bitwarden | Help Center Article

ADMIN CONSOLE > LOGGA IN MED SSO >

About Trusted Devices

View in the help center:
https://bitwarden.com/help/about-trusted-devices/

About Trusted Devices

SSO with trusted devices allows users to authenticate using SSO and decrypt their vault using a device-stored encryption key, eliminating the need to enter a master password. Trusted devices must either be registered in advance of the login attempt, or approved through a few different methods.

SSO with trusted devices gives business end users a passwordless experience that is also zero-knowledge and end-to-end encrypted. This prevents users from getting locked out due to forgotten master passwords and allows them to enjoy a streamlined login experience.

Start using trusted devices

To get started using SSO with trusted devices:

1. Setup SSO with trusted devices for your organization.
2. Provide administrators with information on how to approve device requests.
3. Provide end-users with information on how to add trusted devices.

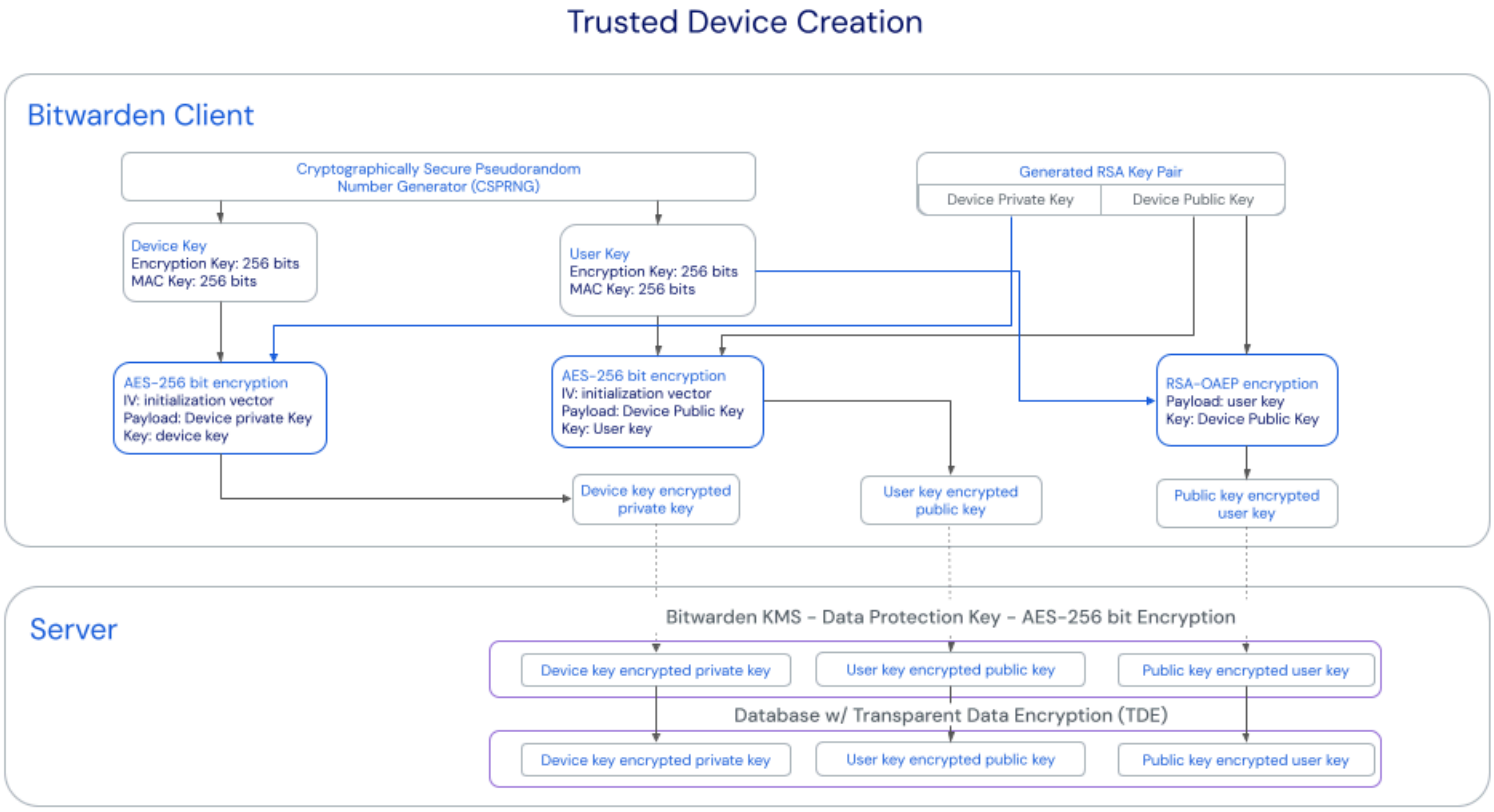
How it works

The following tabs describe encryption processes and key exchanges that occur during different trusted devices procedures:

⇒Onboarding

När en ny användare går med i en organisation skapas en **kontoåterställningsnyckel** (läs mer) genom att kryptera deras kontokrypteringsnyckel med **organisationens offentliga nyckel**. Kontoåterställning krävs för att aktivera SSO med betrodda enheter.

