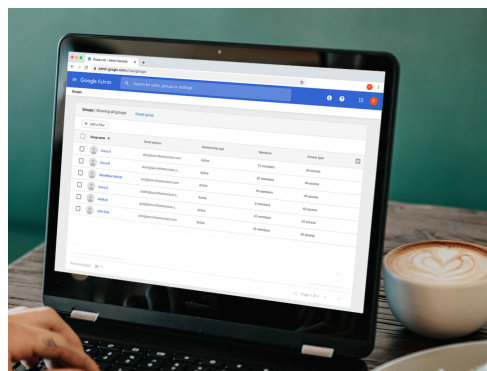




Profile separation with Chrome browser

Last updated July 9, 2024



Introduction

The lines between work and personal life continue to blur, with employees increasingly using work devices for personal activities and vice versa. Additionally, organizations frequently outsource key projects to third parties. This trend makes separation vital to maintain a clear separation between personal data and different working environments. Inadvertent mixing of this data can create significant legal risks and compromise organizational control.

To address these evolving work patterns, we've adapted Chrome to provide a fully customizable solution that seamlessly meets your organization's needs. Chrome profiles offer a user-friendly way to keep personal and work browsing data separate, simplifying the experience, preventing data breaches, and ensuring privacy and compliance.

Examples of browsing data stored in profiles:

- Bookmarks
- History
- Open tabs
- Saved passwords
- Apps/PWAs
- Autofill information
- Reading lists
- Cache
- Cookies
- Preferences
- Themes
- Typed URLs
- Extensions

Chrome has three key states: Local Profile, Personal Profile, and Work Profile.

1. Chrome Local Profile:

- This is the most basic experience.
- Your browsing activity within the Local Profile stays on the device and disappears when you remove the profile.
- **No Google account has been used to sign in or sync data with this profile.**

2. Chrome Personal Profile:

- This is the standard way to use Chrome for personal browsing.

- You sign in with your personal account to access features like bookmarks, browsing history, saved password, extensions, sync.
- Data is synched to the profile and transferred to the user's account on Google Servers.
- This mode provides a personalized browsing experience with your data readily available.

3. Chrome Work Profile:

- This mode involves signing into Chrome with your work or organization's work account (usually different from your personal account).
- It offers many similar features to a personal profile, but with additional benefits for organizations:
 - **Separation of data:** Keeps your work browsing data separate from your personal data, preventing accidental mixing.
 - **Security policies:** Organizations can enforce security settings like website blocking or extension restrictions to protect your work environment.
 - **Work profiles:** Organizations can manage and configure Chrome profiles for employees, ensuring consistency and compliance with company policies.

This technical paper will guide you through common scenarios organizations face daily. It will ensure you configure profiles in a manner that prioritizes both security and user experience.

Google has a continued commitment to the privacy of their users. We believe that these changes will better protect the privacy of end users that may use personal devices for work or access personal resources on their work devices. For more information check out the blog post for this [initiative](#) and the [YouTube video](#).

Scenario 1. Example.com wants to allow end-users to sign-in to Chrome using their work account.

In this case, you need to make sure that [Browser Sign-in settings](#) in Chrome Enterprise Core has been set to Google's default, ie **Enable browser sign-in**.

Scenario 1.1 [Example.com](#) wants to force end-users to sign-in to a separate work profile and suggest that they automatically import browser data from their Local Profile.

Admin experience

In this case, you'll have to configure the [ProfileSeparationSettings](#) policy and the [ProfileSeparationDataMigrationSettings](#) policy as set below:

Enterprise profile separation = Enforce profile separation


Chromium name ProfileSeparationSettings 	Supported on Chrome (Windows, Mac, Linux) since version 119
Inheritance	Locally applied ▼
Configuration	Enforce profile separation ▼ Controls whether a user is required to create a browser profile after signing in to the content area. This policy overrides the 'Separate profile for managed Google identity' policy.

