Recast

Identity Sources

Last Modified on 04.16.26

Get-LiquitIdentitySource

Synopsis

This command is used to display all identity sources or to select a specific identity source.

Syntax

```
Get-LiquitIdentitySource
  [-LiquitContext <LiquitContext>]
  [<CommonParameters>]

Get-LiquitIdentitySource
  [-ID] <guid[]>
  [-LiquitContext <LiquitContext>]
  [<CommonParameters>]

Get-LiquitIdentitySource
  [-EntityRef] <EntityRef[]>
  [-LiquitContext <LiquitContext>]
  [<CommonParameters>]

Get-LiquitIdentitySource
  [-Type] <string[]>
  [-LiquitContext <LiquitContext>]
  [<CommonParameters>]

Get-LiquitIdentitySource
  [-Search] <string>
  [-LiquitContext <LiquitContext>]
  [<CommonParameters>]

Get-LiquitIdentitySource
  [-Name] <string>
  [-LiquitContext <LiquitContext>]
  [<CommonParameters>]
```

Examples

```
Get-LiquitIdentitySource
```

This command displays all identity sources known in the Application Workspace.

```
Get-LiquitIdentitySource -ID 00000000-0000-0000-0000-000000000000
```

This command displays the identity source with the given ID.

Parameters

Name	Value	Description	Required	Default value
Type	`<string[]>`	The type of the identity source.		

Recast

Name	Value	Description	Required	Default value
Search	<string>	This parameter serves a similar purpose to the search box found in the identity sources table from the Application Workspace UI. It enables users to search multiple columns within the table, such as Name and Type. When a search term is provided, the parameter filters records by matching values in these indexed columns. However, it's important to note that not all columns in the table are indexed, meaning that searches for values in these non-indexed columns will not return results. Non-indexed columns include for example the ID and columns containing checkboxes.		
Name	<string>	Searches on the identity source name itself.		
LiquitContext	<LiquitContext>	Determines the selected zone.	No	Default

New-LiquitIdentitySource

Synopsis

This command is used to create a new identity source.

Syntax

For a Microsoft Entra ID (Azure AD) identity source:

```
New-LiquitIdentitySource
   [-Type azuread]
   [-Methods {Login | HTTP | NTLM | Federated | TokenExchange}]
   [-Name] <string>
   [-ClientID] <string>
   [-ClientSecret] <string>
   [-TokenUri] <uri>
   [-AuthorizationUri] <uri>
   [-LogoutUri] <uri>
   [-DisplayName <string>]
   [-Enabled <bool>]
   [-Hidden <bool>]
   [-Description <string>]
   [-ContactFilters <Dictionary[string,Object]>]
   [-Delta <bool>]
   [-AzureADFederation <IdentitySourceAzureADOAuth2Config>]
   [-AzurePhotos {Disabled | Enabled}]
   [-AzureWriteMode {Disabled | GroupMembership}]
   [-UseClientIdAsResource <bool>]
   [-DomainHint <string>]
   [-IncludeNonSecurityGroups <bool>]
   [-RedirectUriMethod {Disabled | Request | Static}]
   [-LiquitContext <LiquitContext>]
```

Example

```
New-LiquitIdentitySource -Type ldap -Methods Federated -Name "insertname" -Password "insertpassword"
```

Parameters

Name	Value	Description	Required	Default value
Type	azuread	The type of the identity source.	Yes	

