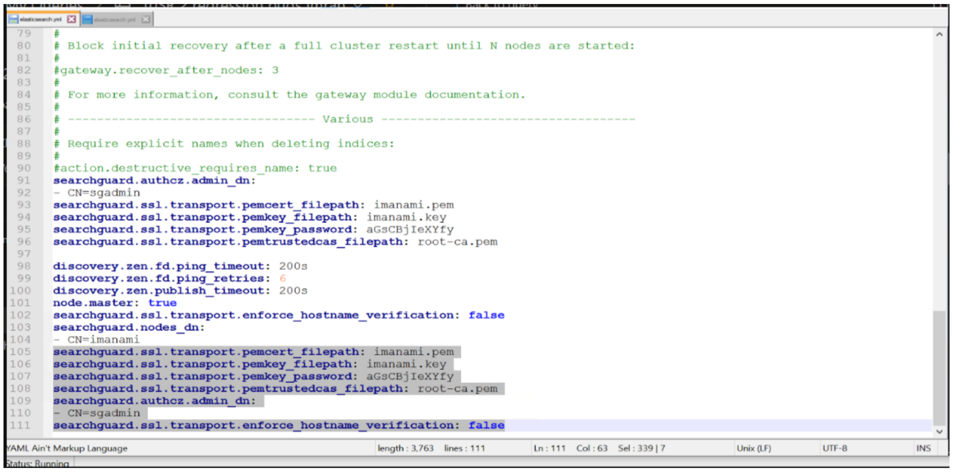
2. Custom navigation links defined in GroupID 7 will not persist after upgrade to GroupID10 SR2 and will require reconfiguration.

3. Group name prefixes defined in GroupID 7 portals will not persist after upgrade to GroupID 10 SR2. You have to redefine them.

4. While upgrading to GID 10 SR 2 Elasticsearch service might get stuck during the GroupID Configuration Tool. (Same box).
   The issue occurs due to one missing tag at the time of Search Guard certificates configuration in GroupID10 SR1. This causes duplicate entries of Search Guard related tags in the *Elasticsearch.yml* file at the following path:

   ```
   [GroupID Installation Drive]:\Program Files\Imanami\GroupID
   10.0\ElasticSearch\elasticsearch-6.2.4\config\
   ```

   Remove these duplicate entries in the file (*as shown in the following snapshot*) and the issue will be resolved.

   
   elasticsearch.yml
elasticsearch.yml
YAML Ain't Markup Language
length : 3,763   lines : 111
Ln : 111   Col : 63   Sel : 339 | 7
Unix (LF)
UTF-8
INS
Status: Running

   ```
   #
   # Block initial recovery after a full cluster restart until N nodes are started:
   #
   #gateway.recover_after_nodes: 3
   #
   # For more information, consult the gateway module documentation.
   #
   # ---------------------------------- Various -----------------------------------
   #
   # Require explicit names when deleting indices:
   #
   #action.destructive_requires_name: true
   searchguard.authcz.admin_dn:
   - CN=sgadmin
   searchguard.ssl.transport.pemcert_filepath: imanami.pem
   searchguard.ssl.transport.pemkey_filepath: imanami.key
   searchguard.ssl.transport.pemkey_password: aGsCBjIeXYfy
   searchguard.ssl.transport.pemtrustedcas_filepath: root-ca.pem

   discovery.zen.fd.ping_timeout: 200s
   discovery.zen.fd.ping_retries: 6
   discovery.zen.publish_timeout: 200s
   node.master: true
   searchguard.ssl.transport.enforce_hostname_verification: false
   searchguard.nodes_dn:
   - CN=imanami
   searchguard.ssl.transport.pemcert_filepath: imanami.pem
   searchguard.ssl.transport.pemkey_filepath: imanami.key
   searchguard.ssl.transport.pemkey_password: aGsCBjIeXYfy
   searchguard.ssl.transport.pemtrustedcas_filepath: root-ca.pem
   searchguard.authcz.admin_dn:
   - CN=sgadmin
   searchguard.ssl.transport.enforce_hostname_verification: false
   ```

5. When upgrading from a previous version, an Azure identity to GroupID10 SR2, Imanamai Replication Service replicates objects to Elastic, but not distribution lists. They will be replicated when Certificate Thumbprint is provided in the Azure identity store in GroupID.

6. Microsoft's throttling policy restricts an application (such as GroupID) to create a maximum of 3 concurrent sessions with Microsoft Azure. With this in view, GroupID allows only one active session at any given time, which is used by GroupID Data service and Imanami Replication service.

7. After upgrading from a previous GroupID version to GroupID 10 SR2, for an existing Azure identity store you have to perform the following steps:

    a. run the schema replication scheduler, SchemReplication_schemaReplication (defined in Windows Task Scheduler) to update the schema for the identity store.

    b. provide certificate Thumbprint in the identity store properties.

    c. run restore replication.

8. A Synchronize job to create mailbox with Office 365 as a messaging provider will not be upgrade to GroupID SR 2. You need to recreate the job by providing Certificate Thumbprint assigned to the certificate you uploaded in Azure portal while configuring GroupID.

9. If you install GroupID 10 SR2 on a different box by copying GroupID database of GroupID 10 SR1, copy the attribute to replicate list, Self-Service and Password Center folders from GroupID 10 SR1 box to GroupID 10 SR2 box. For details see the **Appendix D – Backing Up and Restoring GroupID Data** in the *GroupID 10 Installation & Configuration Guide*.

    The following section provides instructions for backing up and restoring the data from GroupID 10 SR1 box to GroupID 10 SR2 box:

    Attribute to replicate list of Identity stores

    Backup

    Follow these steps to back up the attribute to replicate list from GroupID SR1 box:

    a. Go to the following location on GroupID 10 SR1 box:

    ```
    [GroupID Installation Drive]:\Program
    Files\Imanami\GroupID 10.0\Replication\
    ```

    b. Copy the *IdentityStoresReplicationAttributes* folder.
    c. Create a new folder (ideally on a different drive) and paste the copied data into that folder.

    Restore

    Follow these steps to restore attribute to replicate list of identity store(s) on GroupID 10 SR2 box:

    a. Copy the folder from the backup folder you created in the previous steps.
    b. Go to the following location on GroupID 10 SR2 box:

    ```
    [GroupID Installation Drive]:\Program
    Files\Imanami\GroupID 10.0\Replication\
    ```

    c. Paste the copied folder at the above location.

GroupID Self-Service Portals

Back Up

Follow these steps to back up the Self-Service portals created using GroupID 10 SR1:

a. Go to the Inetpub folder:

```
[GroupID Installation Drive]:\Program
Files\Imanami\GroupID 10.0\SelfService\Inetpub\
```

b. Copy the folder for each virtual server or portal.
c. Create a new folder (ideally on a different drive) and paste the copied data into that folder.

Restore

Follow these steps to restore GroupID Self-Service portals:

a. Copy the folders containing the portals from the backup folder you created in the previous steps.
b. Go to the Inetpub folder on the GroupID 10 SR2 box.

```
[GroupID Installation Drive]:\Program
Files\Imanami\GroupID 10.0\SelfService\Inetpub\
```

c. Paste the copied data in the location.

GroupID Password Center Portals

Back Up

Follow these steps to back up Password Center User and Helpdesk portals created on GroupID SR1 box:

a. Go to the PasswordCenter folder of the product's installation directory:

```
[GroupID Installation Drive]:\Program
Files\Imanami\GroupID 10.0\PasswordCenter\Inetpub\
```

```
[GroupID Installation Drive]:\Program
Files\Imanami\\GroupID
10.0\PasswordCenter\Helpdesk\Inetpub\
```

b. Copy the folders of each portal from the above two folders.
c. Create new folders (on a different drive) and paste the copied data into those folders.

Restore

Follow these steps to restore Password Center portals to GroupID 10 SR2 box:

a. Copy the folders containing the Password Center portals from the backup folder you created in the previous steps.

```
[GroupID Installation Drive]:\Program
Files\Imanami\GroupID 10.0\PasswordCenter\Inetpub\
```

```
[GroupID Installation Drive]:\Program
Files\Imanami\\GroupID
10.0\PasswordCenter\Helpdesk\Inetpub\
```

b. Go to the PasswordCenter\ folder of the GroupID installation directory:
c. Paste the copied data in the location.

Known Issues

1.	User is unable to enroll their identity store account with YubiKey.
2.	On the MFA selection page, the *Go Back to select different authentication* option redirects to the login page rather than to the MFA selection page.
3.	Linked mailbox users are not created correctly even though two-way trust has been established between the domains
4.	Workflow approver acceleration history is not shown in GroupID Management Console but displayed in the exported file.
5.	When a user rearranges attributes under Mailbox, the MMC crashes.
6.	In update wizard mode, the direct reports URL takes a user to object reference screen.
7.	When a user adds new members to a group, it blocks pagination.
	While creating/updating Flat Managerial Dynasty, an incorrect Out of Bounds error message is displayed.
8.	When a user selects Redirect as Request Binding mechanism at GroupID and Provider end, they are unable to authenticate, and an error message is displayed.
9.	The Self-Service portal does not display contact under manager suggestion even if user/contact's department is same as targeted user's department.
10.	In Automate, when Set Manager as Owner check box is selected, the top manager is listed in the Additional Owners grid and is not getting removed.
	If a linked user is deleted through GroupID portal, the master account and other linked accounts are unable to reset their passwords on Password Center User portal.
	When a user updates object type in General tab of Smart Group query, the Self-Service portal does not display correct history of object type update.
	After deleting top manager, the Dynasty Options page for Managerial Dynasties displays object reference exception.
11.	When a GroupID security role is copied using the Role Copy feature, membership of the role is not resolved.
	Identity store of a child domain is not created using a gMSA account.
	When a user adds alias to a mapped database column attribute, object reference exception is thrown and Smart Group criteria gets corrupted.
12.	When a user sets a new criteria, database attribute from attribute list changes to CN on preview.
13.	The Insights dashboard does not display stats when bulk data objects are replicated. It also takes some time before displaying shared folders on the File Server page.

14.	After creating a group, the *Smart Group and Number of Expected Member Report* is not generated and the downloaded snapshot file is also empty.
15.	In multi-factor authentication, UI gets disturbed if multiple authentication factors including PhoneID are required.
16.	In the Self-Service portal, *My expiring groups* tab is not displaying those groups to which the logged-in user is an additional owner.
17.	When a user creates a group and selects *Other* as expiration policy, the properties still display the expiration policy as *Never Expire*.
18.	Status of additional manager with *'addition pending'* doesn't update to temporary manager when Managedby lifecycle job runs at its beginning date.
19.	When a user creates or modifies a static group with the scope Global, the Quick Add Search displays Universal Groups.
20.	Quick Add Search does not display Domain Local groups in domain local group and universal group creation. Similarly, it does not display global groups Domain Local group properties.
21.	When a wrong SMS gateway is configured, no error message is displayed to a user upon getting enrolled through the mobile authentication type.
	Self-Service portal does not display *membership type*, *beginning date* and *ending date* filters on user's Member Of tab.
22.	Self-Service portal does not display *ending date* filter on group's Member tab.
23.	While upgrading from GroupID 9 SR1 to GroupID 10 SR2, an error occurred on the Mobile Service module.
24.	In Security Roles Helpdesk polices, *Don't allow helpdesk to reset password without end user's interaction* checkbox is unchecked by default and Restricted mode behaves same as Un-restricted mode by default.
25.	When a user scrolls through the results in query designer in Automate, an error message is displayed.
26.	If you click on the name of a Manager (mailbox user), it displays its properties on Self-Service portal in the User profile > Organization tab.
27.	In Self-Service portal, when objects are exported through Group properties, escape characters i.e. &, " etc. are displayed as html strings.
28.	After adding triggers in schedule, it displays incorrect date and expiry date is automatically checked.
29.	When a user creates a Smart Group or dynasty and sets a schedule. Work flow doesn't not get triggered and an error message is displayed.

30.	Upon resetting password with *Enforce Multifactor authentication as applies to user* option and minimum multifactor authentication type for the HelpDesk security role is set to 1, an invalid message is displayed.
31.	In Helpdesk policy, value of *Helpdesk must verify answers of atleast N questions* option should be updated according to the number of selected questions in password policy instead of just setting up maximum limit of 5 questions.
32.	Multiple filters for search results are not working. The results keep on loading and do not display.
	In Self-Service portal, a user can self-nest a group through *Add To Group* option in toolbar.
33.	When a user searches an object whose display name starts with a quote i.e., ", the search results display all the objects from the domain instead of following the criteria.
34.	Even if GroupID Management Console is connected with either a parent or a child domain, it is unable to create mailbox users from "Parent to Child" domain.
35.	When a GroupID security role is copied, multi factor authentication policies defined for the role are not copied.
36.	When a user account gets locked after a certain number of failed log on attempts, no error message is displayed.
37.	When the *Delete group* workflow is triggered, the notification displays incorrect message.
38.	In Azure AD, if you update a static group to a Smart Group or dynasty, it does not display the description of the group after the update.
39.	The desktop notification does not display thumbnail photo for a user whose thumbnail photo is set in Azure AD.
40.	In Azure AD, Office365 groups' group type should be listed in the All groups node and search results listing along with security and distribution groups.
41.	The Shared Folder tab does not consider "Files" in "direct file/folder".
42.	History export in .CSV file format has issues if special characters are present in history.
43.	When a user selects *Use identity store service account* option to "Reconnect" under another VM file server, "Access is denied" error message is displayed.
	When a master account’s identity store is removed from the Password Center User portal, child account is unable to reset password using the Password Center portal.
44.	When a master account’s identity store is removed from the Password Center User portal, child linked account can be unlinked using Password Center Helpdesk portal.

