

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de SAML en Keycloak

Ver en el centro de ayuda: https://bitwarden.com/help/saml-keycloak/

Implementación de SAML en Keycloak

Este artículo contiene ayuda **específica de Keycloak** para configurar el inicio de sesión con SSO a través de SAML 2.0. Para obtener ayuda para configurar el inicio de sesión con SSO para otro IdP, consulte Configuración de SAML 2.0.

La configuración implica trabajar simultáneamente con la aplicación web de Bitwarden y el Portal de Keycloak. A medida que avanza, recomendamos tener ambos fácilmente disponibles y completar los pasos en el orden en que están documentados.

⊘ Tip

Already an SSO expert? Skip the instructions in this article and download screenshots of sample configurations to compare against your own.

Jownload Sample ⊥

Abre SSO en la aplicación web

Inicia sesión en la aplicación web de Bitwarden y abre la Consola de Administrador utilizando el conmutador de producto (ﷺ):

| Password Manager | All vaults | | | New V | BW |
|--------------------|--|------|------------------------------------|------------|----|
| 🗇 Vaults | | _ •" | | | |
| 🕼 Send | FILIERS () | | Name | Owner | : |
| \ll Tools \sim | Q Search vau | AZIV | Company Credit Card Visa, *4242 | My Organiz | : |
| ≅ Reports | ✓ All vaults | | Personal Login | | |
| Settings | 🖄 My vault 🗐 My Organiz : | 0 9 | myusername | Me | : |
| | ✓ Teams Org : + New organization | | Secure Note | Ме | : |
| | ✓ All items ☆ Favorites ④ Login □ Card □ Identity □ Secure note | 0 Ø | Shared Login sharedusername | My Organiz | : |
| C Password Manager | ✓ Folders ➡ No folder ✓ Collections | | | | |
| 🗔 Secrets Manager | | | | | |
| Admin Console | Default colle | | | | |
| 🎂 Toggle Width | ₩ Irash | | | | |

Selector de producto

Abra la pantalla de **Ajustes → Inicio de sesión único** de su organización:

Secure and trusted open source password manager for business

| D bit warden | Single sign-on 🗰 🕒 |
|-------------------------------|--|
| B My Organization | Use the <u>require single sign-on authentication policy</u> to require all members to log in with SSO. |
| | Allow SSO authentication |
| A Members | Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials. |
| 器 Groups | sSO identifier (required) unique-organization-identifier |
| | Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification |
| Billing | Member decryption options |
| 🕸 Settings | ∧ ● Master password |
| Organization info Policies | Trusted devices Once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO required policy, and account recovery administration policy with automatic enrollment will turn on when this option is used. |
| Two-step login | C Type |
| Import data | SAML 2.0 |
| Export vault | |
| Domain verification | SAML service provider configuration |
| Single sign-on | Set a unique SP entity ID |
| Device approvals | Generate an identifier that is unique to your organization |
| SCIM provisioning | |
| | SAML 2.0 metadata URL |
| | |

Configuración de SAML 2.0

Si aún no lo has hecho, crea un **identificador SSO** único para tu organización y selecciona **SAML** del menú desplegable de Tipo. Mantén esta pantalla abierta para una fácil referencia.

Puedes desactivar la opción **Establecer una ID de entidad SP única** en esta etapa si lo deseas. Hacerlo eliminará su ID de organización de su valor de ID de entidad SP, sin embargo, en casi todos los casos, se recomienda dejar esta opción activa.

∂ Tip

Hay opciones alternativas de **descifrado de miembro**. Aprenda cómo comenzar a usar SSO con dispositivos de confianza o Conector de clave.

Configuración de Keycloak

Inicie sesión en Keycloak y seleccione Clientes \rightarrow Crear Cliente.

| | | | | | (3 | 0 | admin 🔻 | |
|----------------|---|-----------------------------|----------------|-------------------------|----------|---|---------|-----|
| master - | Clients Clients are applications ar | nd services that can reques | authentication | of a user. Learn more 🗹 | | | | |
| Manage | | | | | | | | |
| Clients | Clients list Initial ac | cess token Client regis | tration | | | | | |
| Client scopes | Q Search for client | → Create client | Import clie | ent | | | 1-6 👻 < | > |
| Realm roles | | | | | | | | |
| Users | Client ID | Name | Туре | Description | Home URL | | | |
| Groups | account | \${client_account} | OpenID Connect | - | | | | *** |
| | account-console | \${client_account-console} | OpenID Connect | - | | | | |
| Sessions | admin-cli | \${client_admin-cli} | OpenID Connect | - | _ | | | |
| Events | broker | \${client_broker} | OpenID Connect | - | _ | | | * |
| Configure | master-realm | master Realm | OpenID Connect | - | - | | | : |
| Realm settings | security-admin-console | \${client_security-admin | OpenID Connect | - | | | | *** |

Create a Client

En la pantalla de Crear cliente, complete los siguientes campos:

| Campo | Descripción |
|--------------------|---|
| Tipo de cliente | Selecciona SAML. |
| ID de cliente | Establezca este campo en el ID de Entidad SP pre-generado. Este valor generado automáticamente se puede copiar desde la pantalla de Ajustes → Inicio de sesión único de la organización y variará según su configuración. |
| Nombre | Ingrese un nombre de su elección para el cliente Keycloak. |

Una vez que haya completado los campos requeridos en la página de Ajustes Generales, haga clic en Siguiente.

