EXTERNAL IDENTITY PROVIDERS FOR VIRTUCRYPT

Administrative Guide

TABLE OF CONTENTS

[1] DOCUMENT OVERVIEW 3
[2] PREREQUISITES 4
[3] REGISTER AN EXTERNAL IDENTITY PROVIDER 5
[3.1] CREATE AN OPENID CLIENT 5
[3.2] REGISTER OPENID CLIENT WITH VIP 5
[4] ENABLING IDENTITY PROVIDERS 8
APPENDIX A: TROUBLESHOOTING EXTERNAL IDENTITY PROVIDERS 9
APPENDIX B: XCEPTIONAL SUPPORT 11

[1] DOCUMENT OVERVIEW

The purpose of this guide is to instruct VirtuCrypt users on how to configure the allowed authentication methods for their **VirtuCrypt Intelligence Portal (VIP)** company account.

[2] PREREQUISITES

- Users must have the ability to log in to the VIP Web portal
- Users must have the administrator role in VIP

[3] REGISTER AN EXTERNAL IDENTITY PROVIDER

[3.1] CREATE AN OPENID CLIENT

Create an **OpenID** client application on your identity provider. The parameters of OpenID clients can vary from provider to provider, but the **VIP**-specific configuration will always be the same.

- **Redirect URIs**: These URIs will be the location the browser is redirected to after the user has completed their authentication to the identity provider. VIP only has a single redirect URI for each instance.

  The required format of the URI is: https://<vip url>/rest/api/v2/openid/authorize

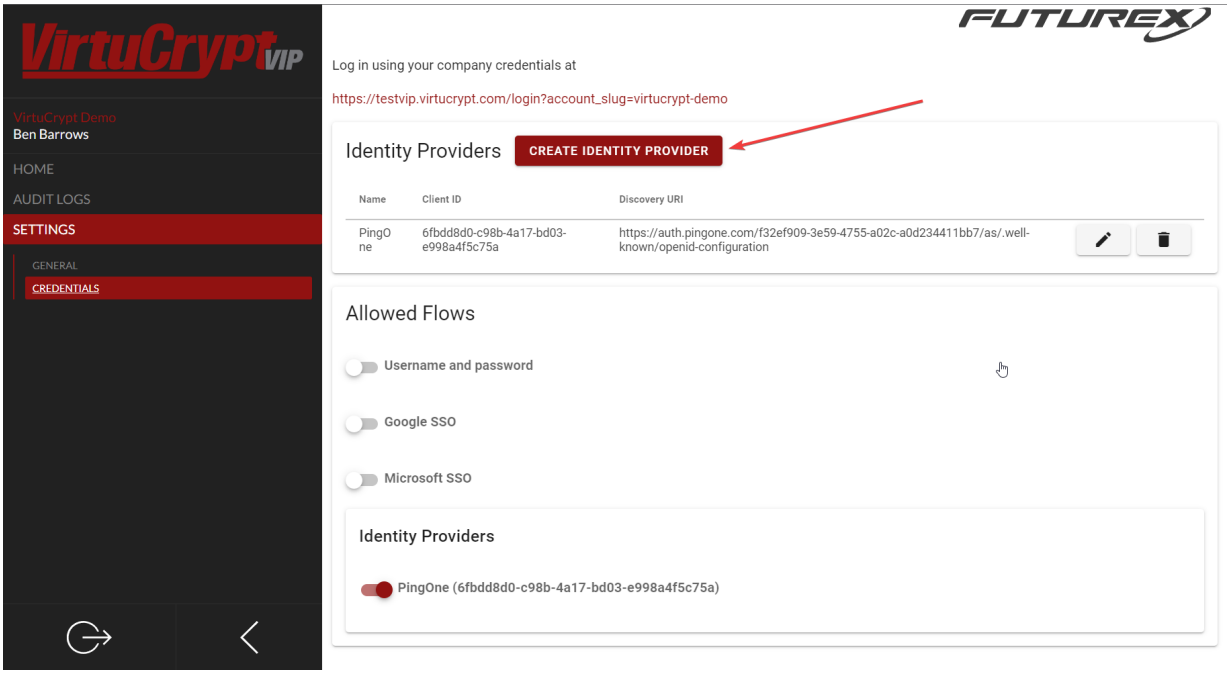
  For the **UAT** VirtuCrypt environment, the URI is:
  https://testvip.virtucrypt.com/rest/api/v2/openid/authorize

  For **Production** VirtuCrypt environment, the URI is:
  https://vip.virtucrypt.com/rest/api/v2/openid/authorize

- **Response Type**: Code
- **Grant Type**: Authorization Code

[3.2] REGISTER OPENID CLIENT WITH VIP

1. Log in to your VirtuCrypt Intelligence Portal (VIP) account with a user that has the administrator role.
2. In the left-hand side menu, select **Settings** > **Credentials**.
3. Select **[Create Identity Provider]** in the main view.