45.	When *Add Temporary* membership policy is applied, a temporarily removed member is permanently removed from the membership of a group.
46.	A temporarily removed/added user is not made permanent even after removing the membership policy and clicking *Yes* on the confirmation message to make the user a permanent member.
47.	In Automate, when a user selects multiple groups, they can change Mail-Enabled security groups expiration policy and security type.
48.	User can manually expire Mail-Enabled security groups through the Self-Service portal search listing and through GLM.
49.	When a user adds disallowed passwords with a regular expression rule, an incorrect error message *undefined* is displayed in the Password Center User portal.
	If a user is logged in to Password Center User portal and Password Center Helpdesk portal and then upon logging out of Helpdesk portal, the User portal stops working.
50.	When a new user (not enrolled yet with any enrollment type) tries to enroll with PhoneID app, GroupID displays an error message, *Phone number already registered*.
51.	The Request tab on GroupID Management Console does not display correct value for ObjectCategory and does not resolve ObjectClass.
52.	When a direct report moves from one OU to another on dynasty update, the Start-in does not get updated.
53.	When a manager terminates his/her direct report using the Self-Service portal, a request is sent to an invalid user.
54.	Mailbox create notification does not display subscription lists.
55.	An error message is displayed upon deleting contacts from the Self-Service portal.
56.	Instead of the name, the ObjectID of workflow approver is displayed when create / delete request is approved or denied.

Appendix A

ReadmeFirst.txt File (Patch # 20832)

The steps for converting Elastic URLs from HTTP to HTTPS are available in the ReadmeFirst.txt file at the following path:

```
[GroupID Installation Drive]:\Program Files\Imanami\GroupID 10.0\ElasticSearch\elasticsearch-6.2.4\
```

The steps are:

1. Download the Offline TLS Tool from the given link: https://docs.search-guard.com/latest/offline-tls-tool

2. Unzip the TLS tool and place it in a directory of your choice.

3. Go to the following path:

   ```
   [GroupID Installation Drive]\search-guard-tlstool-1.8\config)
   ```

   Edit *example.yml* as follows.

   - Replace pkPassword: admin with “pkPassword: none”.

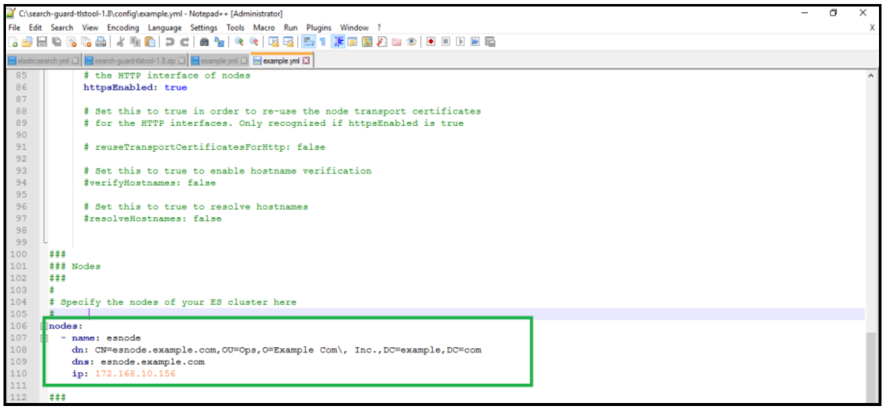
   - Move to nodes tag and remove all the nodes under the tag. Once all the nodes are removed, add the following inside Node tag:

     ```
     “- name: esnode

        dn: CN=esnode.example.com,OU=Ops,O=Example Com\, Inc.,DC=example,DC=com

        dns: esnode.example.com

        ip: (IP of your system)”
     ```


C:\search-guard-tlstool-1.8\config\example.yml - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
elasticsearch.yml
search-guard-tlstool-1.8.zip
example.yml
example.yml

```
        # the HTTP interface of nodes
        httpsEnabled: true

        # Set this to true in order to re-use the node transport certificates
        # for the HTTP interfaces. Only recognized if httpsEnabled is true

        # reuseTransportCertificatesForHttp: false

        # Set this to true to enable hostname verification
        #verifyHostnames: false

        # Set this to true to resolve hostnames
        #resolveHostnames: false


###
### Nodes
###
#
# Specify the nodes of your ES cluster here
#
nodes:
  - name: esnode
    dn: CN=esnode.example.com,OU=Ops,O=Example Com\, Inc.,DC=example,DC=com
    dns: esnode.example.com
    ip: 172.168.10.156

###
```

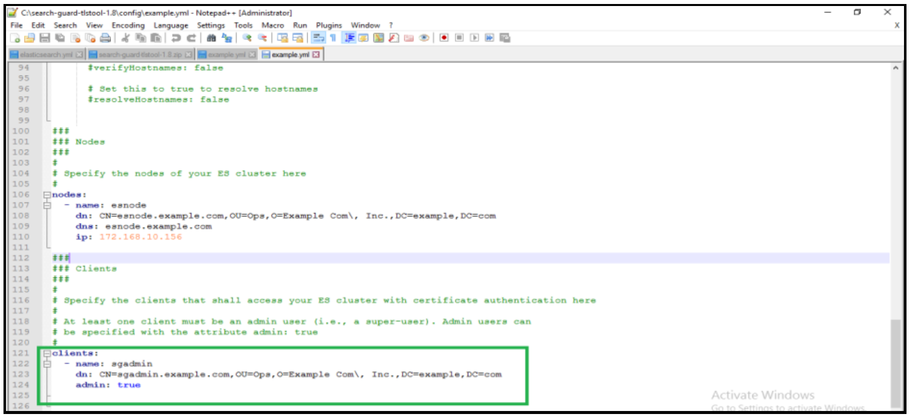
Figure 1: Example.yml file

- Now move to the clients tag and remove all the clients under the tag. Add the following clients:

```
“- name: sgadmin

   dn: CN=sgadmin.example.com,OU=Ops,O=Example
Com\, Inc.,DC=example,DC=com

   admin: true”
```


C:\search-guard-tlstool-1.8\config\example.yml - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
elasticsearch.yml
search-guard-tlstool-1.8.zip
example.yml
example.yml
Activate Windows
Go to Settings to activate Windows.

```
        #verifyHostnames: false

        # Set this to true to resolve hostnames
        #resolveHostnames: false


###
### Nodes
###
#
# Specify the nodes of your ES cluster here
#
nodes:
  - name: esnode
    dn: CN=esnode.example.com,OU=Ops,O=Example Com\, Inc.,DC=example,DC=com
    dns: esnode.example.com
    ip: 172.168.10.156

###
### Clients
###
#
# Specify the clients that shall access your ES cluster with certificate authentication here
#
# At least one client must be an admin user (i.e., a super-user). Admin users can
# be specified with the attribute admin: true
#
clients:
  - name: sgadmin
    dn: CN=sgadmin.example.com,OU=Ops,O=Example Com\, Inc.,DC=example,DC=com
    admin: true
```

Figure 2: Example.yml file

4. Save and close the edited file once all the changes are made.
5. Open Command Prompt and use the following commands for generating the certificates:

```
•cd <Installation directory>\search-guard-tlstool-
1.8\tools

•tools>sgtlstool.bat

•tools>sgtlstool.bat -c ../config/example.yml -ca -crt
```

6. Once the certificates are generated, move on to the following path:

```
[GroupID Installation Drive]\search-guard-tlstool-1.8\tools\out
```

7. Copy the below mentioned certificates from the path given above:

```
•esnode.key (rename it as esnode-key.pem)

•esnode.pem

•root-ca.pem

•sgadmin.key

•sgadmin.pem
```

Place them in the following folder:

```
ElasticSearch\elasticsearch-6.2.4\config
```

8. Once copied, edit the *elasticsearch.yml* and comment out the following in file:

```
•searchguard.ssl.transport.enforce_hostname_verification: false

•searchguard.authcz.admin_dn:

- CN=sgadmin
```

9. Add the following at the end of edited file and save it.

```
searchguard.ssl.transport.pemcert_filepath: esnode.pem

searchguard.ssl.transport.pemkey_filepath: esnode-key.pem

searchguard.ssl.transport.pemtrustedcas_filepath: root-ca.pem

searchguard.ssl.transport.enforce_hostname_verification: false

searchguard.ssl.http.enabled: true

searchguard.ssl.http.pemcert_filepath: esnode.pem

searchguard.ssl.http.pemkey_filepath: esnode-key.pem

searchguard.ssl.http.pemtrustedcas_filepath: root-ca.pem

searchguard.allow_unsafe_democertificates: true

searchguard.allow_default_init_sgindex: true

searchguard.authcz.admin_dn:

  - CN=sgadmin

searchguard.enable_snapshot_restore_privilege: true
searchguard.check_snapshot_restore_write_privileges:
true

searchguard.restapi.roles_enabled: ["SGS_ALL_ACCESS"]
```

10. Open Registry editor and go to the following path:

    ```
    Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Imanami\GroupID\V
    ersion 10.0\Replication”
    ```

    Change ElasticSearchUrl to https.

11. Restart the Elasticsearch and replication services.

Appendix B

Add multi-value attributes in a report (Patch # 32347)

This appendix describes the method of adding a multi-value attribute such as *Memberof*, *email* and so on in a GroupID report.

1. Go to the following folder:

   ```
   C:\Program Files\Imanami\GroupID 10.0\Reporting\
   ```

   Locate the report file by report name and with .*ReportTemplate* extension, for example, ActiveDirectory.ReportTemplate for the Groups and members report.

2. Open the file in a text editor. In the report area, find the FIELDS xml element.

3. Add the template as defined, remember to change the name of field and set attribute name as its value. An example is given below:

   ```
   <FIELD name="MemberOf" type="enum" value="memberOf">

   <FIELD name="Name" value="CN"/>

   </FIELD>
   ```

   Field name is the display name of attribute and value is the actual name of the attribute.

   Same can be done for other attributes like *AuthOrig*, *Additional owners* (x Additional owners attribute).

   Another attribute can be added as sub attribute manually, for example:

   ```
   <FIELD name="Email" value="mail"/>
   ```

NOTE After adding a new multi-value attribute in a report template, restart GroupID Management Console and generate the report again so that template changes can take effect.

Computer objects in members attribute

In *Groups and members* report, sometimes computers object membership is not displayed properly, add the *Name* attribute and move it to first place. To further ensure that computer object membership display, It is a good idea to add other some other computer object specific attributes such as *DNShostname* and *Operating system.*

We can add both DN based (*MemberOf* , *ManagedBY*) and non DN based attributes (*Additional owners*, *Authorig*) in template file, however, from UI we can only add more attributes in DN based attributes only. For Non DN based attributes (we will require manual addition as described above).

When a report is already created and saved as a template, in option file of that saved template, report name is as follows:

```
<ReportName>testgroupsandmembers</ReportName>
```

It is required that name of the report is changed to its default report name i.e. Groups and members:

```
<ReportName>GroupsXMembers</ReportName>
```

This template will be then shown in Groups and members reports.

Appendix C

Changing Search Guard User Password (Patch # 31899)

If password of Admin user of Search Guard is changed from the Replication node in GroupID Management Console, the message confirming that password has been changed successfully does not appear. In fact, password is not changed and the Admin user could not login to Elasticsearch. As a result of this, replication stops working causing GroupID to

To fix this error, deploy this patch in your environment where multiple instances (let's say 3) of GroupID Server exist.

1. Deploy this patch via GroupID Updates on all GroupID instances.
2. On GroupID master node instance, change the password of Search Guard user as follows:
    a. In GroupID Management Console, click the Replication node.
    b. Provide the current password, for example *admin* for the Admin user account in the Current Password box.
    c. Specify a new password for example *admin1* in the New Password and Confirm New Password boxes.
    d. Click Change Password.
3. On GroupID's second instance, follow the same steps from a – d in point number 2 above with the following 2 changes:
    a. In step b, give *admin1* as Current Password
    b. In step c, give *admin1* in the New Password and Confirm New Password boxes.

4. Repeat step 3 on GroupID’s third instance.

NOTE

Before changing password on master node verify the state of cluster and after changing password on master node and in between changing password on slave nodes (keep GroupID clients offline such as Self-Service portals, Password Center portals, GroupID Management Shell and so on).