En la pantalla de **ajustes de inicio de sesión**, complete el siguiente campo:

| Campo | Descripción |
|--------------------------------------|---|
| URI de redireccionamiento válidos | Establezca este campo en la URL del Servicio de Consumo de Aserciones (ACS) pre-generada. Este valor generado automáticamente se puede copiar desde la pantalla de Ajustes → Inicio de sesión único de la organización y variará según su configuración. |

Selecciona Guardar.

Seleccione la pestaña de Keys y cambie la opción Se requiere firma del cliente a Desactivado.

| master 🔹 | Clients > Client details | | | | | | | | |
|----------------|---|--|--|--|--|--|--|--|--|
| | https://mat.bitwarden.support/sso/saml2 SAML O Enabled O Action - | | | | | | | | |
| Manage | Clients are applications and services that can request authentication of a user. | | | | | | | | |
| Clients | Settings Keys Roles Client scopes Sessions Advanced | | | | | | | | |
| Client scopes | | | | | | | | | |
| Realm roles | | | | | | | | | |
| Users | Signing keys config | | | | | | | | |
| Groups | If you enable the "Client signature required" below, you must configure the signing keys by generating or importing keys, and the | | | | | | | | |
| Sessions | client will sign their saml requests and responses. The signature will be validated. | | | | | | | | |
| Events | Client signature Off required () | | | | | | | | |
| Configure | | | | | | | | | |
| Realm settings | | | | | | | | | |

Keycloak Keys Config

Por último, en la navegación principal de Keycloak, selecciona **Ajustes de Realm** y luego la **pestaña de Llaves**. Ubique el Certificado **RS256** y seleccione **Certificado**.

U bitwarden

Secure and trusted open source password manager for business

| master 👻 | < 0 | General L | ogin Email | Themes | Keys | Events | Localizati | on | Security defenses | Sessions | Tokens | Clie | > |
|--------------------|--------------------|-----------|----------------------|-------------|------------|---------------|------------|-----|-------------------|----------|----------|----------------|--------|
| Manage | Keys list | Providers | | | | | | | | | | | |
| Clients | T Active ke | ys 🔻 | Q , Search ke | У | | \rightarrow | | | | | 1-4 | . < | > |
| Client scopes | | | | | | | | | | | | | |
| Realm roles | Algorithm | Туре | Kid | | | | | Use | Provider | Publi | c keys | | |
| Users | AES | ОСТ | a3282835-06 | 6db-42cc-b2 | 9a-ff9692 | 26eca9 | | ENC | aes-generated | | | | |
| Groups | | | | | | | | | j | | | | |
| Sessions | HS256 | OCT | be68f437-88 | 3a6-4c3b-b9 | 2f-bf3b114 | beeb6 | | SIG | hmac-generate | d | | | |
| Events | | | | | | | | | | | | | |
| Configure | RSA-OAEP | RSA | zXKBnvtriZQ | U7MbyXJIIf6 | i0wGotgDl | oZwpG8_x7 | wE1QQ | ENC | rsa-enc-genera | ited Pu | blic key | Certi | ficate |
| Realm settings | | | | | | | | | | | | | |
| Authentication | RS256 | RSA | T3IREov-EM | gD0EnJ5AsH | lsv0GX-Z(|)s89jCy1oy6 | ofmlsE | SIG | rsa-generated | Pu | blic key | Certi | ficate |
| Identity providers | | | | | | | | | | | | | |
| User federation | | | | | | | | | | | 1-4 💌 | < | > |

Keycloak RS256 Certificate

Se requerirá el valor del certificado para la siguiente sección.

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto del Portal Keycloak. Regresa a la aplicación web de Bitwarden y selecciona **Ajustes** → **Inicio de sesión único** desde la navegación.

La pantalla de inicio de sesión único separa la configuración en dos secciones:

- La configuración del proveedor de servicios SAML determinará el formato de las solicitudes SAML.
- La configuración del proveedor de identidad SAML determinará el formato que se esperará de las respuestas SAML.