Användaren tillfrågas sedan om de vill komma ihåg, eller lita på, enheten. När de väljer att göra det:



Create a trusted device

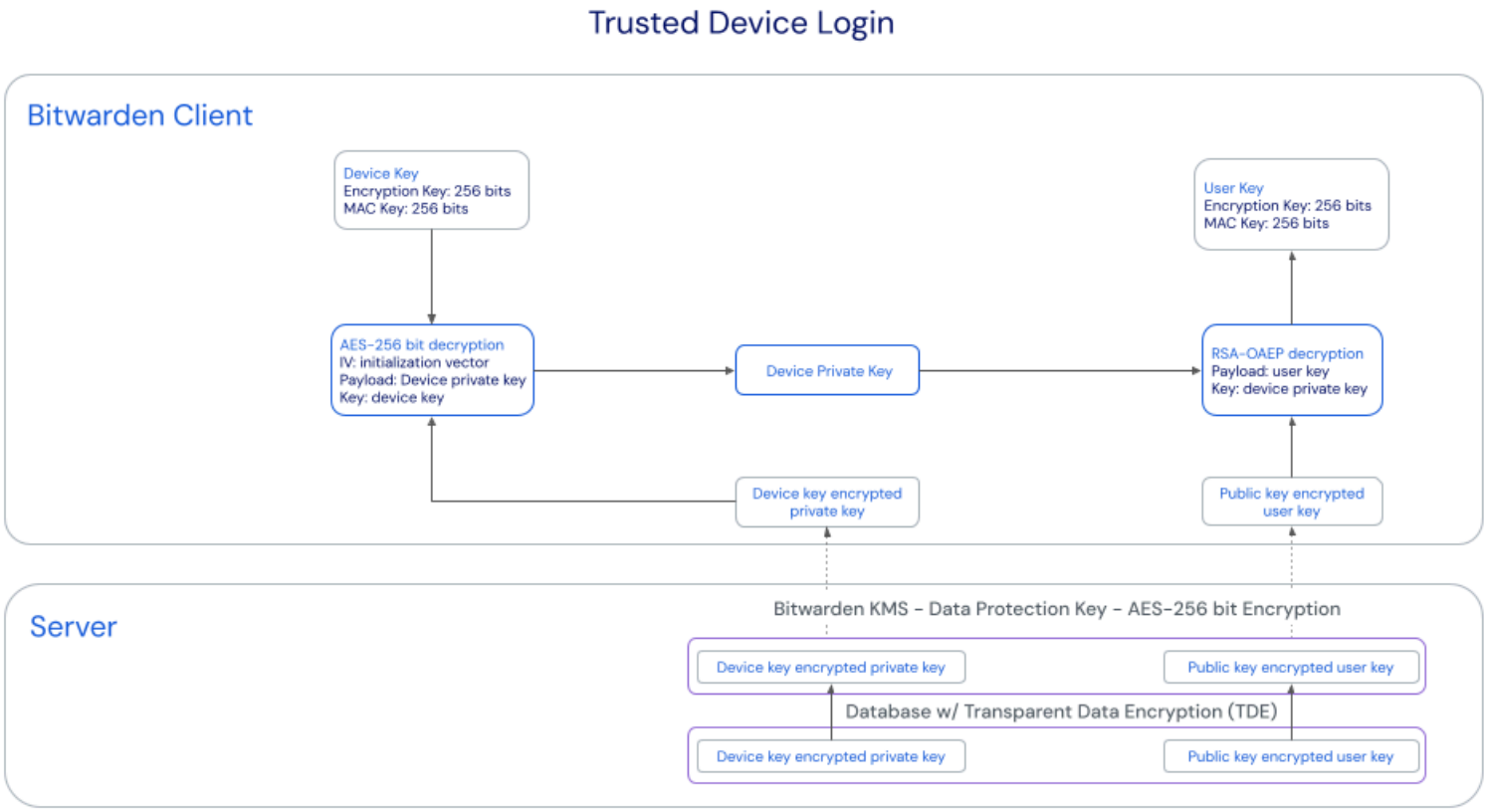
1. En ny **enhetsnyckel** genereras av klienten. Denna nyckel lämnar aldrig klienten.
2. Ett nytt RSA-nyckelpar, kallat **Device Private Key** och **Device Public Key**, genereras av klienten.
3. Användarens kontokrypteringsnyckel krypteras med den okrypterade **enhetens publika nyckel** och det resulterande värdet skickas till servern som den **offentliga nyckelkrypterade användarnyckeln**.
4. Den offentliga **enhetens nyckel** krypteras med **användarens kontokrypteringsnyckel och det resulterande värdet skickas till servern som den användarnyckelkrypterade publika nyckeln**.
5. **Enhetens privata nyckel** krypteras med den första **enhetsnyckeln** och det resulterande värdet skickas till servern som den **enhetsnyckelkrypterade privata nyckeln**.