An example of Search Guard password:

pass#@$%11*_1

The following special characters are not valid for Search Guard password:
& ^ '

Appendix D

Preferred Domain Controllers List (Patch # 28062)

In a multi-domain environment, GroupID takes time to look up the Domain Controllers in a domain. As a result, the creation and update of objects takes considerable time, to the extent that the GroupID DC lookup process halts object creation at times. On average, it takes about 5 minutes to create an object.

After applying the patch, proceed to define a preferred DC list under the GroupID registry.

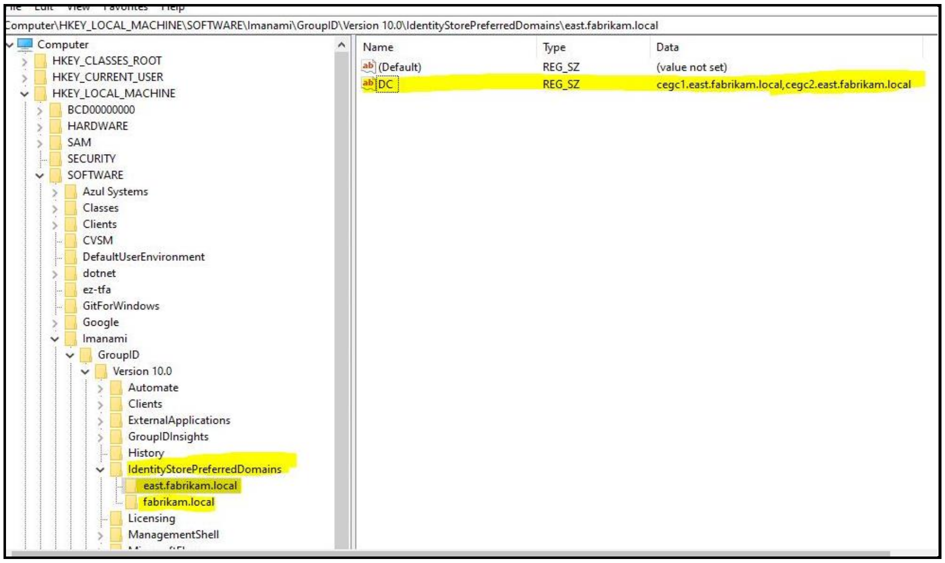
This list must be defined for each domain in the forest; else the normal lookup process will take effect for domains for which the preferred DC list is not available.

1. Open the Windows Registry Editor by typing **regedit** in the Windows Run dialog box.
2. At the following registry path:

   ```
   HKEY_LOCAL_MACHINE>SOFTWARE>Imanami>GroupID>Version
   10>
   ```

   Create the following registry key:

   ```
   IdentityStorePreferredDomains
   ```



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Imanami\GroupID\Version 10.0\IdentityStorePreferredDomains\east.fabrikam.local

Name	Type	Data
(Default)	REG_SZ	(value not set)
DC	REG_SZ	cegc1.east.fabrikam.local,cegc2.east.fabrikam.local

Figure 3: Registry Editor window

3. Under this registry key, add registries for each domain, using the domain names (FQDN).

   For example,
   - east.fabrikam.local
   - fabrikam.local

4. For each specified domain, do the following:

   - Create a key with the name, *DC*, and
   - Provide the name(s) of the domain controllers (FQDN) in the domain as its value. In case of multiple names, use a comma to separate them. For example:

   ```
   DC=cegc1.east.fabrikam.local,cegc2.east.fabrikam.local
   ```

   Specify these names in the order of priority.

5. Restart IIS after setting the DCs.

GroupID will perform operations on the first DC in the list for a specific domain. For example, to create a group in the *east.fabrikam.local* domain, GroupID will communicate with the first DC in the preferred list for the domain. In case, the DC is down, GroupID will check the next DC in the list.

NOTE For Exchange operations (on-prem Microsoft Exchange), it is recommended that each DC in the preferred list in the registry must also be a global catalog.

A Limitation

If we have a domain **demo1.com** with multiple DCs as *DC1* , *DC2* , *DC3* and *DC4* .

Preferred DC list is defined as follows:

1. DC2.demo1.com
2. DC1.demo1.com

We have a dynasty with 10 child dynasties:

Dynasty1

Dynasty1-chid1
Dynasty1-child2
Dynasty1-child3
.
.
.
Dynasty1-child10

At time of dynasty creation, context of GroupID DataService was locked to DC2 and dynasty along with its 10 children was created in DC2 and replicated to Elastic.

DC2 goes down without replicating the dynasty's children into DC1 or any other DC. The *Server not operational* error appears on UI and in logs upon update of the dynasty.

Upon subsequent updates of the dynasty, The *Server not operational* error occurs as context of the DataService is locked to DC2 and its not operational.

However, if IIS is reset and upon next update of the dynasty, context is changed to DC1 (*second in the preferred DC list or DC3 or DC4 , if DC1 is also down and DC3 or DC4 was cached with normal lookup process*).

GroupID DataService will try to update dynasty children which were earlier replicated to Elastic but an error will occur as these dynasties are not present in any other DC (*except DC2*).

Workaround for this scenario is to reset IIS , delete replication (*Dyn1-child1 and other child dynasties will be deleted from Elastic*) and then update the dynasty, now parent and child dynasties will be created first in newly cached DC (*DC1 or others*) and will be updated as well.

Appendix E

GroupID 10 App Pool Configurations (Patch # 32697)

This patch addresses an intermittent issue, *No identity store exists,* which appears at the time of login into a Self-Service portal. After the deployment of this patch, it is recommended that initialization feature of IIS Manager is enabled for *GroupIDDataservice*, *GroupIDSecurityService* and *GroupIDAppPool10*.

It is also recommended recycling time and interval for GroupID App Pools are specified in IIS Manager to ensure that this error does occur again.

IIS Initialization settings for GroupID Data Service

IIS Initialization settings for GroupID Security Service

IIS initialization settings for GroupID App Pools

By default, *GroupIDAppPool10* recycling configurations in IIS are disabled and Imanami Management Service is responsible for IIS and App Pool restart. If GroupID Configuration tool is run, *GroupIDAppPool10* recycling configurations remain disabled. If you want to use them, disable Imanami Management Service and enable recycling configuration in IIS.

IIS Initialization settings for GroupID Data Service

1. Click the Windows Start button and open Internet Information Services (IIS) Manager.
2. In the Connections pane, select *GroupIDDataService* as shown in the following snapshot and click Configuration Editor.

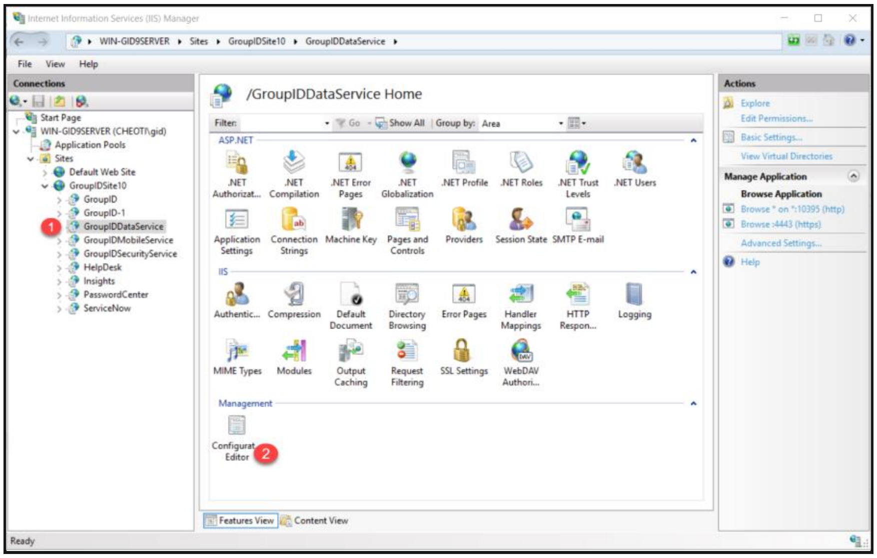


Figure 4: IIS Manager window

3. On the Configuration Editor page, in the Selection drop down, select and expand, *System.webserver* and then click *ApplicaionInitialization*.

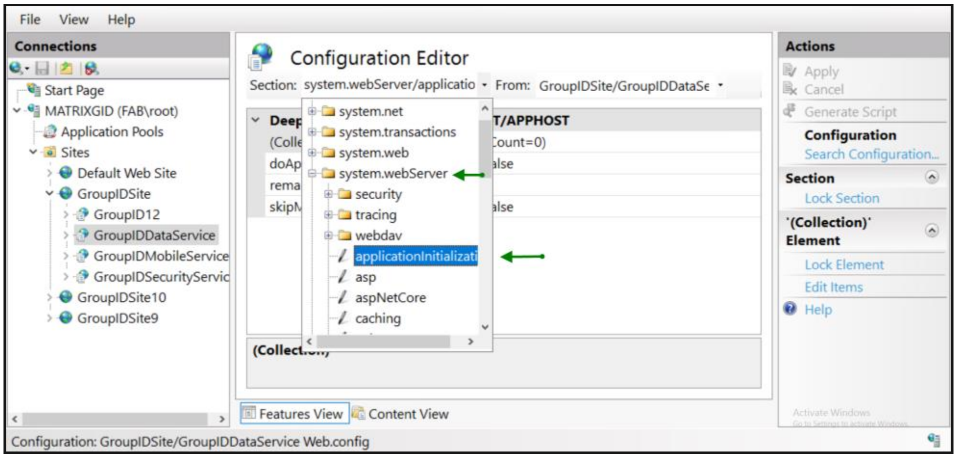
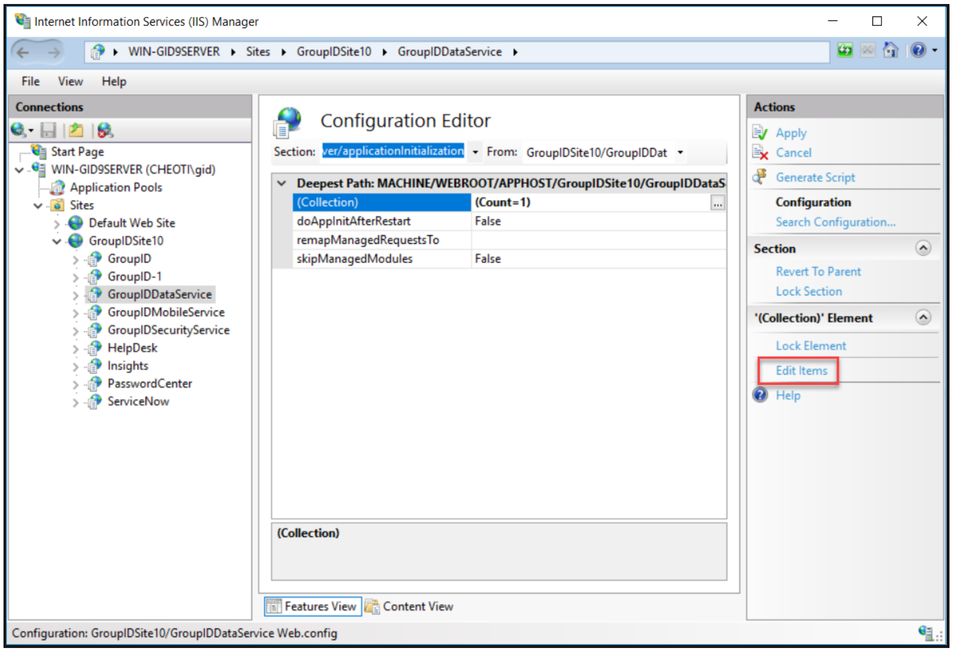


Figure 5: Configuration Editor page

4. Click Edit Items in the Actions pane.



Section: ver/applicationInitialization From: GroupIDSite10/GroupIDDat

Deepest Path: MACHINE/WEBROOT/APPHOST/GroupIDSite10/GroupIDDataS

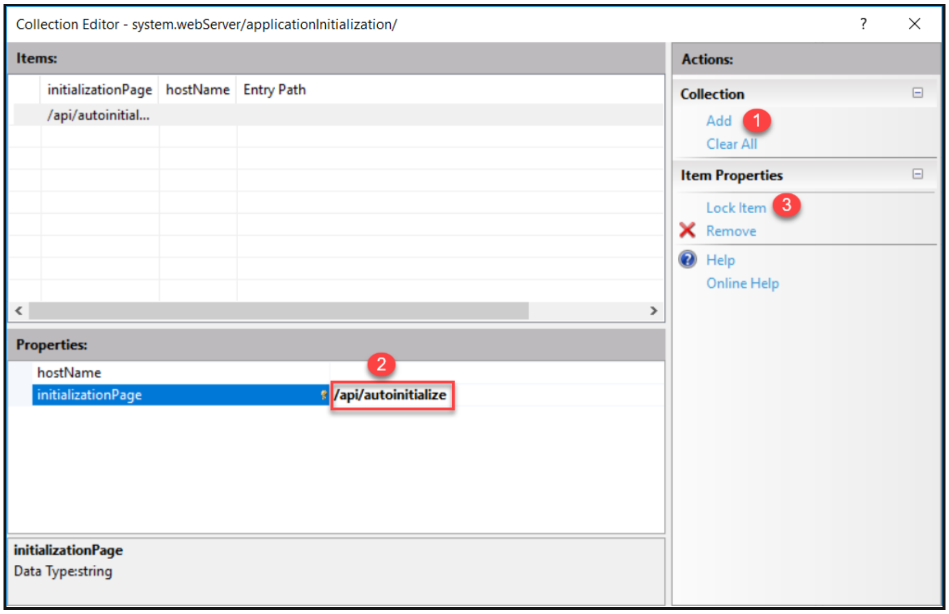
(Collection)	(Count=1)
doAppInitAfterRestart	False
remapManagedRequestsTo	
skipManagedModules	False

(Collection)

Configuration: GroupIDSite10/GroupIDDataService Web.config

Figure 6: Configuration Editor page

5. Click Add and in the Properties section, type */api/autoinitialize* in the. InitializationPage box. Click Lock Item and close the window.