Figure 1

Profile separation data migration = Suggest to users to bring their existing data in the managed profile and give them a choice not to

Chromium name ProfileSeparationDataMigrationSetti...	Supported on Chrome (Windows, Mac, Linux) since version 119
Inheritance	Locally applied ▼
Configuration	Suggest to users to bring their existing data in the managed profile and give them a choice not to ▼

Figure 2

End user experience: Local Profile to Work Profile

When a user signs into a Google service for the first time with their work account, the profile separation dialog will appear and the migration data box will be **checked**. If the user clicks on the continue button, a new profile is generated with the user's browsing data.

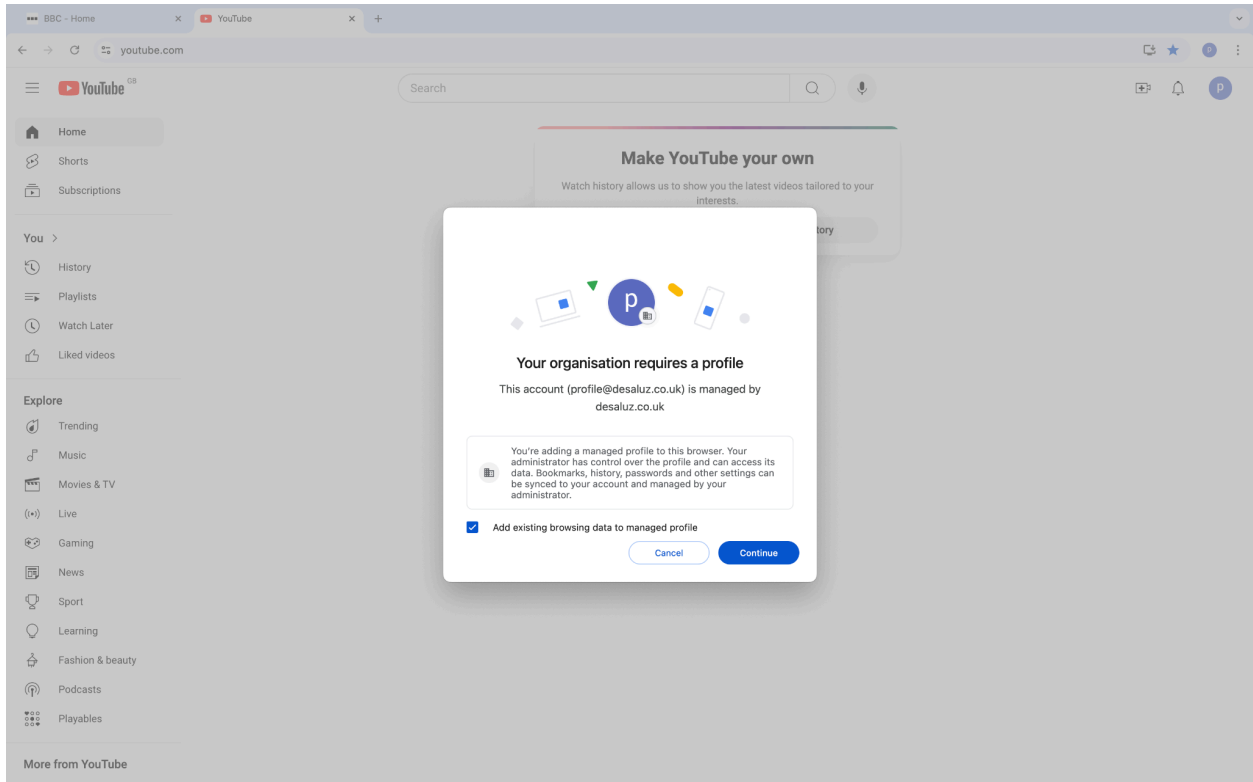


Figure 3

End user experience: Personal Profile to Work Profile

When a user is already signed in with a non-work account and attempts to add a work account, they will be required to create a new profile. In this case however, they will not be able to migrate their data over to the new profile. This is because migration options are offered only when the user is signing in for the first time into the content area.

To migrate data from a personal profile to your work profile, sign out of all Google Services within the profile before signing in with your work account.