Den **offentliga nyckel-krypterade användarnyckeln** och **enhetsnyckel-krypterade privata nyckel** kommer, avgörande, att skickas från server till klient när en inloggning initieras.

Den **användarnyckel-krypterade publika nyckeln** kommer att användas om användaren behöver rotera sin kontokrypteringsnyckel.

⇒Loggar in

När en användare autentiserar med SSO på en redan betrodd enhet:



Use a trusted device

1. Användarens **Public Key-Encrypted User Key**, som är en krypterad version av kontokrypteringsnyckeln som används för att dekryptera valvdata, skickas från servern till klienten.

2. Användarens **Device Key-Encrypted Private Key**, vars okrypterade version krävs för att dekryptera den **Public Key-Encrypted User Key**, skickas från servern till klienten.

3. Klienten dekrypterar den **enhetsnyckel-krypterade privata nyckeln** med hjälp av **enhetsnyckeln**, som aldrig lämnar klienten.

4. Den nu okrypterade **enhetens privata nyckel** används för att dekryptera den **offentliga nyckel-krypterade användarnyckeln**, vilket resulterar i användarens kontokrypteringsnyckel.

5. Användarens kontokrypteringsnyckel dekrypterar valvdata.

⇒Godkännande

När en användare autentiserar med SSO och väljer att dekryptera sitt valv med en opålitlig enhet (dvs. en **Device Symmetric Key finns** inte på den enheten), måste de välja en metod för att godkänna enheten och eventuellt lita på den för framtida användning utan ytterligare godkännande. Vad som händer härnäst beror på det valda alternativet:

- **Godkänn från en annan enhet**:

  1. Processen som dokumenteras här utlöses, vilket resulterar i att klienten har erhållit och dekrypterat kontokrypteringsnyckeln.

  2. Användaren kan nu dekryptera sina valvdata med den dekrypterade kontokrypteringsnyckeln. Om de har valt att lita på enheten etableras förtroende med klienten enligt beskrivningen på **fliken** Onboarding.

- **Begär administratörsgodkännande**:
  1. Den initierande klienten POSTAR en begäran, som inkluderar kontots e-postadress, en unik offentlig nyckel för autentiseringsbegäran[a] och en åtkomstkod, till en tabell för autentiseringsbegäran i Bitwarden-databasen.
  2. Administratörer kan godkänna eller neka begäran på sidan Enhetsgodkännanden.
  3. När begäran godkänns av en administratör, krypterar den godkännande klienten användarens kontokrypteringsnyckel med hjälp av den **offentliga autentiseringsnyckeln** som finns med i begäran.
  4. Den godkännande klienten PUTAR sedan den krypterade kontokrypteringsnyckeln till posten för autentiseringsbegäran och markerar begäran som uppfylld.
  5. Den initierande klienten HÅR den krypterade kontokrypteringsnyckeln **och dekrypterar** den lokalt med den privata nyckeln för autentiseringsbegäran.
  6. Genom att använda den dekrypterade kontokrypteringsnyckeln etableras förtroende med klienten enligt beskrivningen på **fliken** Onboarding.

[a] – **Offentliga** och **privata autentiseringsnycklar** genereras unikt för varje lösenordslös inloggningsförfrågan och existerar bara så länge som begäran gör det. Ej godkända förfrågningar upphör att gälla efter 1 vecka.

- **Godkänn med huvudlösenord**:
  1. Användarnas kontokrypteringsnyckel hämtas och dekrypteras enligt dokumentationen i avsnittet Autentisering och dekryptering av säkerhetsdokumentet.
  2. Genom att använda den dekrypterade kontokrypteringsnyckeln etableras förtroende med klienten enligt beskrivningen på **fliken** Onboarding.