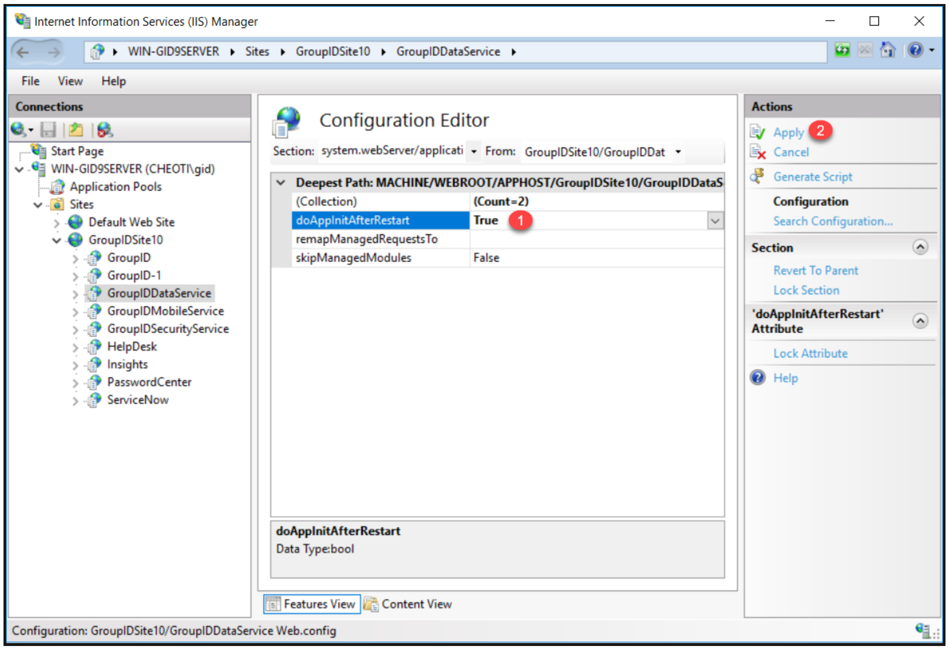
initializationPage	hostName	Entry Path
/api/autoinitial...		

hostName	
initializationPage	/api/autoinitialize

initializationPage
Data Type:string

Figure 7: Edit Items page

6. Set value of *doApplnitAfterRestart* value to *Ture* and click Apply.



Section: system.webServer/applicati From: GroupIDSite10/GroupIDDat

Deepest Path: MACHINE/WEBROOT/APPHOST/GroupIDSite10/GroupIDDataS

(Collection)	(Count=2)
doApplnitAfterRestart	True
remapManagedRequestsTo	
skipManagedModules	False

doApplnitAfterRestart
Data Type:bool

Configuration: GroupIDSite10/GroupIDDataService Web.config

Figure 8: Configuration Editor page

IIS Initialization settings for GroupID Security Service

1. Repeat the steps # 1-4 in the above section (IIS Initialization settings for GroupID Data Service) for GroupIDSecurityService.

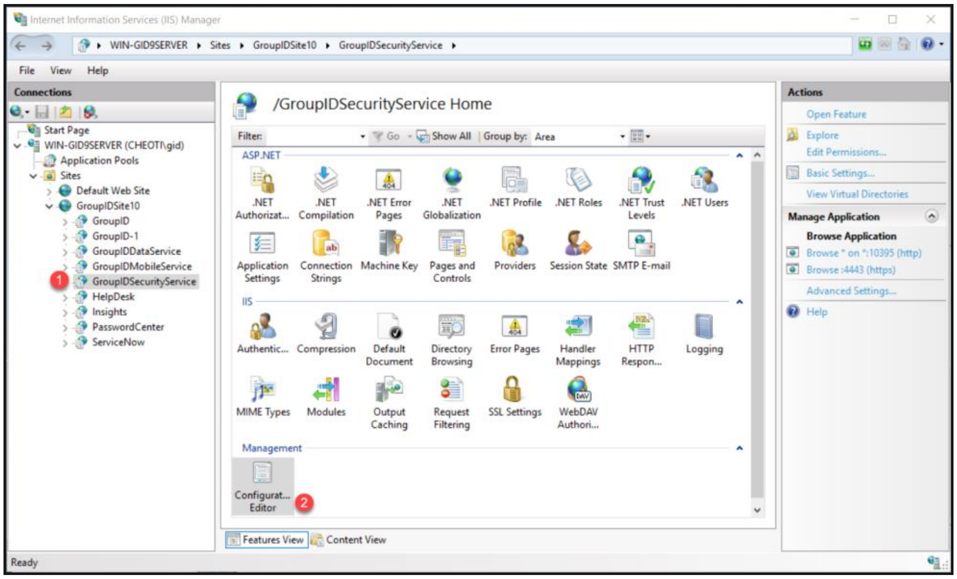
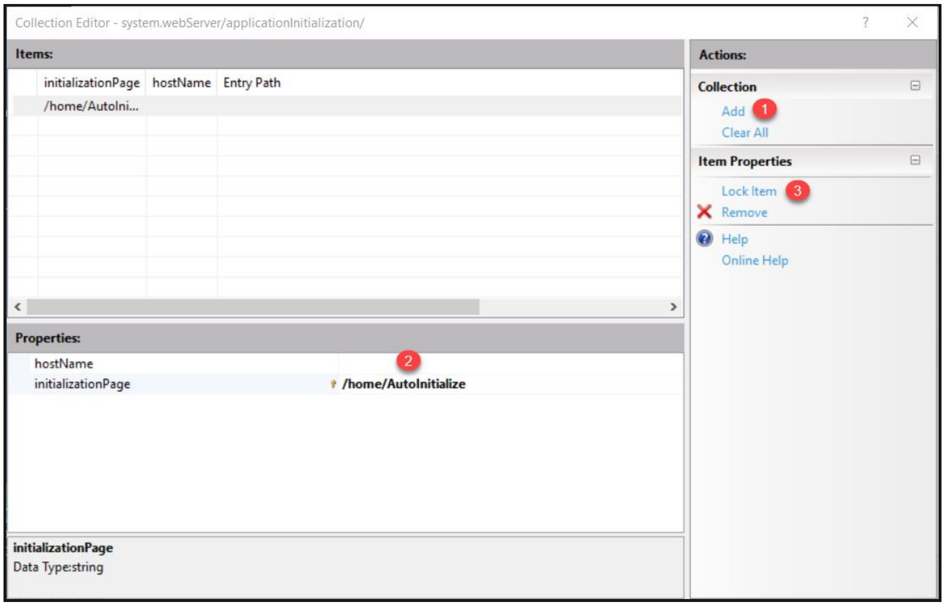


Figure 9: GroupIDSecurityService Home page

2. Click Add and in the Properties section, type */home/AutoInitialize* in the. InitializationPage box. Click Lock Item and close the window



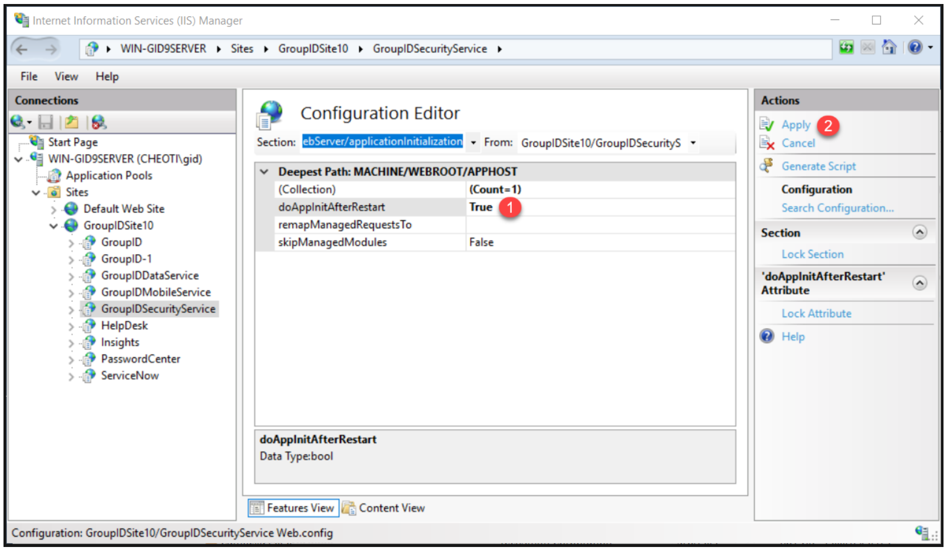
initializationPage	hostName	Entry Path
/home/AutoIni...		

hostName	
initializationPage	/home/AutoInitialize

initializationPage
Data Type:string

Figure 10: Initialization page

3. Set value of *doAppInitAfterRestart* to *Ture* and click Apply.



Section: ebServer/applicationInitialization From: GroupIDSite10/GroupIDSecurityS

Deepest Path: MACHINE/WEBROOT/APPHOST	
(Collection)	(Count=1)
doAppInitAfterRestart	True
remapManagedRequestsTo	
skipManagedModules	False

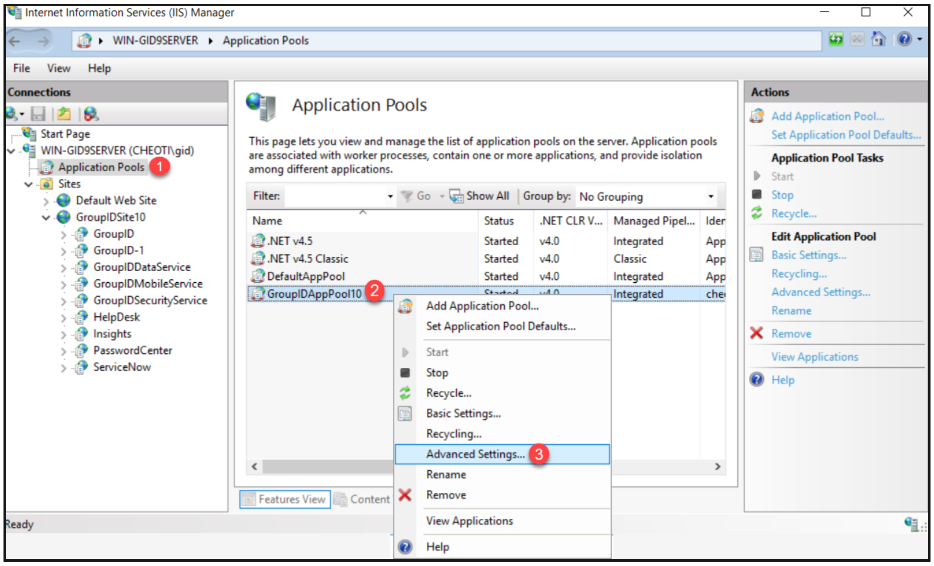
doAppInitAfterRestart
Data Type:bool

Configuration: GroupIDSite10/GroupIDSecurityService Web.config

Figure 11: Configuration Editor page

IIS initialization settings for GroupID App Pools

1. Click the Windows Start button and open Internet Information Services (IIS) Manager.
2. In the Connection pane, select Application Pools.
3. In the Filters list on the Application Pools page, right click *GroupIDAppPool10* and select Advanced Settings.



Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET CLR V...	Managed Pipel...	Ider
.NET v4.5	Started	v4.0	Integrated	App
.NET v4.5 Classic	Started	v4.0	Classic	App
DefaultAppPool	Started	v4.0	Integrated	App
GroupIDAppPool10	Started	v4.0	Integrated	che

Figure 12: Application Pools page

4. On the Advanced Settings window, scroll to Rapid Fail Protection section, and update the values for:

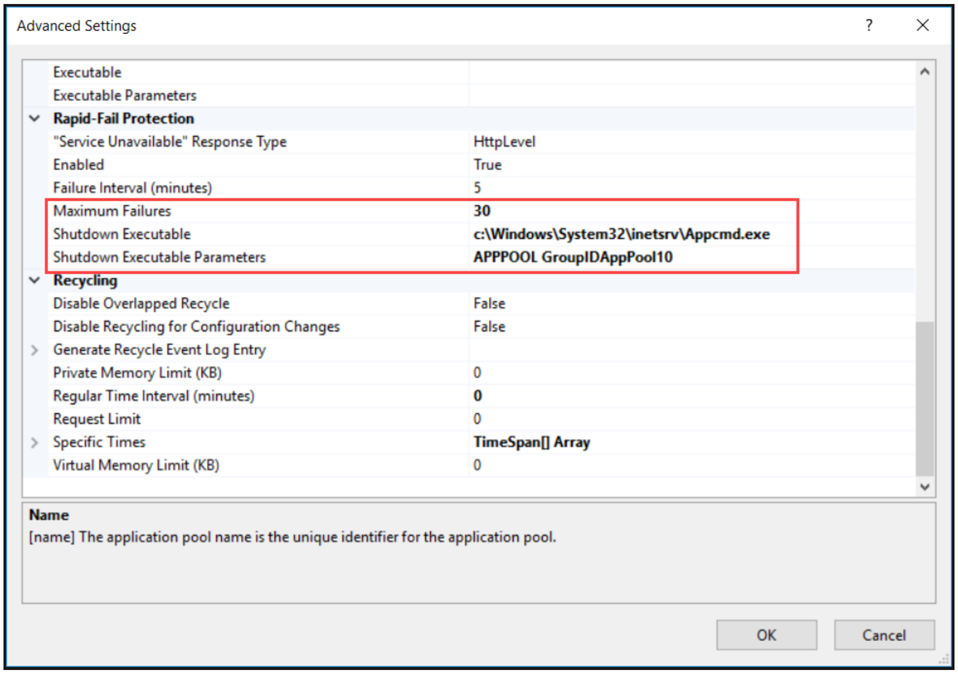
   - Maximum Failures from 20 to higher, let's say 30
   - Shutdown Executable:

     ```
     c:\Windows\System32\inetsrv\Appcmd.exe
     ```

   - Shutdown Executable Parameters:

     ```
     APPPOOL GroupIDAppPool10.
     ```

   Click Ok.



Executable	
Executable Parameters	
Rapid-Fail Protection	
"Service Unavailable" Response Type	HttpLevel
Enabled	True
Failure Interval (minutes)	5
Maximum Failures	**30**
Shutdown Executable	**c:\Windows\System32\inetsrv\Appcmd.exe**
Shutdown Executable Parameters	**APPPOOL GroupIDAppPool10**
Recycling	
Disable Overlapped Recycle	False
Disable Recycling for Configuration Changes	False
Generate Recycle Event Log Entry	
Private Memory Limit (KB)	0
Regular Time Interval (minutes)	**0**
Request Limit	0
Specific Times	**TimeSpan[] Array**
Virtual Memory Limit (KB)	0

Name
[name] The application pool name is the unique identifier for the application pool.

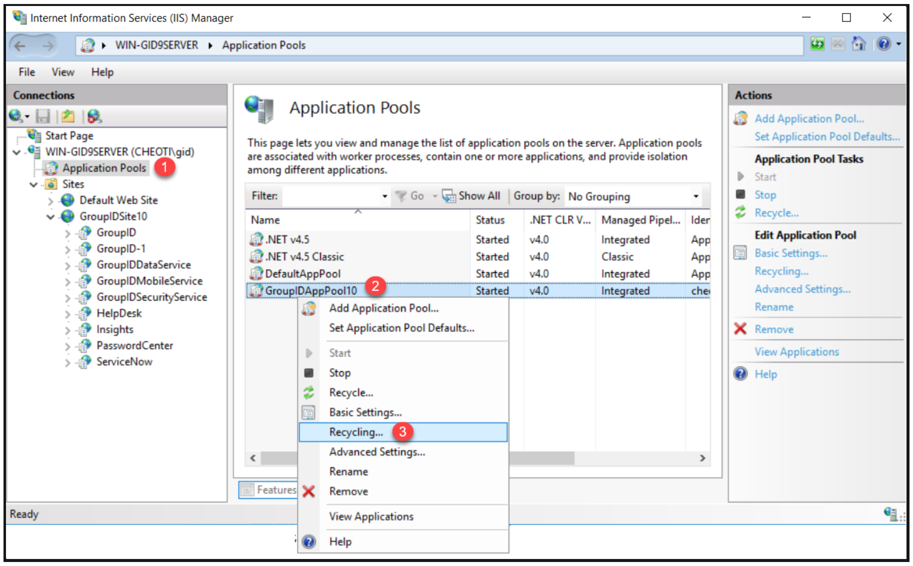
Figure 13: Advanced Settings page

Settings Recycling time of GroupID App Pools

From IIS, we can also change the recycle time of GroupID App Pool10 to any specific time or interval.

1. Click the Windows Start button, open Internet Information Services (IIS) Manager.
2. In the Connections pane, select Application Pools.

3. In the Filters list on the Application Pools page, right click *GroupIDAppPool10* and select Recycling.

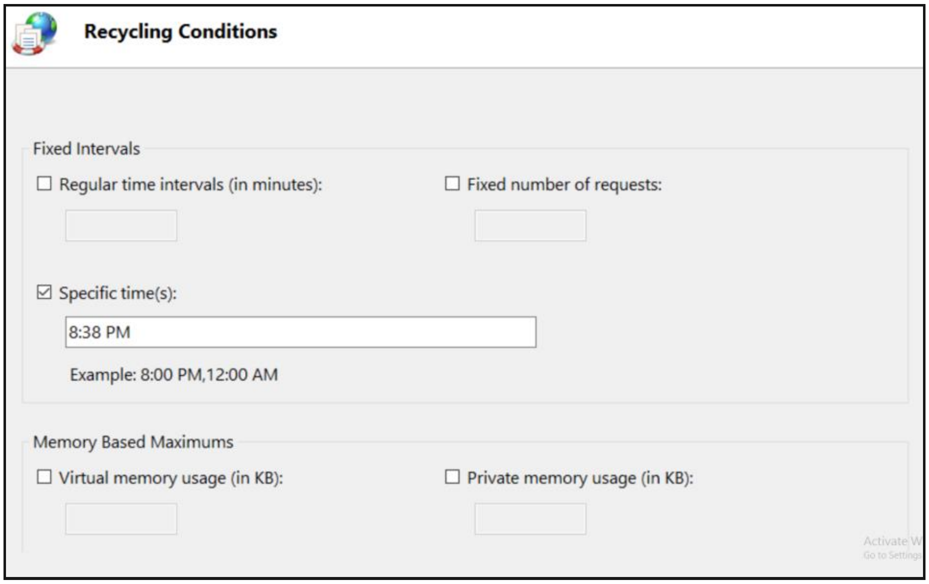


This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET CLR V...	Managed Pipel...	Ider
.NET v4.5	Started	v4.0	Integrated	App
.NET v4.5 Classic	Started	v4.0	Classic	App
DefaultAppPool	Started	v4.0	Integrated	App
GroupIDAppPool10	Started	v4.0	Integrated	che

Figure 14: Application Pools page

On the Recycling Conditions window, specify intervals or specific time(s) per day for GroupID App Pools recycling.



Recycling Conditions

Fixed Intervals

☐ Regular time intervals (in minutes):

☐ Fixed number of requests:

☑ Specific time(s):

8:38 PM

Example: 8:00 PM,12:00 AM

Memory Based Maximums

☐ Virtual memory usage (in KB):

☐ Private memory usage (in KB):

Figure 15: Recycling Conditions page

Appendix F

Imanami Management Service (Patch # 35882)

The Imanami Management Service is a Windows service that does the following:

- It recycles the GroupID app pool in IIS.
  The app pool recycle settings in IIS allow for a single recycling instance for an app pool in 24 hours. The Imanami Management Service enables you to recycle it multiple times in a day.
  By default, the recycle setting for the GroupID app pool in IIS are not applicable, as this service takes care of the recycling task.

- It clears the Task Reporter tables in the GroupID database.
  When a GroupID schedule runs, the events and statuses shown on the progress bar are stored in these tables. The residue keeps building up, which sometimes impacts performance.

NOTE: The service runs at regular intervals to perform these tasks. Separate intervals can be specified for app pool recycling and database table cleanup, thus improving the overall performance of GroupID.

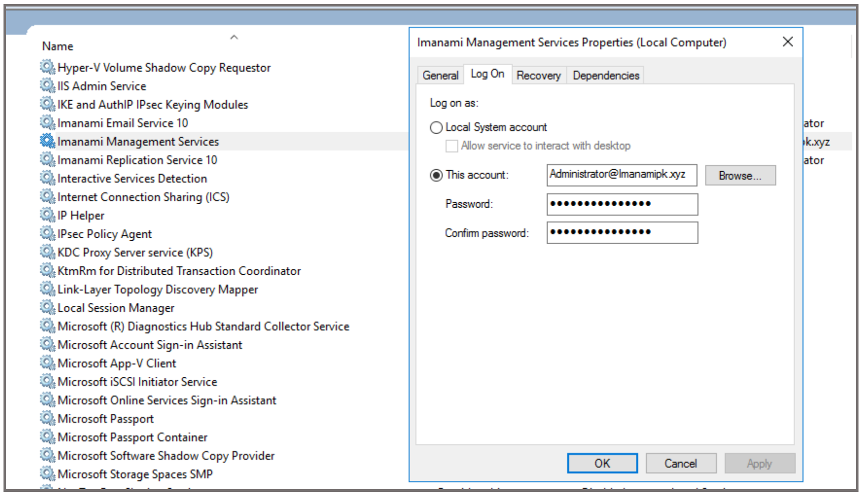
- It checks whether the GroupID Data Service is running.
  The Imanami Management Service checks the liveliness of the GroupID Data Service after IIS, app pool, and GroupID10 site restart.

- It restarts the Imanami Replication service.

Specify a service account for the service

You must change the user account for running the Imanami Management Service to a high integrity account and restart the service.

- For changing the account, go to Windows Services Manager, right-click Imanami Management Service and select **Properties**. On the **Log On** tab, provide the credentials of an admin account and click **OK**.



Name

Hyper-V Volume Shadow Copy Requestor
IIS Admin Service
IKE and AuthIP IPsec Keying Modules
Imanami Email Service 10
Imanami Management Services
Imanami Replication Service 10
Interactive Services Detection
Internet Connection Sharing (ICS)
IP Helper
IPsec Policy Agent
KDC Proxy Server service (KPS)
KtmRm for Distributed Transaction Coordinator
Link-Layer Topology Discovery Mapper
Local Session Manager
Microsoft (R) Diagnostics Hub Standard Collector Service
Microsoft Account Sign-in Assistant
Microsoft App-V Client
Microsoft iSCSI Initiator Service
Microsoft Online Services Sign-in Assistant
Microsoft Passport
Microsoft Passport Container
Microsoft Software Shadow Copy Provider
Microsoft Storage Spaces SMP

Imanami Management Services Properties (Local Computer)

Log on as:

○ Local System account
□ Allow service to interact with desktop

● This account: Administrator@Imanamipk.xyz

Password: •••••••••••••••
Confirm password: •••••••••••••••

Figure 16: Service Properties window – Log on tab

- To restart the service, right-click Imanami Management Service and select Restart.

Service Logs

Logs for the Imanami Management Service are created in the %temp% folder of the account configured as service account for the service. Access using the %TEMP% environment variable.

Service Settings

You can change certain default settings for the Imanami Management Service, such as the GroupID app pool name and the trigger time.

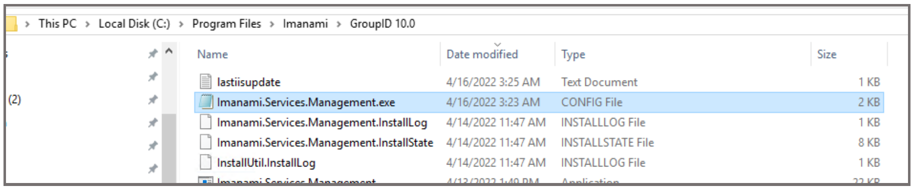
The Imanami.Services.Management.exe file contains settings to control the triggers and scope of the service.