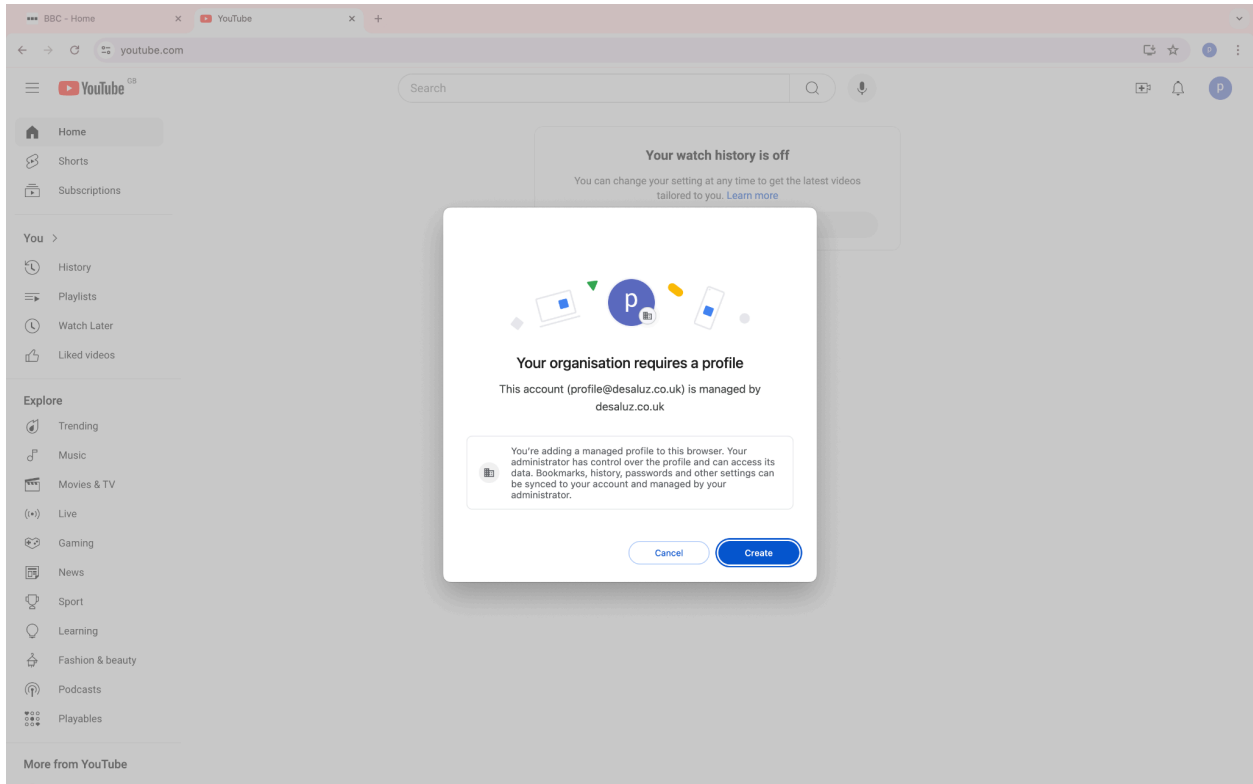


Figure 4

End user experience: Add profile

When signing into Chrome directly from the profile picker, users will not see data migration options. They will be prompted for their email address and password, followed by a profile creation notification.