Recast

Name	Value	Description	Required	Default value
Methods	{Login | HTTP | NTLM | Federated | TokenExchange}]	Configure the methods available to authenticate	Yes	
Name	<string>	The name of the identity source.	Yes	
ClientID	<string>	The Application ID corresponding to your Microsoft Entra ID (Azure AD) app registration.	Yes	
ClientSecret	<string>	The Microsoft Entra ID (Azure AD) app registration secret.	Yes	
TokenUri	<uri>	The logout URI provided by the Microsoft Entra ID (Azure AD) app registration. For example: https://login.microsoftonline.com/[Tennant ID]/oauth2/logout?post_logout_redirect_uri=< redirection URL > The redirection URI needs to be encoded to work properly.	Yes	
AuthorizationUri	<uri>	The authorization URI provided by the Microsoft Entra ID (Azure AD) app registration. For example: https://login.microsoftonline.com/[Tennant ID]/oauth2/authorize	Yes	
LogoutUri	<uri>	The logout URI provided by the Microsoft Entra ID (Azure AD) app registration. For example: https://login.microsoftonline.com/[Tennant ID]/oauth2/logout?post_logout_redirect_uri=< redirection URL > The redirection URI needs to be encoded to work properly.	Yes	
Hidden	<bool>	When an identity source is hidden, it will not appear on the login screen.		
ContactFilters	<Dictionary[string,Object]>	Choose which attributes to be synchronized to Liquit Workspace. For the parameters of this objects, see New-LiquitIdentitySourceContactFilters		
Delta	<bool>	If enabled, delta synchronization of the Microsoft Entra ID (Azure AD) will be enabled. This causes an initial full synchronization to be performed, after which only changes are incrementally synchronized per Application Workspace Server. This reduces the time it takes to fetch all users and groups from Microsoft Entra ID (Azure AD) after the initial synchronization is completed.		
AzureADFederation	<IdentitySourceAzureADOAuth2Config>	Configure the federated authentication method. For the parameters of this objects, see New-LiquitIdentitySourceAzureADOAuth2Config.		
AzurePhotos	{Disabled | Enabled}	Select if photos need to be synchronized or not. This option requires settings additional permissions in Microsoft Entra ID (Azure AD). See SSO with Microsoft Entra ID for more information.		

Recast

Name	Value	Description	Required	Default value
AzureWriteMode	{Disabled | GroupMembership}	What kind of modifications are allowed for Microsoft Entra ID (Azure AD). Additional permissions are needed for modifying group membership. See SSO with Microsoft Entra ID (Azure AD) for more information.		
UseClientIdAsResource	<bool>	When enabled, the application ID will be used to request access to the Microsoft Entra ID (Azure AD). Otherwise, the default Azure AD Graph ID will be used.		
DomainHint	<string>	You can provide Microsoft Entra ID (Azure AD) login page with a hint to which domain you want to authenticate. If the user has multiple active Microsoft Entra ID (Azure AD) sessions, and one session is matching the domain hint, then Microsoft Entra ID (Azure AD) will use that account and will not ask the user to select an account anymore. For example: liquit.com		
IncludeNonSecurityGroups	<bool>	Enable support for groups that are not security enabled within Microsoft Entra ID (Azure AD). Like Microsoft 365 groups. This feature requires the Access Manager license.		
RedirectUriMethod	{Disabled | Request | Static}	The site to which the authorization server directs the user when the app has been successfully approved and an authorization code or access token has been issued. The redirection URL needs to be encoded to work properly.		
LiquitContext	<LiquitContext>	Determines the selected zone.	No	Default

For the Microsoft Entra ID (Azure AD) configuration options in Application Workspace, see Microsoft Entra ID.

For an LDAP identity source:

```
New-LiquitIdentitySource
   [-Type ldap]
   [-Methods {Login | HTTP | NTLM | Federated}]
   [-Name] <string>
   [-Username] <string>
   [-Password] <string>
   [-ContactFilters <Dictionary[string,Object]>]
   [-IdFormat {Name | ID}]
   [-LDAPPhotos {Disabled | Enabled | Cached}]
   [-LDAPWriteMode {Disabled | Passwords | Enabled}]
   [-Schema {ActiveDirectory | eDirectory | JumpCloud}]
   [-LDAPFederation <IdentitySourceLdapOAuth2Config>]
   [-Servers <IdentitySourceLdapServer[]>]
   [-Contexts <IdentitySourceLdapContext[]>]
   [-ServerDiscovery {Manual | DNS | DCLocator}]
   [-Domain <string>]
   [-Secure <bool>]
   [-Delta <bool>]
```