To change service settings:

1. Go to the following location on the GroupID server:

```
[GroupID Installation Drive]:\Program
Files\Imanami\GroupID 10.0\
```

2. Open the Imanami.Services.Management.exe.config file with a text editor, such as Notepad++.

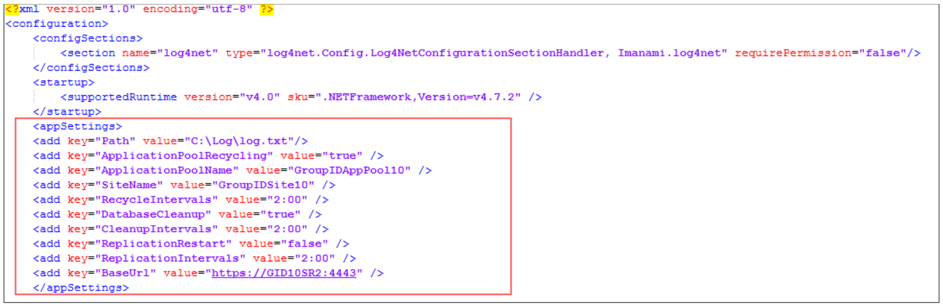


This PC › Local Disk (C:) › Program Files › Imanami › GroupID 10.0

Name	Date modified	Type	Size
lastiisupdate	4/16/2022 3:25 AM	Text Document	1 KB
Imanami.Services.Management.exe	4/16/2022 3:23 AM	CONFIG File	2 KB
Imanami.Services.Management.InstallLog	4/14/2022 11:47 AM	INSTALLLOG File	1 KB
Imanami.Services.Management.InstallState	4/14/2022 11:47 AM	INSTALLSTATE File	8 KB
InstallUtil.InstallLog	4/14/2022 11:47 AM	INSTALLLOG File	1 KB
Imanami.Services.Management	4/13/2022 1:40 PM	Application	22 KB

Figure 17: Imanami Management Service listed in GroupID Installation folder

3. The appSettings section of this file contains keys for GroupID app pool settings:



```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <configSections>
        <section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler, Imanami.log4net" requirePermission="false"/>
    </configSections>
    <startup>
        <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
    </startup>
    <appSettings>
    <add key="Path" value="C:\Log\log.txt"/>
    <add key="ApplicationPoolRecycling" value="true" />
    <add key="ApplicationPoolName" value="GroupIDAppPool10" />
    <add key="SiteName" value="GroupIDSite10" />
    <add key="RecycleIntervals" value="2:00" />
    <add key="DatabaseCleanup" value="true" />
    <add key="CleanupIntervals" value="2:00" />
    <add key="ReplicationRestart" value="false" />
    <add key="ReplicationIntervals" value="2:00" />
    <add key="BaseUrl" value="https://GID10SR2:4443" />
    </appSettings>
```

Figure 18: Imanami.Services.Management.exe.config file – appSettings section

4. Update the key values as required. A brief description of the keys is given below:

Key	Description
ApplicationPoolRecycling	Set its value to True or False, to enable or disable app pool recycling by the Imanami Management Service. The value is True by default, indicating that the service will recycle the GroupID app pool.
ApplicationPoolName	The name of the GroupID app pool to be recycled by the service. By default, GroupIDAppPool10 is given.
SiteName	The name of the GroupID site in IIS. By default, GroupIDSite10 is given.
RecycleIntervals	Set a time for triggering the service. You can set multiple triggers per day, using a semicolon to separate each trigger. Use the 24-hour time to specify the triggers, for example: “3:15;8:15;13:15;18:15” By default, the recycling time is set to 2:00, i.e., the service is triggered at 2 am daily. NOTE For the app pool you specify in this file, remove the recycle time from the app pool settings in IIS, to control its recycling with this service.

Key	Description
DatabaseCleanup	Set its value to True to clear the Task Reporter tables in the GroupID SQL database by the Imanami Management Service. The value is True by default. Set its value to False to prevent the service from clearing the tables. NOTE If a GroupID schedule is already running when the Imanami Management service runs, the database cleanup task will not be triggered.
CleanupIntervals	Set a time to trigger the service for clearing the Task Reporter tables in the GroupID database. You can set multiple triggers per day, using a semicolon to separate each trigger. Use the 24-hour time to specify the triggers, for example: “3:15;8:15;13:15;18:15” By default, the table cleanup time is set to 2:00, i.e., the service is triggered at 2 am daily to clear the tables.
ReplicationRestart	To enable/disable restart mechanism for Imanami replication service (by default its false)
ReplicationIntervals	Set a time for triggering the replication service. You can set multiple triggers per day, using a semicolon to separate each trigger. Use the 24-hour time to specify the triggers, for example: “3:15;8:15;13:15;18:15”
Baseurl	This key can be added for checking custom URL for GroupID dataserivce (by default this key is not present) Base URL should be given with hostname (CName or Alias) and port number: <add key="BaseUrl" value="https://gid10sr2:4443" />

Key	Description
	Service will add "/GroupIDDataservice/Histroy.svc" at the end of Base URL to check the status of DataService, e.g.: https://gid10sr2:4443" GroupIDDataService/History.svc

Table 1: AppSettings keys in Imanami Management service

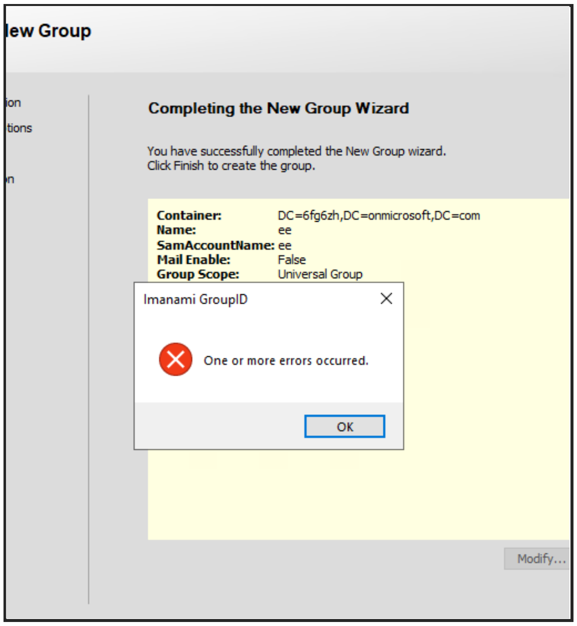
5. Save your changes and close the file.

6. Restart the Imanami Management Service after making any changes to the Imanami.Services.Management.exe.config file.

Appendix G

Modern Authentication and gMSA permissions (for an Azure identity store)

If you are using a gMSA as service account for GroupID services and app pool, an error would be displayed when you try to create a distribution group in an Azure Identity store.



Completing the New Group Wizard

You have successfully completed the New Group wizard.
Click Finish to create the group.

Container: DC=6fg6zh,DC=onmicrosoft,DC=com
Name: ee
SamAccountName: ee
Mail Enable: False
Group Scope: Universal Group

Imanami GroupID

One or more errors occurred.

Figure 19: Modern authentication issue while creating distribution groups

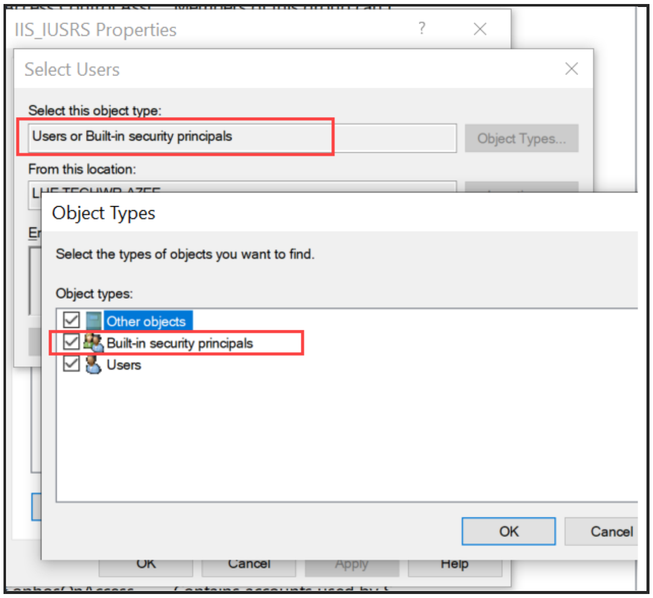
To avoid this issue:

1. Add the gMSA account to the membership of the IIS_IUSRS group on the local machine / GroupID server.
2. For modern authentication, GroupID requires a certificate thumbprint to communicate with the GroupID app in the Azure portal.
   You have to add the IIS_IUSRS group in the 'Manage Private Keys' permission for this certificate on the local computer.

Add gMSA to the IIS_IUSRS group

1. Launch the Computer Management console on your computer.
2. Click **System Tools** > **Local Users and Groups** > **Groups**.
3. In the groups list, locate the IIS_IUSRS group, right-click it and select **Properties**.
4. In the **Members** area, click **Add**. On the **Select Users** dialog box, search and select the gMSA account to make it a member of the IIS_IUSRS group.

   By default, service accounts cannot be searched on the **Select Users** dialog box. Click **Object Types** and select **Builtin security principals**. Now you would be able to add a gMSA on the **Select Users** dialog box.



Select this object type: Users or Built-in security principals

Object Types

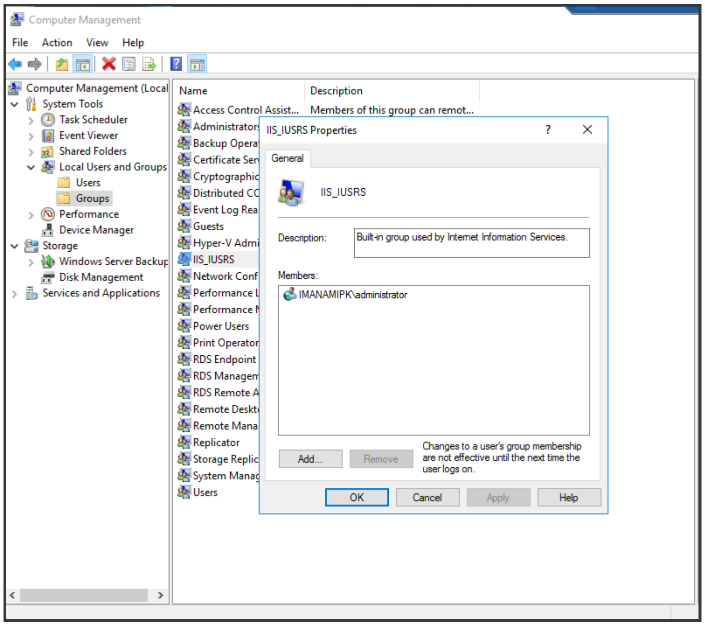
Select the types of objects you want to find.

Object types:

☑ Other objects
☑ Built-in security principals
☑ Users

Figure 20: Object Types page

5. On adding the gMSA as a group member, it would be displayed as:



IIS_IUSRS Properties

IIS_IUSRS

Description: Built-in group used by Internet Information Services.

Members:

IMANAMIPK\administrator

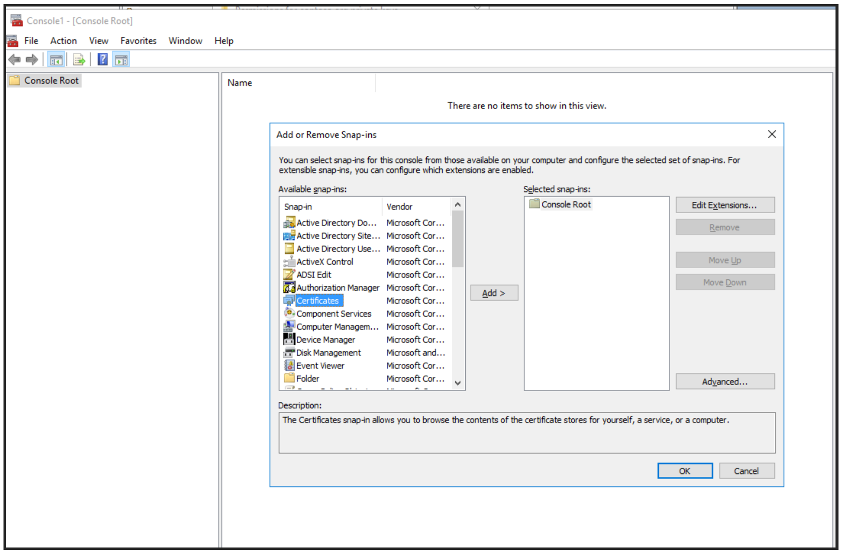
Changes to a user's group membership are not effective until the next time the user logs on.

Figure 21: IIS_IUSRS Properties page

Add IIS_IUSRS to the ‘Manage Private Keys’ certificate permission

GroupID uses a certificate for modern authentication. You must add the IIS_IUSRS group to the ‘Manage Private Keys’ permission for this certificate.

1. Type **mmc** in the Windows search box to launch Microsoft Management Console.
2. In MMC, click File > Add/Remove Snap-in.
3. On the Add or Remove Snap-ins dialog box, click Certificates and then Add.



There are no items to show in this view.

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...

