

ADMIN CONSOLE > MORE

Proof-of-Concept Project Checklist

View in the help center:

<https://bitwarden.com/help/proof-of-concept/>

Proof-of-Concept Project Checklist

This guide is designed by our Product, Implementation, and Sales specialists at Bitwarden to help guide your business in running a PoC of Bitwarden. Bitwarden offers a free trial for [Enterprise Organizations](#), and we're confident that spreading out these steps over that time will help shape a successful PoC.

Phase 1: Installation

Step	Key Person	Action	Resource	Duration (hrs)
Identify Organization Owner	Organization Owner	Create a free Bitwarden account for your Organization Owner, who will manage your Organization's settings, structure, and subscription. Note: If you wish to have a EU-hosted cloud instance, instead navigate to https://vault.bitwarden.eu	Create your Bitwarden Account	0.1
Create Organization	Organization Owner	Create a free organization on the Bitwarden cloud. Once created, let us know and we'll upgrade you to an Enterprise trial. If you're self-hosting, this Organization will be used only for billing purposes.	Organizations	0.1
Self-hosting only Download a license file for your self-hosted installation	Organization Owner	If you're self-hosting Bitwarden, a license file enables Enterprise functionality and the right number of seats for your instance.	License Paid Features	0.1
Self-hosting only Install self-hosted instance	Organization Owner / IT Team	Setup your Bitwarden server. We recommend deploying on Linux for optimal performance and lowest total cost of ownership.	Install and Deploy	2.5
Add administrators	Organization Owners + Admins	Onboard Admins to Bitwarden, who can manage most Organization structures. We also recommend adding a second Owner for redundancy.	User Management	0.2

Step	Key Person	Action	Resource	Duration (hrs)
Create Collections for vault items	Organization Owners + Admins	Collections gather items for secure sharing with Groups of users.	Collections	0.25
Create Groups to assign users to	Organization Owners + Admins	Groups gather users for scalable assignment of permissions and access to Collections. If you decide to sync Groups and users from your Identity Provider or Directory Service, you may need to reconfigure user and Group assignments later.	Groups	0.25
Assign Groups to Collections	Organization Owners + Admins	Assign Groups to Collections, making shared items available to supersets of users.	Collections Assignment	0.25
Share items to Collections	Organization Owners + Admins	Add items manually or import data from another password management application.	Sharing Import to an Organization	0.25
Select collection management settings	Owner	Choose how collections will behave in the organization. These settings allow for a spectrum of full admin control to completely self-serve where users can create their own collections. These settings can be used to establish a policy of least privilege.	Collection Management Resource: Collections Management Settings	
Configure Enterprise Policies	Organization Owners + Admins	Enterprise Policies can be used to tailor your Bitwarden Organization to fit your security needs. Enable and configure desired policies before user onboarding begins.	Enterprise Policies	0.1

Step	Key Person	Action	Resource	Duration (hrs)
Configure Login with SSO (optional)	Organization Owners + Admins	Configure Bitwarden to authenticate using your SAML 2.0 or OIDC Identity Provider. Choose how vault data will be decrypted after users authenticate using SSO. For a streamlined SSO workflow for end-users, verify the ownership of your domain with a DNS TXT record.	About Login with SSO Member Decryption Options Domain Verification Resource: Choose the Right SSO Login Strategy	1.5
Review additional integrations	Organization Owners + Admins	Visit the Integrations page in the Admin Console to review relevant integrations and complete the set-up process. Additional integrations may be achieved using the two Bitwarden APIs	Bitwarden Integrations	
Add early users to Groups	Organization Owners + Admins	Add a set of users to your Organization manually and assign them to different groups. With these users, you'll broadly test all pre-configured functionality in the next step, before moving on to advanced functions like Directory Connector.	User Management	0.5
Download Bitwarden Client Applications	All POC users	All Organization members added for the POC should download Bitwarden on an assortment of devices, login, and test access to shared items/Collections/Groups and application of applied Policies. If you're self-hosting, users will need to connect each client to your server.	Download Bitwarden	0.5
Choose between SCIM and Directory Connector	Organization Owners + Admins	Decide whether SCIM or Directory Connector is the right user onboarding and user lifecycle management solution for your Organization.	About SCIM About Directory Connector	1

Step	Key Person	Action	Resource	Duration (hrs)
Configure and test user onboarding with SCIM or Directory Connector	Organization Owners + Admins	Configure and test Bitwarden SCIM integrations or the Bitwarden Directory Connector application to automatically sync users and groups.		1.5
Onboard users with SCIM or Directory Connector	Organization Owners + Admins	Execute on SCIM or Directory Connector syncing to invite your remaining users to the Organization.		1

Phase 2: Test and evaluate features

When evaluating Bitwarden Password Manager be sure to also review the features highlighted below. Choose to use your own data for your POC or import an [example vault](#) for testing.