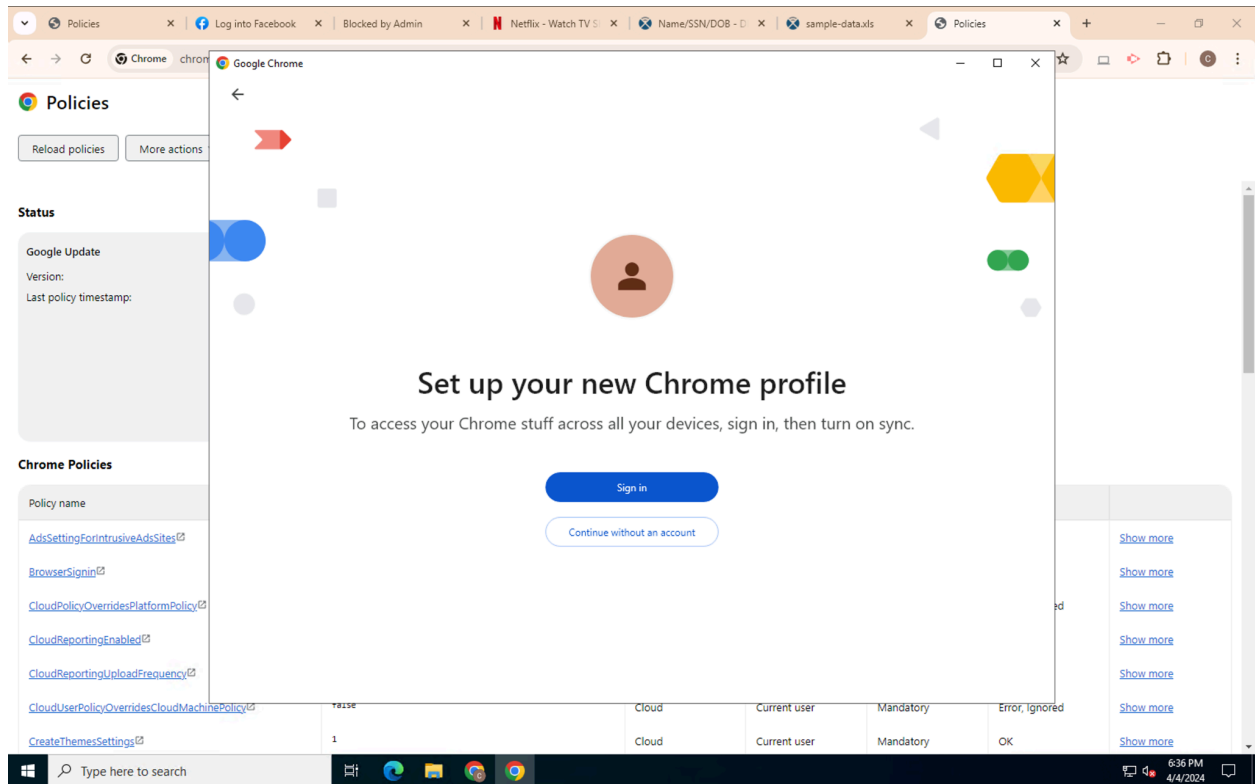


Figure 5

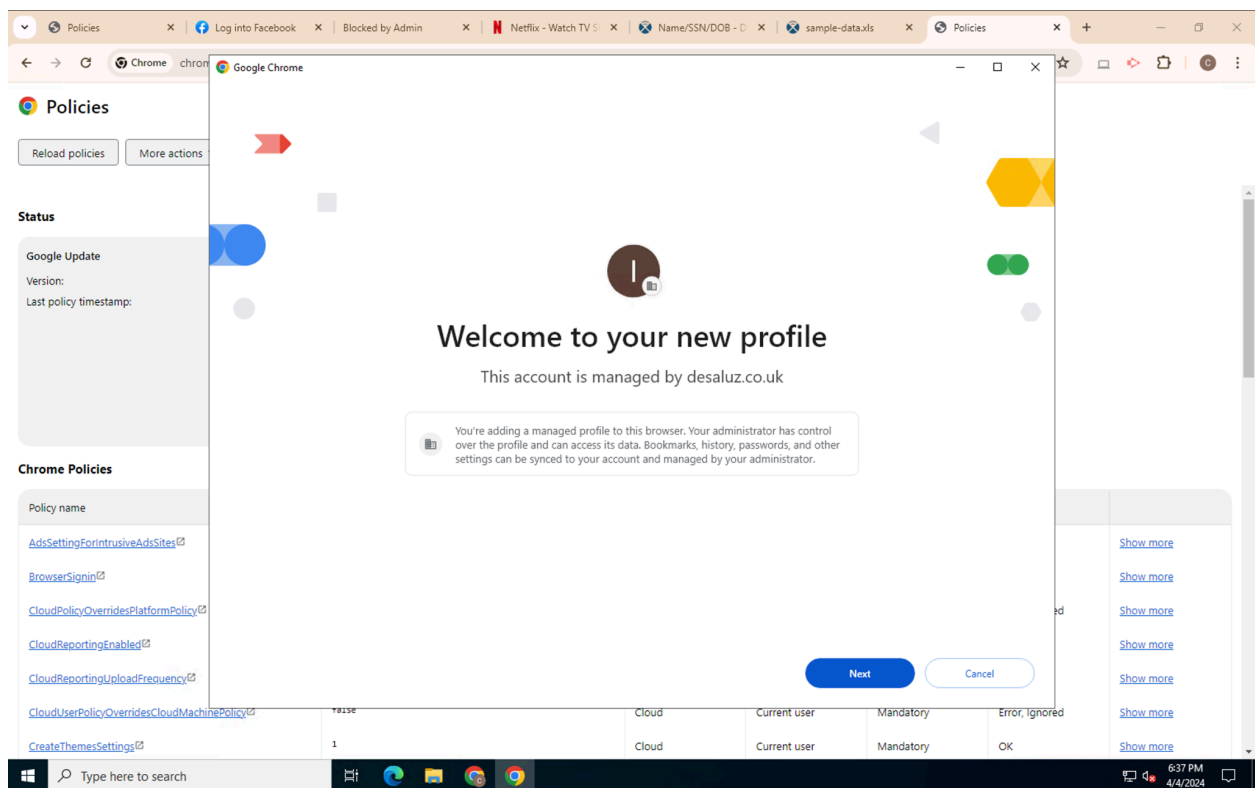


Figure 6

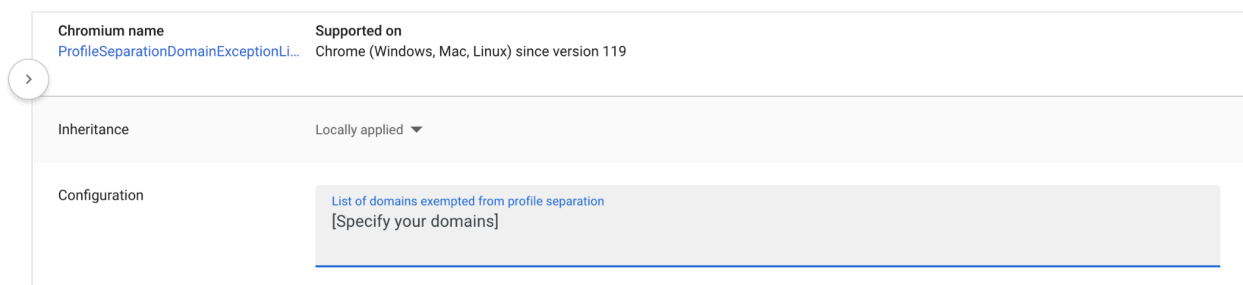
Scenario 1.1.1 [Example.com](#) wants to allow specific domains to coexist in the same work profile

It is common for organizations to own multiple domains, especially as a result of mergers or acquisitions. Consequently, users may have multiple work accounts that they use to sign in to Google services. To streamline the user experience, organizations may want to exempt users from having to create a new profile every time they sign in to Google services with a different work account.

Admin experience

In this case, you'll have to configure the [ProfileSeparationDomainExceptionList](#) policy as set below:

Profile separation exemptions = [Specify your domains]



The screenshot shows the configuration page for the [ProfileSeparationDomainExceptionList](#) policy in the Google Admin console. The page has a left sidebar with a navigation menu. The main content area is divided into three sections: 'Chromium name', 'Supported on', and 'Configuration'. The 'Chromium name' section shows the policy name. The 'Supported on' section indicates that the policy is supported on Chrome (Windows, Mac, Linux) since version 119. The 'Configuration' section is currently set to 'Locally applied' and contains a text input field labeled 'List of domains exempted from profile separation' with the placeholder text '[Specify your domains]'. A blue underline is visible at the bottom of the input field.