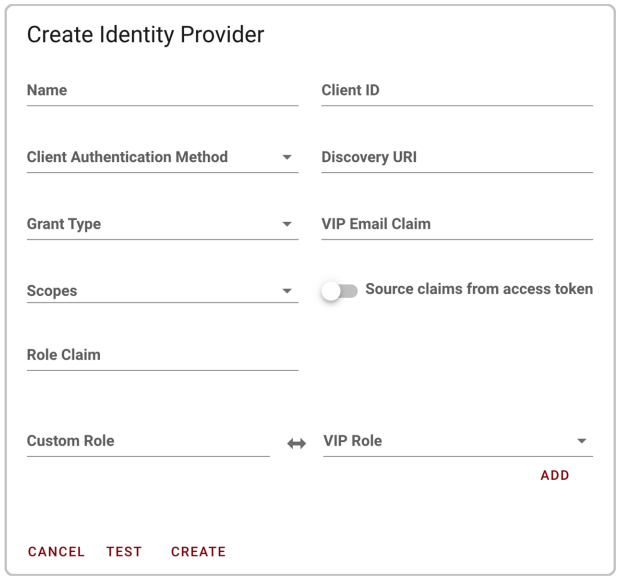


4. This will bring up the **Create Identity Provider** dialog:

Note: Special functionality has been added to this dialog that allows you to derive your authorization from your identity provider. This can be done using the Role Claim and Role Mapping fields.

Role Claim is where you specify the claim containing a list of roles to map to VIP roles. If blank, roles will not be mapped from the authorization token retrieved from the authorization server and instead will be derived from those linked to the authenticated user in VIP.

Role Mapping allows you to derive your authorization from your identity provider. After authenticating, if a role claim is defined, identities will be granted any role matching "Custom Role". This mapping determines which VIP role is associated with the IDP roles.



Descriptions for each of the fields is outlined below:

- **Client ID** - An identifier generally provided by your identity provider. This ID is specific to the VIP client application. This ID will be sent when performing authentication flows.
- **Client Authentication Method** - The two client authentication methods that VIP supports (i.e., Client Secret and Public key/Private key), are outlined below.
    - **Client Secret** - A client secret is a secret known only to the OIDC application and the authorization server. It is generated by your identity provider. VIP supports using client secrets as one of the methods for client authentication. A client has to provide its client secret to authorize itself and to be able to get a token. The client secret serves as a means of confirming the client's authenticity.
    - **Public key/Private key** - Public/Private key is an authentication method that utilizes JSON Web Tokens. In this method, instead of sending the client secret directly, the VIP sends a symmetrical signed JWT using its private key to create the signature. In this method the token is signed using VIP's secret (with the HMAC algorithm).
- **Discovery URI** - An endpoint returning a JSON structure as defined in RFC8259

- **Grant Type** - OAuth grants, also called OAuth flows, refer to the methods of getting tokens to make requests to a resource server.
  - **Authorization Code** - According to the OAuth authorization code grant flow, an authorization server sends a temporary (authorization) code to a client. The code is exchanged for a token.
  - **Authorization code with PKCE** - Authorization code grant with the Proof Key of Code Exchange (PKCE) is an extension of the standard authorization code grant OAuth flow. It is designed to be a secure substitute for the implicit flow for single-page applications (SPA) or native applications.
- **VIP Email Claim** - When the authorization server returns a JWT, this claim will be used to pull the VIP identity's username. If blank, VIP will derive the username from preferred_username if present, or fall back to email.
- **Scopes** - The scopes that will be sent when initiating the authentication flow. OpenID and profile scopes will be appended to this list. If blank, only OpenID and profile scopes will be sent.
- **Source Claims from Access Token** - If enabled, VIP will determine the identity's username from the access_token instead of the id_token
- **Role Claim** - The claim containing a list of roles to map to VIP roles. If blank, roles will not be mapped from the authorization token retrieved from the authorization server and instead will be derived from those linked to the authenticated user in VIP.
- **Role Mapping** - After authenticating, if role claim is defined, identities will be granted any role matching "Custom Role". This mapping determines which VIP role is associated with the IDP roles.

5. Click **[Test]** to verify the configuration is correct. If the test is successful, you will see a message stating that the identity provider is valid.

   Note: See Test Button Troubleshooting in **Appendix A** for information on how to resolve any errors you encounter here.

6. Click **[Create]** to save the settings and create the new Identity Provider.

[4] ENABLING IDENTITY PROVIDERS

1. Log in to your VirtuCrypt Intelligence Portal (VIP) account with a user that has the administrator role.
2. In the left-hand side menu, select **Settings** > **Credentials**.
3. In the **Allowed Flows** section, disable all authentication methods except for your external identity provider.
4. At the top of the **Credentials** page, you will see a URL you can use to authenticate using your company account's configured authentication flows (e.g., https://testvip.virtucrypt.com/login?account_slug=virtucrypt-demo).
5. Navigating to the company account specific URL will display the available authentication methods.