Feature	Action	Resource
Account Recovery Administration	As a test, begin the account recovery process for an enrolled user. Create a new master password for the user. Send that new master password to the user in a secure channel, such as through a Bitwarden Send, so they can log in and create a new master password. Note: in cases where access to the account is needed, the admin can use the new master password to log in and access stored individual vault items. This simple, streamlined process makes it easy to reset account passwords or gain access to accounts for separated employees.	Account Recovery
Assign an item to multiple collections	In the admin console, go to Collections, choose any vault item, and click on the three dot menu > Collections. Use the check boxes to add that item to as many collections as you like. Navigate to the collections you assigned the item to and see it there. Make a change to the item, such as the name, and note that the update is reflected in all the other collections the item is assigned to. This makes updating or deleting an item easy and instant, with no need to duplicate items to have it available to multiple user groups.	Move an item between collections

Feature	Action	Resource
Download and test the CLI	The Bitwarden command-line interface (CLI) allows for scripting, automation, and API-based commands.	Password Manager CLI
Review collections access options	In the admin console, go to Settings > Organization info > Collection management. There are two toggleable options, leading to four possible configurations. These options allow for a policy of least privilege, where only intended users have access to vault items. Your organization can be configured so that Administrators will only have access to items that they were intentionally assigned to. These options and a collection-level Manage collection permission enables a framework similar to Privileged-Access Management (PAM) solutions. Individual vault item access and adjustments to the collection management settings trigger auditable security events that can raise alerts within Security Incident Event Management (SIEM) tools. Note: Collections management settings are only available to the organization owner	Collections management settings
Public and Vault APIs	Review the two APIs available to your organization: The Public API and the Vault Management API. These APIs can be used for scripting, automation, and integration with third-party applications, such as SIEM tools.	Bitwarden APIs
Event logs	Navigate to the Event logs in the Admin Console. Review the data displayed on-screen, and export the logs for more detailed viewing in another application. Event logs can also be viewed for specific users or vault items from the Members or Collections windows through the item modals. These detailed and auditable event logs aid in security investigation, auditing, and compliance certification.	Event Logs
Bitwarden Send	Create a test Send from any Bitwarden client. Choose to send either text or a file, adjust the security settings to your preferences and save. Share the link or test it yourself. The file or text is encrypted end-to-end. The key to decode the file is included within the shared URL and is a zero-knowledge process. Bitwarden Send can be used to share sensitive information within the company, such as HR documents, or share with external partners, such as creative agencies. It may also be completely disabled with an enterprise policy.	Bitwarden Send

Feature	Action	Resource
Export and Import data	Export the items you have stored in your organization vault. The created export file can be used as a partial backup solution or for migrating to another service if necessary. Data can also be imported into the organization vault from other services. Test the import function from your prior solution or from this example file.	Export your data
Nested collection	Create a nested collection - one collection within another. In the Admin Console, open a parent collection, and from the New dropdown select Collection. The nested collection is for display purposes for organizing the vault and will not inherit permissions from the parent collection. This prevents accidental access and ensures all access to vault items is intentional.	Nested Collections
Custom role creation	Access a test user in your organization and change their role to Custom. Evaluate the available options. These permissions are useful for various scenarios, such as giving Help Desk employees access to the organization to assist end users, but limiting their ability to access other settings such as SSO.	Custom role
Manage collection permission	Create a test collection, such as "Finance team test." Assign an individual user, such as your company's accountant, to that collection and grant the Manage collection permission. This user can now add/remove items, and add/remove users and groups to the collection. Assign a group, such as "IT department" to the collection with the same Manage collection permission. Now anyone within that group can add/remove items and add/remove users and groups. This permission for collections allows for delegation of control to team leads or to a group of administrators that help in the day-to-day company work processes.	User permissions
Compare app store ratings of clients	Read the reviews on app stores and note the rating of the Bitwarden app and compare it to other solutions. End user satisfaction is an important factor for successful adoptions, and app ratings offer a proxy evaluation of usability.	Bitwarden app store listings

Feature	Action	Resource
Free families plan for all enterprise users	Visit Account settings > Free Bitwarden Families. All users of your enterprise plan are granted a free license for a Bitwarden Families Plan. This reinforces good security habits by having employees practice them at home. Note that the families plan requires a different email address than the user's email that is attached to the enterprise plan. This maintains separation of personal and work accounts.	Families for enterprise
Browse the Bitwarden Community Forum	Bitwarden has an active community of users, both personal and professional. The community forums are a channel for providing feedback, getting support from others, and participating in user research studies and beta programs.	Bitwarden Community Forum
Visit the Bitwarden GitHub repo and review source code	View the Bitwarden source code and browse the available repositories to see the work going into Bitwarden Password Manager. Bitwarden is open source, and all the code is visible for security researchers, the community, and customers to review. Source code transparency is the foundation of trust in important security solutions. Having the eyes of thousands of security enthusiasts on the Bitwarden code makes it safer, with any vulnerabilities quickly discovered and rapidly resolved.	Open source security Bitwarden GitHub

Deployment best practices

We've seen a lot of deployments and have found that taking the following actions can positive contribute towards a successful PoC and successful adoption with your users:

Step	Key Person	Action	Resource
Determine timeline for rollout to first-wave users	Senior Leadership & Security teams	There are lots of different strategies for rolling out Bitwarden. Take things at whatever pace best suits your team.	

Step	Key Person	Action	Resource
Craft internal messaging about Bitwarden rollout	Internal Training & Managers	Bitwarden provides a lot of resources to help users quickly adopt, check some out with the links in the Resource(s) column.	Bitwarden YouTube Channel Help Center Learning Center

Next steps

When you're ready to move from a proof-of-concept to putting Bitwarden into production, use the following resources:

- [Prepare your Trial Organization for Production](#)