Parameters

Recast

Name	Value	Description	Required	Default value
Type	`ldap`	The type of the identity source.	Yes	
Methods	`{Login | HTTP | NTLM | Federated}]`	Configure the methods available to authenticate	Yes	
Name	`<string>`	The name of the identity source.	Yes	
Username	`<string>`	The username used to connect to LDAP.	Yes	
Password	`<string>`	The password used to connect to LDAP.	Yes	
ContactFilters	`<Dictionary[string,Object]>`	Choose which attributes to be synchronized to Liquit Workspace. For the parameters of this objects, see New-LiquitIdentitySourceContactFilters		
IdFormat	`{Name | ID}`	Determines which attribute will be used to synchronize to the Application Workspace. The following options are available: • **ID** The guid corresponding to the user is used to synchronize (Active Directory only). • **Name** The SAM-Account-Name attribute is used to synchronize (Active Directory only).		
LDAPPhotos	`Disabled | Enabled | Cached`	Determines how the user images are retrieved: • Disabled – No user photos are retrieved or shown in the Liquit Workspace. • Enabled – The user photos are actively retrieved upon requesting. Note that this can have performance impact on large LDAP directories. • Cached – The user photos are stored in the cache of Liquit Workspace.		
LDAPWriteMode	`{Disabled | Passwords | Enabled}`	Determines which modification can be made to the LDAP directory: • *Disabled* – No modifications are allowed. • *Passwords* – Only the passwords of the users can be modified. • *Enabled* – All user attributes can be modified.		
Schema	`ActiveDirectory | eDirectory | JumpCloud`	The schema cannot be changed once the identity source is created.		
LDAPFederation	`<IdentitySourceLdapOAuth2Config>`	Configure the federated authentication method. For the parameters of this objects, see New-LiquitIdentitySourceLdapOAuth2Config.		
Servers	`<IdentitySourceLdapServer[]>`	Define the LDAP server that can be contacted for retrieving data. For the parameters of this objects, see New-LiquitIdentitySourceLdapServer		
Contexts	`<IdentitySourceLdapContext[]>`	Define the context in which the users and groups need to be fetched. For the parameters of this objects, see New-LiquitIdentitySourceLdapContext		
ServerDiscovery	`Manual | DNS | DCLocator`	Available only for Active Directory: • Manual – Manually configure LDAP servers and priorities. • DNS – Auto detect LDAP servers based on DNS records for the specified FQDN of the Active Directory domain. • DC Locator – Auto detect LDAP servers using the Microsoft DC Locator process, take into account Active Directory sites and use the LDAP servers that are geographically closer to the Liquit Workspace servers.		

Recast

Name	Value	Description	Required	Default value
Domain	<string>	Available only for Active Directory. Represents the FQDN of the Active Directory domain; For example: ad.liquit.com		
Delta	<bool>	Use delta synchronization to synchronize changes since last synchronization operation instead of performing a full synchronization at every refresh. (available only for Active Directory). For Active Directory delta synchronization you need to apply additional rights. Grant the LDAP user "Replicating Directory Changes" rights on the AD domain object as explained in the Microsoft documentation.		
LiquitContext	<LiquitContext>	Determines the selected zone.	No	Default

For the LDAP configuration options in Application Workspace, see LDAP.

Set-LiquitIdentitySource

Synopsis

This command is used to edit the properties of a specific identity source.

Syntax

```
Set-LiquitIdentitySource
   [-IdentitySource] <IdentitySource[]>
   [-Hidden <bool>]
   [-Methods {Login | HTTP | NTLM | Federated | TokenExchange}]
   [-DisplayName <string>]
   [-Enabled <bool>]
   [-Description    <string>]
   [-ContactFilters <Dictionary[string,Object]>]
   [-LDAPPhotos {Disabled | Enabled | Cached}]
   [-LDAPWriteMode {Disabled | Passwords | Enabled}]
   [-Username <string>]
   [-Password <string>]
   [-LDAPFederation <IdentitySourceLdapOAuth2Config>]
   [-AzureADFederation <IdentitySourceAzureADOAuth2Config>]
   [-Servers <IdentitySourceLdapServer[]>]
   [-Contexts <IdentitySourceLdapContext[]>]
   [-ServerDiscovery {Manual | DNS | DCLocator}]
   [-Domain <string>]
   [-Secure <bool>]
   [-Delta <bool>]
   [-ClientId <string>]
   [-ClientSecret <string>]
   [-AzureWriteMode {Disabled | GroupMembership}]
   [-AzurePhotos {Disabled | Enabled}]
   [-UseClientIdAsResource <bool>]
   [-TokenUri <uri>]
   [-AuthorizationUri <uri>]
   [-LogoutUri <uri>]
   [-DomainHint <string>]
   [-IncludeNonSecurityGroups <bool>]
   [-RedirectUriMethod {Disabled | Request | Static}]
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

Local identity source
The `hidden` parameter is the only one that can be used for the *Local* identity source, all the other ones will be ignored.

Remove-LiquitIdentitySource

Synopsis

This command is used to remove an existing identity source.

Syntax

```
Remove-LiquitIdentitySource
   [-IdentitySource] <IdentitySource[]>
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

New-LiquitIdentitySourceAzureADOAuth2Config

Recast

Synopsis

This item needs to be assigned to an identity source as an AzureADFederation. Note that it is not saved automatically on the local device, it is available only in your current PowerShell session.