Selected snap-ins:

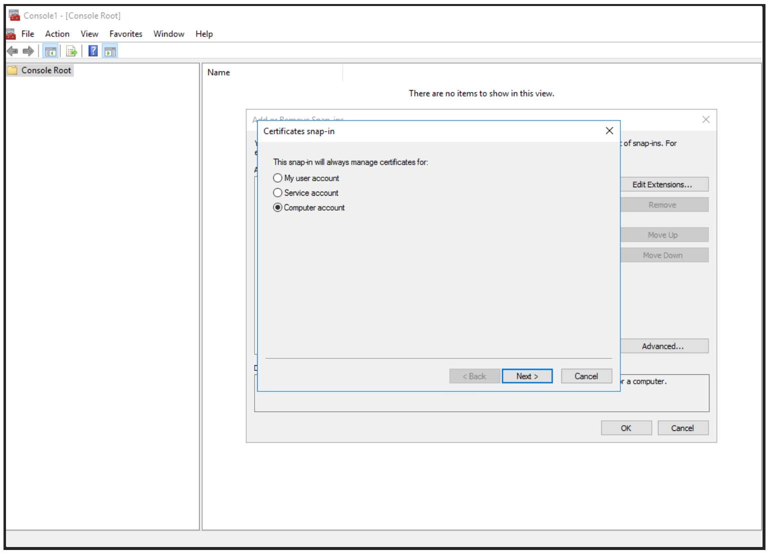
Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Figure 22: Microsoft Management Console – Add or remove snap-ins page

4. On clicking Add, the Certificates snap-in dialog box is displayed. Select Computer Account and click Next.



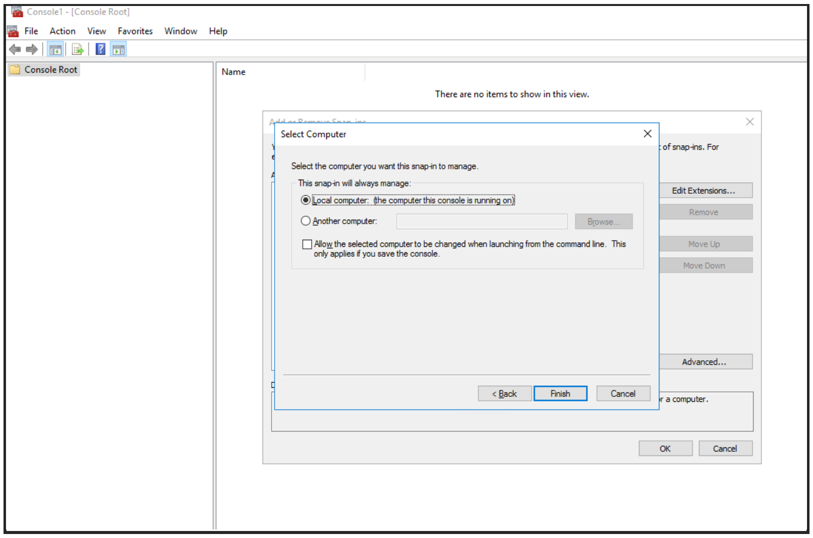
There are no items to show in this view.

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

Figure 23: Certificate snap-in page

5. On the Select Computer dialog box, select the Local Computer option and click Finish.



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

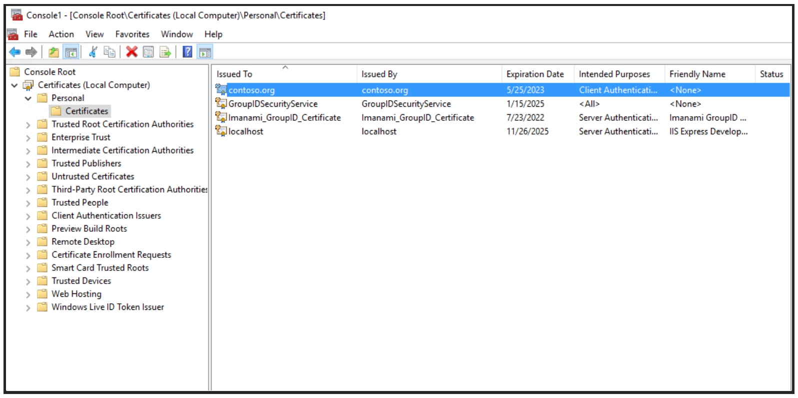
○ Another computer: Browse...

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

< Back | Finish | Cancel

Figure 24: Select Computer page

6. The snap-in is added to MMC. In the left pane, click Certificates (Local Computer) > Personal > Certificates.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Issuer

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
contoso.org	contoso.org	5/25/2023	Client Authenticati...	<None>	
GroupIDSecurityService	GroupIDSecurityService	1/15/2025	<All>	<None>	
Imanami_GroupID_Certificate	Imanami_GroupID_Certificate	7/23/2022	Server Authenticati...	Imanami GroupID ...	
localhost	localhost	11/26/2025	Server Authenticati...	IIS Express Develop...	

Figure 25: Certificates page

All certificates added on the local computer are displayed here.

7. Search for the certificate that GroupID uses for modern authentication. It can be a self-signed or third-party certificate.

   In this example, the certificate has been created in contoso.org. We are using its thumbprint for modern authentication.

8. Right click the certificate > All Tasks > Manage Private Keys.

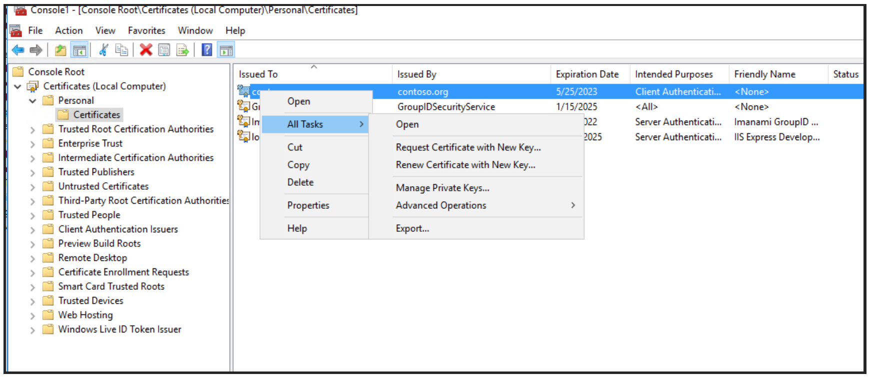
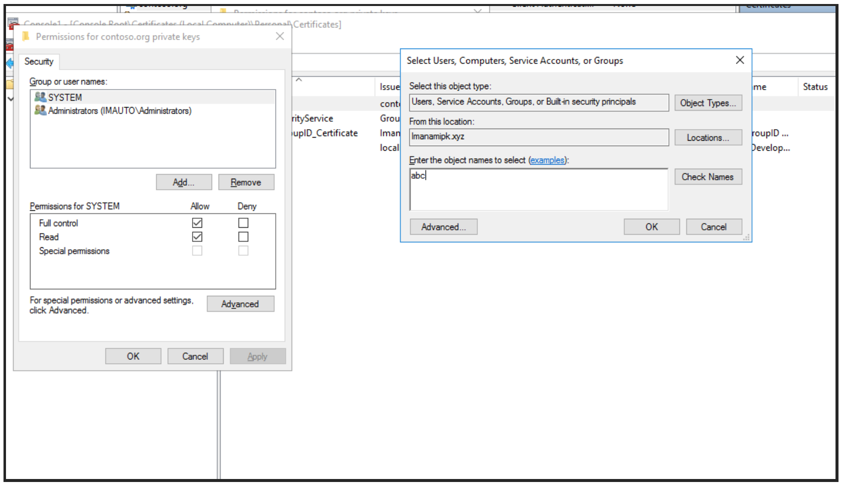


Figure 26: Certificate options

9. On the Permissions dialog box, click Add.

10. On the Select Users, Computers, Service Accounts, or Groups dialog box, add the IIS_IUSRS group. On clicking OK, the group would be displayed on the Permissions dialog box.



Select this object type: Users, Service Accounts, Groups, or Built-in security principals

From this location: Imanamipk.xyz

Enter the object names to select (examples): abc

Figure 27: Select Users, Computers, Service Accounts or Groups page

Appendix H

Extension attributes' support for an Azure AD Identity store

In GroupID, you can replicate the extension attributes in an Azure identity store and use them in the Query Designer for creating Smart Group queries:

When extensionattribute1, extensionattribute2, extensionattribute3 - extensionattribute15 for user objects in Active Directory are synced via Azure AD Connect to Azure AD, they are reflected in the following Azure AD attributes:

- Extension property attributes, displayed as *Extension_attributename*. For example, *Extension_EmployeeID*, *Extension_cn*, *Extension_extensionattribute1*, etc.
- Custom extension attributes, also called *onpremisesExtensinoattributes*, are displayed as *extensionattribute1*, *extensionattribute2*, till *extensionattribute15*.

Hence, both these extension attributes are replicated and useable in GroupID's Query Designer.

In this document, we will discuss the following:

- Sync extension attributes from on-premises AD to Azure AD.
- Use extension attributes in the Query Designer in GroupID.

How are extension attributes populated?

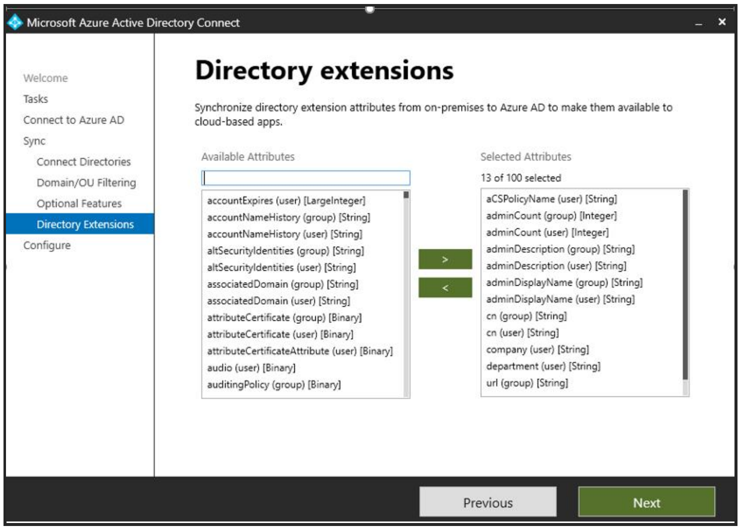
Populating extensionattribute1 - extensionattribute15 is not within the scope of this document.

However, you can use the Exchange Online console to provide values for *extensionattribute1* - *extensionattribute15* for a mailbox, which would populate these attributes in Active Directory.

Sync attribute from a source to Azure AD

Use Azure AD Connect to sync attributes from a source (such as on-premises AD) to Azure AD. This is required to populate the extension attributes in Office 365 / Azure AD, which are s available at the backend, but not exposed on the UI.

On the Directory Extensions page of the Azure AD Connect tool, you can specify the attributes to sync.



Directory extensions

Synchronize directory extension attributes from on-premises to Azure AD to make them available to cloud-based apps.

Available Attributes

- accountExpires (user) [LargeInteger]
- accountNameHistory (group) [String]
- accountNameHistory (user) [String]
- altSecurityIdentities (group) [String]
- altSecurityIdentities (user) [String]
- associatedDomain (group) [String]
- associatedDomain (user) [String]
- attributeCertificate (group) [Binary]
- attributeCertificate (user) [Binary]
- attributeCertificateAttribute (user) [Binary]
- audio (user) [Binary]
- auditingPolicy (group) [Binary]

Selected Attributes

13 of 100 selected

- aCSPolicyName (user) [String]
- adminCount (group) [Integer]
- adminCount (user) [Integer]
- adminDescription (group) [String]
- adminDescription (user) [String]
- adminDisplayName (group) [String]
- adminDisplayName (user) [String]
- cn (group) [String]
- cn (user) [String]
- company (user) [String]
- department (user) [String]
- url (group) [String]

Figure 28: Directory extensions page

Run schema replication for GroupID

When a new schema attribute is added (in this case through syncing), GroupID does not pick it automatically. As a next step, run the schema replication scheduler, SchemReplication_schemaReplication (defined in Windows Task Scheduler) to update the schema for the identity store.

By default, this scheduler runs daily, but you may run it manually to get the extension attributes added to the schema for replication. Relaunch GroupID Management Console MMC after schema replication completes. For Self-Service too, users must re-login after schema replication completes.

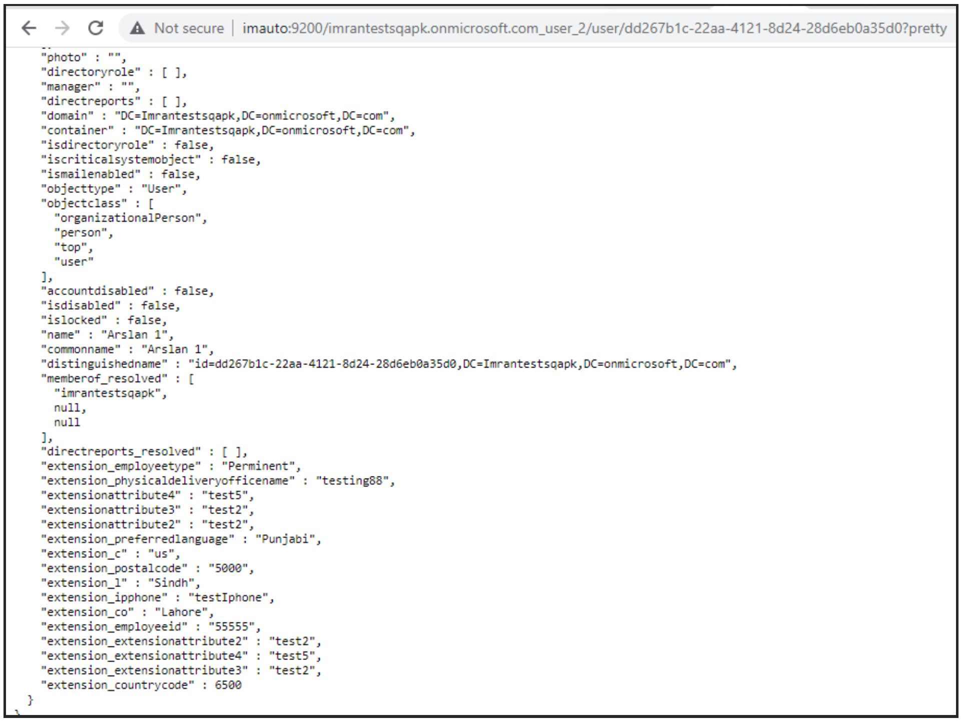
However, if a new identity store for Azure AD is created, schema will be replicated by default.