   Example:

APPENDIX A: TROUBLESHOOTING EXTERNAL IDENTITY PROVIDERS

[4.1] TEST BUTTON TROUBLESHOOTING

Error:

Failed to retrieve OpenID configuration from discovery URI: An unexpected error occurred while retrieving configuration from discovery URI.

Possible Causes:

- Incorrect discovery URI provided
- Discovery endpoint is down

Resolution:

Try using curl against the discovery URI you are using.

```
# Perform a GET request against their OpenID discovery URI

curl https://auth.pingone.com/f32ef909-3e59-4755-a02c-a0d234411bb7/as/.well-known/openid-con-
figuration
```

Curl should succeed, and your output should look like JSON.

```
{
  "issuer" : "https://auth.pingone.com/f32ef909-3e59-4755-a02c-a0d234411bb7/as",
  "authorization_endpoint" : "https://auth.pingone.com/f32ef909-3e59-4755-a02c-a0d234411b-
b7/as/authorize",
  "token_endpoint" : "https://auth.pingone.com/f32ef909-3e59-4755-a02c-a0d234411bb7/as/token",
  "userinfo_endpoint" : "https://auth.pingone.com/f32ef909-3e59-4755-a02c-a0d234411b-
b7/as/userinfo",
  "jwks_uri" : "https://auth.pingone.com/f32ef909-3e59-4755-a02c-a0d234411bb7/as/jwks",
  "end_session_endpoint" : "https://auth.pingone.com/f32ef909-3e59-4755-a02c-a0d234411b-
b7/as/signoff",
  "introspection_endpoint" : "https://auth.pingone.com/f32ef909-3e59-4755-a02c-
a0d234411bb7/as/introspect",
  "revocation_endpoint" : "https://auth.pingone.com/f32ef909-3e59-4755-a02c-a0d234411b-
b7/as/revoke",
  "claims_parameter_supported" : false,
  "request_parameter_supported" : true,
  "request_uri_parameter_supported" : false,
  "scopes_supported" : [ "openid", "profile", "email", "address", "phone" ],
  "response_types_supported" : [ "code", "id_token", "token id_token", "code id_token", "code
token", "code token id_token" ],
  "response_modes_supported" : [ "pi.flow", "query", "fragment", "form_post" ],
  "grant_types_supported" : [ "authorization_code", "implicit", "client_credentials", "refresh_
token" ],
  "subject_types_supported" : [ "public" ],
  "id_token_signing_alg_values_supported" : [ "RS256" ],
  "userinfo_signing_alg_values_supported" : [ "none" ],
  "request_object_signing_alg_values_supported" : [ "none", "HS256" ],
  "token_endpoint_auth_methods_supported" : [ "client_secret_basic", "client_secret_post" ],
  "claim_types_supported" : [ "normal" ],
  "claims_supported" : [ "sub", "iss", "auth_time", "acr", "name", "given_name", "family_name",
"middle_name", "preferred_username", "profile", "picture", "zoneinfo", "phone_number", "updated_
at", "address", "email", "locale" ],
  "code_challenge_methods_supported" : [ "plain", "S256" ]
}
```

[4.2] LOGIN TROUBLESHOOTING

After successfully authenticating to my external identity provider, VIP says, "Identity Provider is not associated with the account".

Possible Causes:

- The user you authenticated with does not belong to the company account owning this identity provider.
- Your user you authenticated with does not exist in VIP.

Resolution:

Ensure the user you are authenticating with exists in VIP under the company account owning this identity provider.

APPENDIX B: XCEPTIONAL SUPPORT

In today's high-paced environment, we know you are looking for timely and effective resolutions for your mission-critical needs. That is why our Xceptional Support Team does whatever it takes to ensure you have the best experience and support possible. Every time. Guaranteed.

- 24x7x365 mission critical support
- Level 1 to level 3 support
- Extremely knowledgeable subject matter experts

At Futurex, we strive to supply you with the latest data encryption innovations as well as our best-in-class support services. Our Xceptional Support Team goes above and beyond to meet your needs and provide you with exclusive services that you cannot find anywhere else in the industry.

- Technical Services
- Onsite Training
- Virtual Training
- Customized Consulting
- Customized Software Solutions
- Secure Key Generation, Printing, and Mailing
- Remote Key Injection
- Certificate Authority Services

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

ENGINEERING CAMPUS

864 Old Boerne Road

Bulverde, Texas, USA 78163

Phone: +1 830-980-9782

+1 830-438-8782

E-mail: info@futurex.com

XCEPTIONAL SUPPORT

24x7x365

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com