Figure 7

End user experience: Sign-in with an account from a domain on the ProfileSeparationDomainExceptionList Policy

If a user attempts to sign into a Google service within a work profile using an account whose domain is specified in the [ProfileSeparationDomainExceptionList](#) policy, they will not be prompted to create a new profile. They will however get a suggestion to create a profile, but they can choose not to.

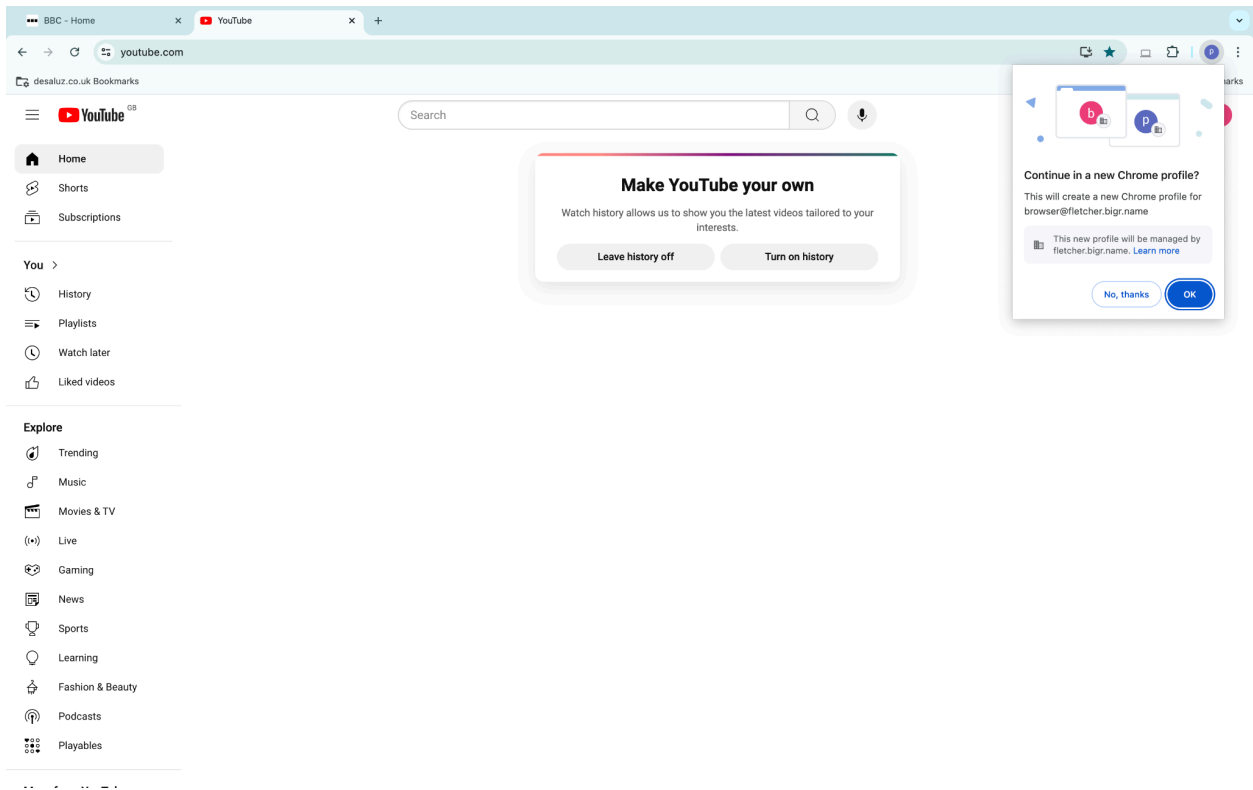


Figure 8

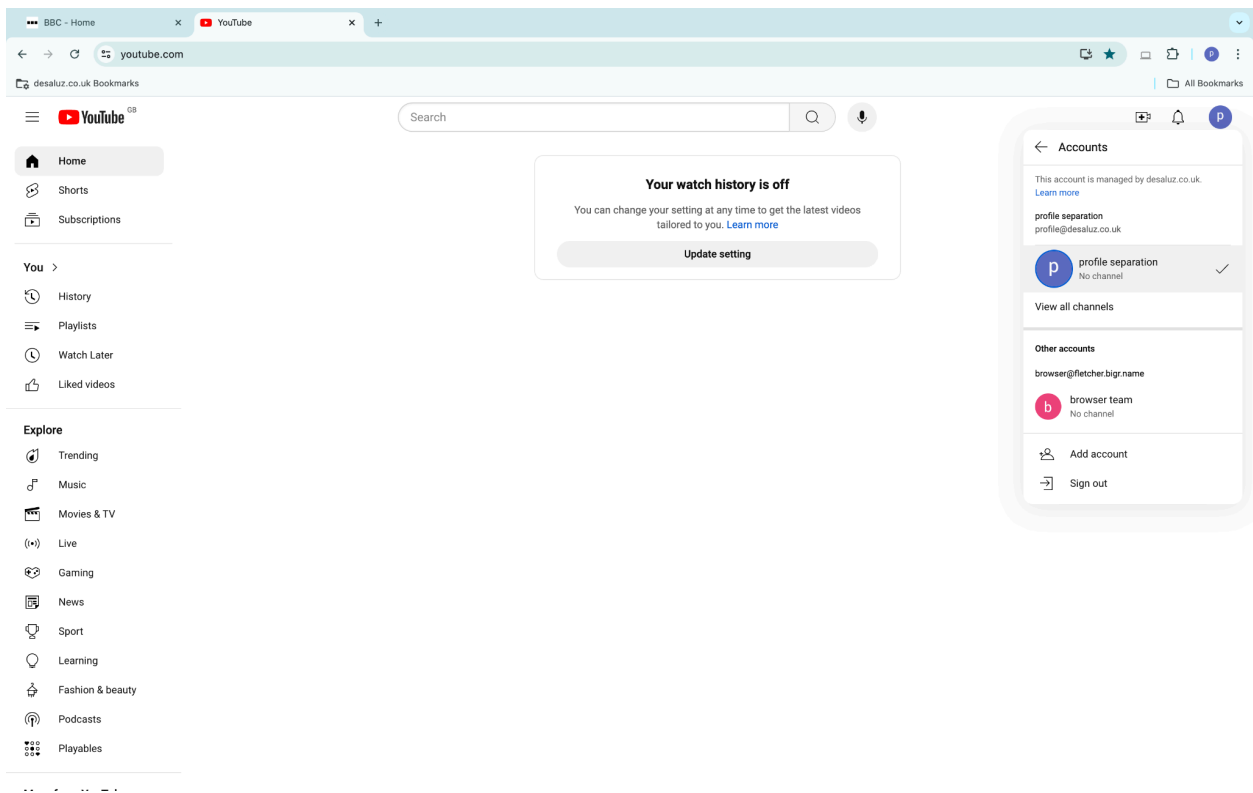


Figure 9

End user experience: Sign-in with an account from a domain not on the ProfileSeparationDomainExceptionList Policy

If a user attempts to sign into a Google service within a work profile using an account whose domain is not specified in the [ProfileSeparationDomainExceptionList](#) policy, a new profile will be created.