Replicate attributes for an identity store

After schema replication, the next step is to replicate the attributes for an identity store in GroupID.

Imanami Replication Service is responsible for replicating the attributes for an identity store (including extension attributes) from the directory to Elasticsearch. In this way, any change to the attributes' values is duly updated in Elasticsearch.

After replication, these attributes can be viewed on object properties in Elasticsearch:


Not secure
imauto:9200/imrantestsqapk.onmicrosoft.com_user_2/user/dd267b1c-22aa-4121-8d24-28d6eb0a35d0?pretty

```
    "photo" : "",
    "directoryrole" : [ ],
    "manager" : "",
    "directreports" : [ ],
    "domain" : "DC=Imrantestsqapk,DC=onmicrosoft,DC=com",
    "container" : "DC=Imrantestsqapk,DC=onmicrosoft,DC=com",
    "isdirectoryrole" : false,
    "iscriticalsystemobject" : false,
    "ismailenabled" : false,
    "objecttype" : "User",
    "objectclass" : [
      "organizationalPerson",
      "person",
      "top",
      "user"
    ],
    "accountdisabled" : false,
    "isdisabled" : false,
    "islocked" : false,
    "name" : "Arslan 1",
    "commonname" : "Arslan 1",
    "distinguishedname" : "id=dd267b1c-22aa-4121-8d24-28d6eb0a35d0,DC=Imrantestsqapk,DC=onmicrosoft,DC=com",
    "memberof_resolved" : [
      "imrantestsqapk",
      null,
      null
    ],
    "directreports_resolved" : [ ],
    "extension_employeetype" : "Perminent",
    "extension_physicaldeliveryofficename" : "testing88",
    "extensionattribute4" : "test5",
    "extensionattribute3" : "test2",
    "extensionattribute2" : "test2",
    "extension_preferredlanguage" : "Punjabi",
    "extension_c" : "us",
    "extension_postalcode" : "5000",
    "extension_l" : "Sindh",
    "extension_ipphone" : "testIphone",
    "extension_co" : "Lahore",
    "extension_employeeid" : "55555",
    "extension_extensionattribute2" : "test2",
    "extension_extensionattribute4" : "test5",
    "extension_extensionattribute3" : "test2",
    "extension_countrycode" : 6500
  }
```

Figure 29: Object properties in Elasticsearch

Here,

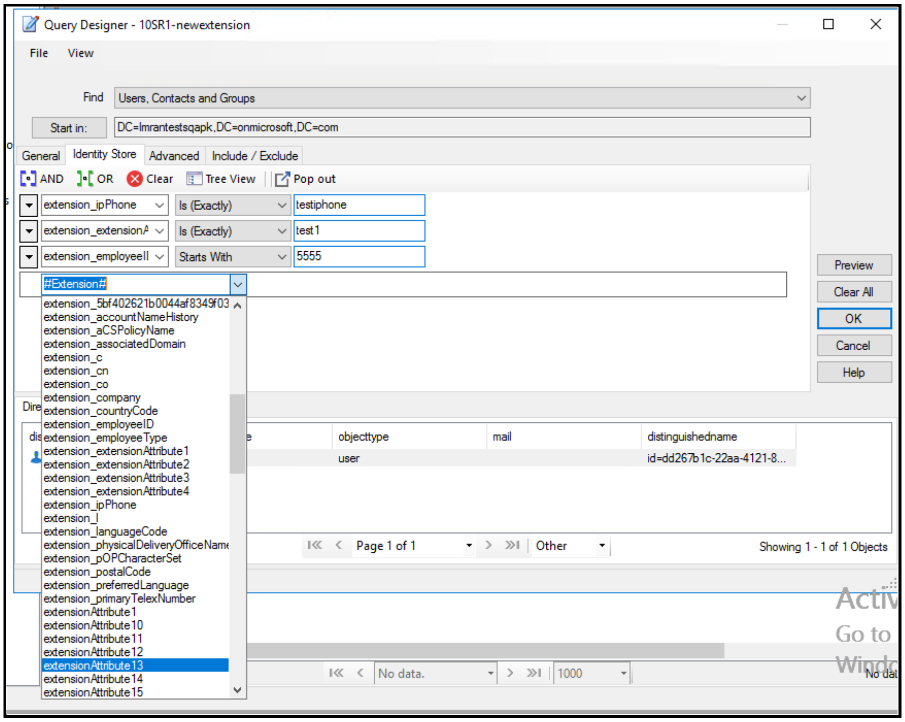
- Extension property attributes are displayed as Extension_attributename (e.g., Extension_EmployeeID, Extension_cn, Extension_extensionattribute1, etc.).
- Custom extension attributes - onpremisesExtensinoattributes are displayed as extensionattribute1, extensionattribute2, and so on.

Note:

- Extension attributes cannot be manipulated from GroupID.

- By default, these attributes are not displayed on the object properties page in the Self-Service portal. However, you can expose them in the portal via the Designs node (to view their values as read-only).

- Extension attributes are available in the Query Designer (Automate and Self-Service) and can be used to create queries. Hence, they can be queried to update Smart Group membership.



Query Designer - 10SR1-newextension

Find: Users, Contacts and Groups

Start in: DC=Imrantestsqapk,DC=onmicrosoft,DC=com

extension_ipPhone	Is (Exactly)	testiphone
extension_extensionA	Is (Exactly)	test1
extension_employeeI	Starts With	5555

#Extension#

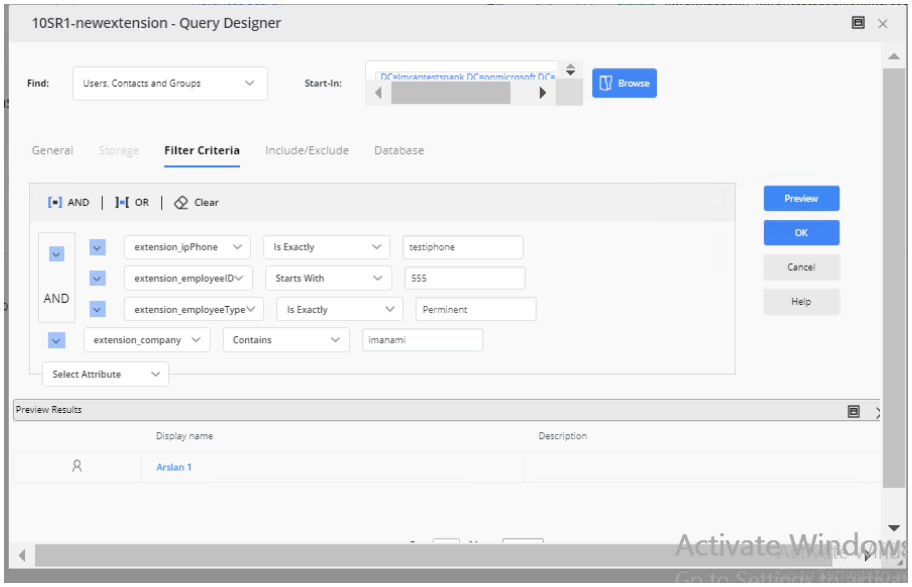
extension_5bf402621b0044af8349f03
extension_accountNameHistory
extension_aCSPolicyName
extension_associatedDomain
extension_c
extension_cn
extension_co
extension_company
extension_countryCode
extension_employeeID
extension_employeeType
extension_extensionAttribute1
extension_extensionAttribute2
extension_extensionAttribute3
extension_extensionAttribute4
extension_ipPhone
extension_l
extension_languageCode
extension_physicalDeliveryOfficeName
extension_pOPCharacterSet
extension_postalCode
extension_preferredLanguage
extension_primaryTelexNumber
extensionAttribute1
extensionAttribute10
extensionAttribute11
extensionAttribute12
extensionAttribute13
extensionAttribute14
extensionAttribute15

objecttype	mail	distinguishedname
user		id=dd267b1c-22aa-4121-8...

Page 1 of 1 · Other · Showing 1 - 1 of 1 Objects

No data. · 1000

Figure 30: Query Designer window in Automate



10SR1-newextension - Query Designer

Find: Users, Contacts and Groups

Start-In: DC=Imrantestsqapk,DC=onmicrosoft,DC=

AND

extension_ipPhone	Is Exactly	testiphone
extension_employeeID	Starts With	555
extension_employeeType	Is Exactly	Perminent
extension_company	Contains	imanami

Select Attribute

Preview Results

Display name	Description
Arslan 1	

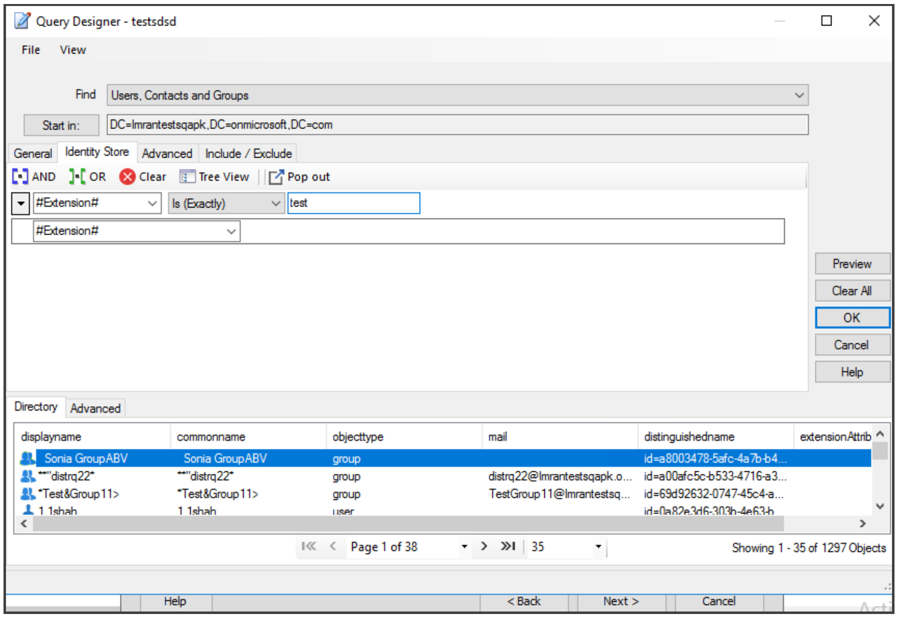
Figure 31: Query Designer in Self-Service portal

The #Extension# attribute

In GroupID, the **#Extension#** attribute controls the replication of all extension attributes (extension property and custom extension attributes) in the schema.

Note the following:

- The #Extension# attribute is also displayed in the Query Designer. This is just a pseudo attribute with no use at the front-end. It is not recommended to query on it.
- If this attribute is used in a query, all objects are returned as a result (whether or not you provide a value for it). It is as shown below:



Find: Users, Contacts and Groups

Start in: DC=lmrantestsqapk,DC=onmicrosoft,DC=com

#Extension# | Is (Exactly) | test

#Extension#

displayname	commonname	objecttype	mail	distinguishedname	extensionAttrib
Sonia GroupABV	Sonia GroupABV	group		id=a8003478-5afc-4a7b-b4...	
**"distrq22*	**"distrq22*	group	distrq22@lmrantestsqapk.o...	id=a00afc5c-b533-4716-a3...	
*Test&Group11>	*Test&Group11>	group	TestGroup11@lmrantestsq...	id=69d92632-0747-45c4-a...	
1 1shah	1 1shah	user		id=0a82e3d6-303b-4e63-b	

Page 1 of 38 | 35 | Showing 1 - 35 of 1297 Objects

Figure 32: Query Designer window

If you do not want to replicate the extension attributes, see Prevent replication of extension attributes.

Prevent replication of extension attributes

If you do not want to replicate the extension property and custom extension attributes to an Azure AD identity store, do the following:

1. Before creating an identity store for Azure AD, remove the #Extension# attribute key and *onpremisesextensionattribute* key from the DirectorySchema.xml file at the location:

   ```
   [GroupID installation drive]:\Program
   Files\Imanami\GroupID
   10.0\GroupIDDataService\Extensions\Azure\
   ```

2. Make sure that onpremisesextensionatribute is not present in the SyncAttributes_Windows Azure.xml file at the location:

   ```
   [GroupID installation drive]:\Program
   Files\Imanami\GroupID 10.0\Replication\
   ```