Complete los siguientes campos en la sección de configuración del proveedor de servicio SAML:

| Campo | Descripción |
|---------------------------------|--|
| Formato de ID de nombre | Seleccione Correo electrónico . |
| Algoritmo de Firma de Salida | El algoritmo que Bitwarden utilizará para firmar solicitudes SAML. |

| Campo | Descripción |
|---|--|
| Comportamiento de Firma | Si/cuando las solicitudes SAML serán firmadas. |
| Algoritmo de Firma de Entrada Mínima | Seleccione el algoritmo que el cliente Keycloak está configurado para usar para firmar documentos o afirmaciones SAML. |
| Quiero Firmas en las Afirmaciones | Si Bitwarden espera que las afirmaciones SAML estén firmadas. Si está activado, asegúrate de configurar el cliente de Keycloak para firmar afirmaciones. |
| Validar Certificados | Marque esta casilla cuando utilice certificados confiables y válidos de su IdP a través de una CA de confianza. Los certificados autofirmados pueden fallar a menos que se configuren cadenas de confianza adecuadas con la imagen de docker de inicio de sesión de Bitwarden con SSO. |

Complete los siguientes campos en la sección de configuración del proveedor de identidad SAML:

| Campo | Descripción |
|---|--|
| ID de la entidad | Ingrese la URL del reino de Keycloak en el que se creó el cliente, por ejemplo https:///rei nos/. Este campo distingue entre mayúsculas y minúsculas. |
| Tipo de enlace | Selecciona Redirigir . |
| URL del servicio de inicio de sesión único | Ingrese su URL de procesamiento maestro SAML, por ejemplo https:///reinos//protocolo/saml. |
| URL del Servicio de Cierre de Sesión Único | El inicio de sesión con SSO actualmente no admite SLO. Esta opción está planeada para un desarrollo futuro, sin embargo, puedes preconfigurarla con tu URL de cierre de sesión si lo deseas. |

U bitwarden

| Campo | Descripción |
|---|--|
| Certificado público X509 | Ingrese el certificado RS256 que se copió en el paso anterior. El valor del certificado es sensible a mayúsculas y minúsculas, espacios extra, retornos de carro y otros caracteres extraneous harán que la validación del certificado falle . |
| Algoritmo de Firma de Salida | Seleccione el algoritmo que el cliente Keycloak está configurado para usar para firmar documentos o afirmaciones SAML. |
| Deshabilitar Solicitudes de Cierre de Sesión Salientes | El inicio de sesión con SSO actualmente no admite SLO. Esta opción está planeada para un desarrollo futuro. |
| Quiere Solicitudes de Autenticación Firmadas | Si Keycloak espera que las solicitudes SAML estén firmadas. |

(i) Note

Al completar el certificado X509, toma nota de la fecha de vencimiento. Los certificados tendrán que ser renovados para prevenir cualquier interrupción en el servicio a los usuarios finales de SSO. Si un certificado ha caducado, las cuentas de Administrador y Propietario siempre podrán iniciar sesión con la dirección de correo electrónico y la contraseña maestra.

Cuando hayas terminado con la configuración del proveedor de identidad, **Guarda** tu trabajo.

⊘ Tip

Puede requerir que los usuarios inicien sesión con SSO activando la política de autenticación de inicio de sesión único. Por favor, tome nota, esto también requerirá la activación de la política de organización única. Más información.

Ajustes adicionales de Keycloak

En la pestaña Configuración del cliente Keycloak, hay opciones de configuración adicionales disponibles:

| Campo | Descripción |
|----------------------|--|
| Firmar Documentos | Especifique si los documentos SAML deben ser firmados por el reino Keycloak. |
| Firmar Declaraciones | Especifique si las afirmaciones de SAML deben ser firmadas por el reino de Keycloak. |

| Campo | Descripción |
|--|--|
| Algoritmo de Firma | Si Afirmaciones de Signo está habilitado, selecciona con qué algoritmo firmar (<mark>sha-256</mark> por defecto). |
| Formato de Identificación de Nombre | Seleccione el formato de ID de nombre que Keycloak utilizará en las respuestas SAML. |

Una vez que hayas completado el foro, selecciona **Guardar**.

Prueba la configuración

Una vez que tu configuración esté completa, pruébala navegando a https://vault.bitwarden.com, ingresando tu dirección de correo electrónico, seleccionando **Continuar**, y seleccionando el botón **Empresa Único-Inicio**:

| Log in to Bitwarden | | | |
|--|--|--|--|
| Email address (required) Remember email | | | |
| Continue | | | |
| or | | | |
| Section 2.1 Sectio | | | |
| 🖻 Use single sign-on | | | |
| New to Bitwarden? Create account | | | |

Inicio de sesión único empresarial y contraseña maestra

Ingrese el identificador de organización configurado y seleccione **Iniciar sesión**. Si su implementación está configurada con éxito, será redirigido a la pantalla de inicio de sesión de Keycloak:

| Log In Username or email | |
|-----------------------------|--|
| Password | |
| Log In | |

Keycloak Login Screen

¡Después de autenticarte con tus credenciales de Keycloak, ingresa tu contraseña maestra de Bitwarden para descifrar tu caja fuerte!

(i) Note

Bitwarden no admite respuestas no solicitadas, por lo que iniciar el inicio de sesión desde su IdP resultará en un error. El flujo de inicio de sesión de SSO debe iniciarse desde Bitwarden.