⇒Nyckelrotation

> **ⓘ Note**
>
> Only users who have a master password can rotate their account encryption key. Learn more.

När en användare roterar sin kontokrypteringsnyckel, under den normala rotationsprocessen:

1. Den **användarnyckelkrypterade publika nyckeln** skickas från servern till klienten och dekrypteras sedan med den gamla kontokrypteringsnyckeln (aka **Användarnyckel), vilket** resulterar i **enhetens publika nyckel**.
2. Användarens nya kontokrypteringsnyckel krypteras med den okrypterade **enhetens publika nyckel** och det resulterande värdet skickas till servern som den nya **offentliga nyckelkrypterade användarnyckeln**.
3. Den offentliga **enhetens nyckel** krypteras med **användarens nya kontokrypteringsnyckel och det resulterande värdet skickas till servern som den nya användarnyckelkrypterade publika nyckeln**.
4. Betrodda enhetskrypteringsnycklar för alla andra enheter som finns kvar på serverlagring rensas för användaren. Detta lämnar endast de tre nödvändiga nycklarna (**public Key-Encrypted User Key**, **User Key-Encrypted Public Key** och **Device Key-Encrypted Private Key** som inte ändrades av denna process) för den enstaka enheten kvar på servern.

Alla nu opålitliga klienter måste återupprätta förtroendet genom en av metoderna som beskrivs på **fliken** Godkännande.

Keys used for trusted devices

This table provides more information about each key used in the procedures described above:

Key	Details
Device Key	AES-256 CBC HMAC SHA-256, 512 bits in length (256 bits for key, 256 bits for HMAC)
Device Private Key & Device Public Key	RSA-2048 OAEP SHA1, 2048 bits in length
Public Key-Encrypted User Key	RSA-2048 OAEP SHA1
User Key-Encrypted Public Key	AES-256 CBC HMAC SHA-256
Device Key-Encrypted Private Key	AES-256 CBC HMAC SHA-256

Impact on master passwords

While SSO with trusted devices eliminates the need for a master password, it doesn't in all cases eliminate the master password itself:

- If a user is onboarded **before** SSO with trusted devices is activated, their account will retain its master password.
- If a user is onboarded **after** SSO with trusted devices is activated and they select **Log in → Enterprise SSO** from the organization invite for JIT provisioning, their account will not have a master password. Should you change to the master password member decryption option, these users will be prompted to create a master password when they log in as long as they are still a member of the organization (learn more).

  > **⚠ Warning**
  >
  > For those accounts that do not have master passwords as a result of SSO with trusted devices, removing them from your organization will cut off all access to their Bitwarden account unless:
  >
  > 1. You assign them a master password using account recovery beforehand.
  > 2. The user logs in at least once post-account recovery in order to fully complete the account recovery workflow.
  >
  > Additionally, users will not be able to re-join your organization unless the above steps are taken before they are removed from the organization. In this scenario, the user will be required to delete their account and be issued a new invitation to create an account and join your organization.
  >
  > Revoking access to the organization, but not removing them from the organization, will still allow them to log in to Bitwarden and access **only** their individual vault.

- If a user account is recovered using account recovery, their account will necessarily be assigned a master password. A master password cannot currently be removed from an account once it has one, so to avoid this outcome we recommend that you (i) instruct the user to

export their data to a backup, (ii) completely delete the lost account, (iii) ask the user to re-onboard to your organization using trusted devices and (iv) once they've done so instruct them to import their backup.

Impact on other features

Depending on whether a master password hash is available in memory for your client, which is dictated by how your client application is initially accessed, it may exhibit the following behavior changes:

Feature	Impact
Verification	There are a number of features in Bitwarden client applications that ordinarily require entry of a master password in order to be used, including exporting vault data, changing two-step login settings, retrieving API keys, and more. If the user doesn't use a master password to access the client, **all these features** will replace master password confirmation with email-based TOTP verification.
Vault lock/unlock	Under ordinary circumstances, a locked vault can be unlocked using a master password. If the user doesn't use a master password to access the client, locked client applications can only be unlocked with a PIN or with biometrics. If neither PIN nor biometrics are enabled for a client application, the vault will always log out instead of lock. Unlocking and logging in will **always** require an internet connection.
Master password re-prompt	If the user does not unlock their vault with a master password, master password re-prompt will be disabled.
Changing email address	Users who do not have master passwords **will not** be able to change their email address.
CLI	Users who do not have master passwords **will not** be able to access Password Manager CLI.