Syntax

```
New-LiquitIdentitySourceAzureADOAuth2Config
   [-ClientID] <string>
   [-AuthorizationURI] <uri>
   [-RedirectURI <uri>]
   [-LogoutURI <uri>]
   [-Resource <string>]
   [-Scope <string>]
   [-UseAuthorizationHeader <bool>]
   [-ClaimAttribute <string>]
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

Parameters

Name	Value	Description	Required	Default value
ClientID	`<string>`	he Application ID corresponding to your Microsoft Entra ID (Azure AD) app registration.	Yes	
AuthorizationURI	`<uri>`	The authorization URI provided by the Microsoft Entra ID (Azure AD) app registration. For example: `https://login.microsoftonline.com/[Tennant ID]/oauth2/authorize`	Yes	
LiquitContext	`<LiquitContext>`	Determines the selected zone.	No	Default

New-LiquitIdentitySourceLdapOAuth2Config

Synopsis

This item needs to be assigned to an identity source as an LDAPFederation. Note that it is not saved automatically on the local device, it is available only in your current PowerShell session.

Syntax

```
New-LiquitIdentitySourceLdapOAuth2Config
   [-ClientID] <string>
   -ClientSecret <string>
   -TokenURI    <uri>
   [-AuthorizationURI] <uri>
   [-RedirectURIMethod {Disabled | Request | Static}]
   [-RedirectURI <uri>]
   [-LogoutURI <uri>]
   [-Resource <string>]
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

Parameters

Recast

Name	Value	Description	Required	Default value
ClientID	`<string>`	The OAuth registration procedure assigns a unique identification to each client (app). Every request for user authentication or token acquisition needs it, and it identifies the application to the authorization server.	Yes	
ClientSecret	`<string>`	A type of password that the client application uses to authenticate itself with the OAuth authorization server. It helps verify the client's identity during token requests.	Yes	
TokenURI	`<uri>`	After obtaining an authorization code, the application uses the token URI to exchange the code for an access token. The client application cannot perform allowed API calls without the access token, which is necessary to access protected resources.	Yes	
AuthorizationURI	`<uri>`	The endpoint URL where users are directed to authenticate and authorize the application to access specific resources on their behalf. This URI initiates the OAuth flow by allowing the app to request authorization and, if successful, receive an authorization code.	Yes	
LiquitContext	`<LiquitContext>`	Determines the selected zone.	No	Default

New-LiquitIdentitySourceLdapContext

Synopsis

This item needs to be assigned to an identity source as a Contexts array. Note that it is not saved automatically on the local device, it is available only in your current PowerShell session.

Syntax

```
New-LiquitIdentitySourceLdapContext
  [-OU] <string>
  [-Scope] {Base | Subtree}
  [-Users <bool>]
  [-Groups <bool>]
  [-LiquitContext <LiquitContext>]
  [-WhatIf]
  [-Confirm]
  [<CommonParameters>]
```

Parameters

Name	Value	Description	Required	Default value
OU	`<string>`	The organizational unit.		
Scope	`{Base | Subtree}`	The location in the LDAP tree where the LDAP DSA looks for matched entities. • Base – Only the users or groups that are contained within the specified container are used. • Subtree – All users or groups that are contained within the specified container or in sub containers are used.		Subtree
Users	`<bool>`	If enabled, the users will be synchronized within this container.		true
Groups	`<bool>`	If enabled, the users will be synchronized within this container.		true
LiquitContext	`<LiquitContext>`	Determines the selected zone.	No	Default

For the LDAP configuration options in Application Workspace, see LDAP.

Recast

New-LiquitIdentitySourceLdapServer

Synopsis

This item needs to be assigned to an identity source as a Servers array. Note that it is not saved automatically on the local device, it is available only in your current PowerShell session.

Syntax

```
New-LiquitIdentitySourceLdapServer
   [-Name] <string>
   [-Address] <string>
   [-Secure <bool>]
   [-Port <uint16>]
   [-Priority <int>]
   [-PageSize <int>]
   [-ConnectionTimeout <int>]
   [-SearchTimeout <int>]
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

Parameters

Name	Value	Description	Required	Default value
Name	`<string>`	The name of the server	Yes	
Address	`<string>`	The DNS name or IP address of the LDAP server	Yes	
Secure	`<bool>`	If enabled, the connection is secure. (this is LDAPS (TLS), the LDAP extension "StartTLS" is not supported)		false
Port	`<uint16>`	The port of the LDAP server. Ports 389 and 636 are standard. Port 389 is suitable for environments where encryption is not a requirement while port 636 is specifically designated for secure LDAP communication using SSL/TLS encryption.	Yes	389
Priority	`<int>`	Servers will be accessed in a particular order based on their assigned priority. Round robin will be used for servers with the same priority.	Yes	100
PageSize	`<int>`	The number of results that will be retrieved per chunk.	Yes	1000
ConnectionTimeout	`<int>`	The number of seconds before an LDAP connection times out.	Yes	15
SearchTimeout	`<int>`	The number of seconds an LDAP server can spend on a search.	Yes	15
LiquitContext	`<LiquitContext>`	Determines the selected zone.	No	Default

New-LiquitIdentitySourceContactFilters

Synopsis

This item needs to be assigned to an identity source as ContactFilters. Note that it is not saved automatically on the local device, it is available only in your current PowerShell session.

Syntax

```
New-LiquitIdentitySourceContactFilters
   [-DisableFields] {city | company | country | department | description | fax | jobTitle | mail | mobile | postalCode | stree
t | telephone}]
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

Parameters

Name	Value	Description	Required	Default value
DisableFields	{city | company | country | department | description | fax | jobTitle | mail | mobile | postalCode | street | telephone}	Choose which attributes to be synchronized to Application Workspace.		
LiquitContext	<LiquitContext>	Determines the selected zone.	No	Default

Set-LiquitIdentitySourceAccountLockoutPolicy

Synopsis

This cmdlet is applicable only for the *Local* identity source.

Syntax

```
Set-LiquitIdentitySourceAccountLockoutPolicy
   [-IdentitySource] <IdentitySource[]>
   [-Enabled <bool>]
   [-ResetInterval <int>]
   [-Threshold <int>]
   [-Duration <int>]
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

Parameters

Name	Value	Description	Required	Default value
ResetInterval	<int>	The period of time during which the [-Threshold <int>] must be reached before the lockout will be applied.		
Threshold	<int>	How many invalid login attempts are allowed before the lockout will be applied.		
Duration	<int>	The amount of time that an account is locked for.		
LiquitContext	<LiquitContext>	Determines the selected zone.	No	Default

Set-LiquitIdentitySourcePasswordPolicy

Synopsis

This cmdlet is applicable only for the *Local* identity source.

Syntax

```
Set-LiquitIdentitySourcePasswordPolicy
   [-IdentitySource] <IdentitySource[]>
   [-Enabled <bool>]
   [-MinimalLength <int>]
   [-MinimalLetters <int>]
   [-MinimalNumbers <int>]
   [-MinimalSpecialChars <int>]
   [-ValidationRegex <string>]
   [-LiquitContext <LiquitContext>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

Parameters

Name	Value	Description	Required	Default value
ValidationRegex	`<string>`	Regex is important in password validation since it allows developers to define tight constraints for password formation and strength.		
LiquitContext	`<LiquitContext>`	Determines the selected zone.	No	Default

Update-LiquitIdentitySource

Synopsis

This command is used to synchronize the selected identity source.

Syntax

```
Update-LiquitIdentitySource
   [-IdentitySource] <IdentitySource[]>
   [-LiquitContext <LiquitContext>]
   [<CommonParameters>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

Examples

This command synchronizes all identity sources.

```
Get-LiquitIdentitySource | Update-LiquitIdentitySource
```

This following script synchronizes a specific identity source.

```
$IdentitySource = Get-LiquitIdentitySource -Type azuread
Update-LiquitIdentitySource -IdentitySource $IdentitySource
```

Further reading

Automating password rotation