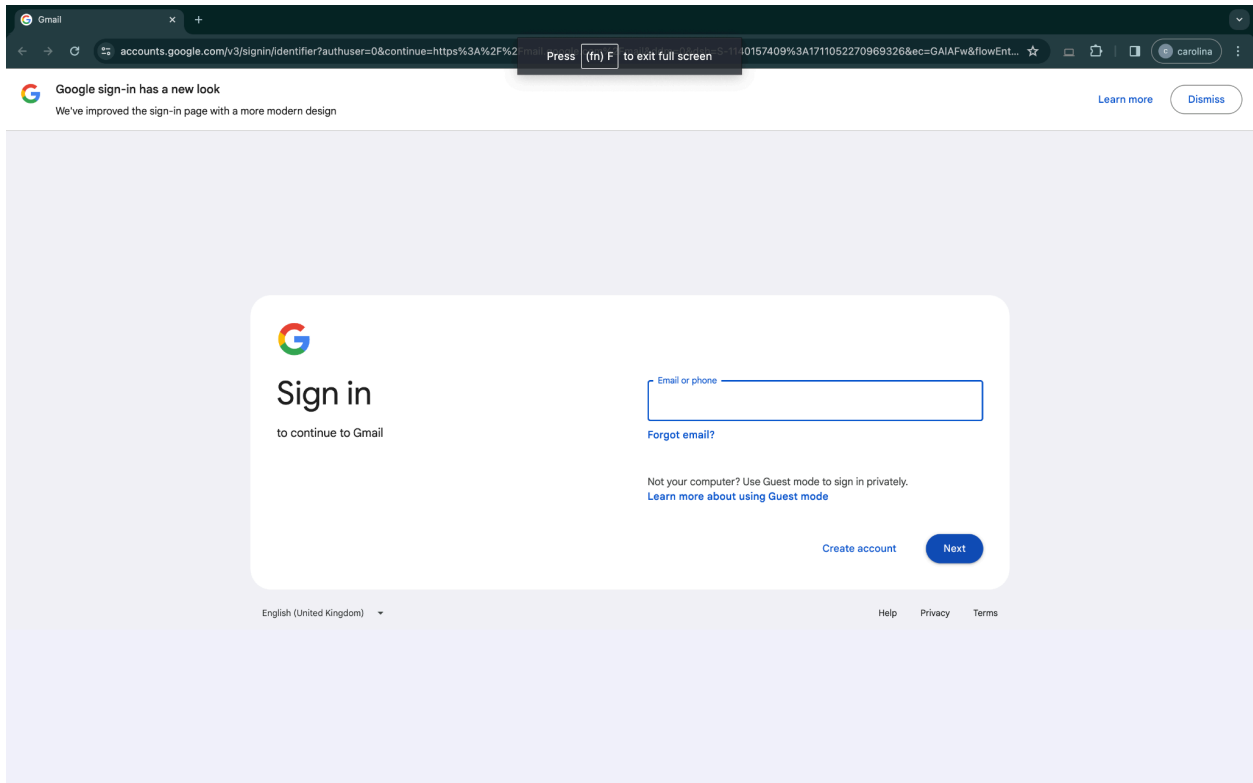


Figure 10

Note 1: If the account that the user is attempting to sign into a Google service within the work profile is targeted by the ProfileSeparationSettings policy, and the policy is enforcing profile separation, the user will be forced to create a new profile. This behavior occurs even if the domain is specified in the ProfileSeparationDomainExceptionList policy.

Scenario 1.2 [Example.com](#) wants to force end-users to sign-in to a separate work profile and allow them to automatically import browser data from their Local Profile.

Admin experience

In this case, you'll have to configure the [ProfileSeparationSettings](#) policy and the [ProfileSeparationDataMigrationSettings](#) policy as set below:

Enterprise profile separation = Enforce profile separation


Chromium name	Supported on
ProfileSeparationSettings 	Chrome (Windows, Mac, Linux) since version 119
Inheritance	Locally applied ▼
Configuration	Enforce profile separation ▼ Controls whether a user is required to create a browser profile after signing in to the content area. This policy overrides the 'Separate profile for managed Google identity' policy.

Figure 11

Profile separation data migration = Let users decide whether to bring existing browsing data into their managed profile

Inheritance	Inherited from Google default
Configuration	Let users decide whether to bring existing browsing data into their managed profile ▼

Figure 12

End user experience: Local Profile to Work Profile

When a user signs into a Google service for the first time, the profile separation dialog will appear and the migration data box will be **unchecked**. If the user clicks on the continue button, a new profile is generated and their existing data remains in the initial profile they were in. If the users wants to migrate their browsing data to the new profile they will have to **manually check** the migration data box.

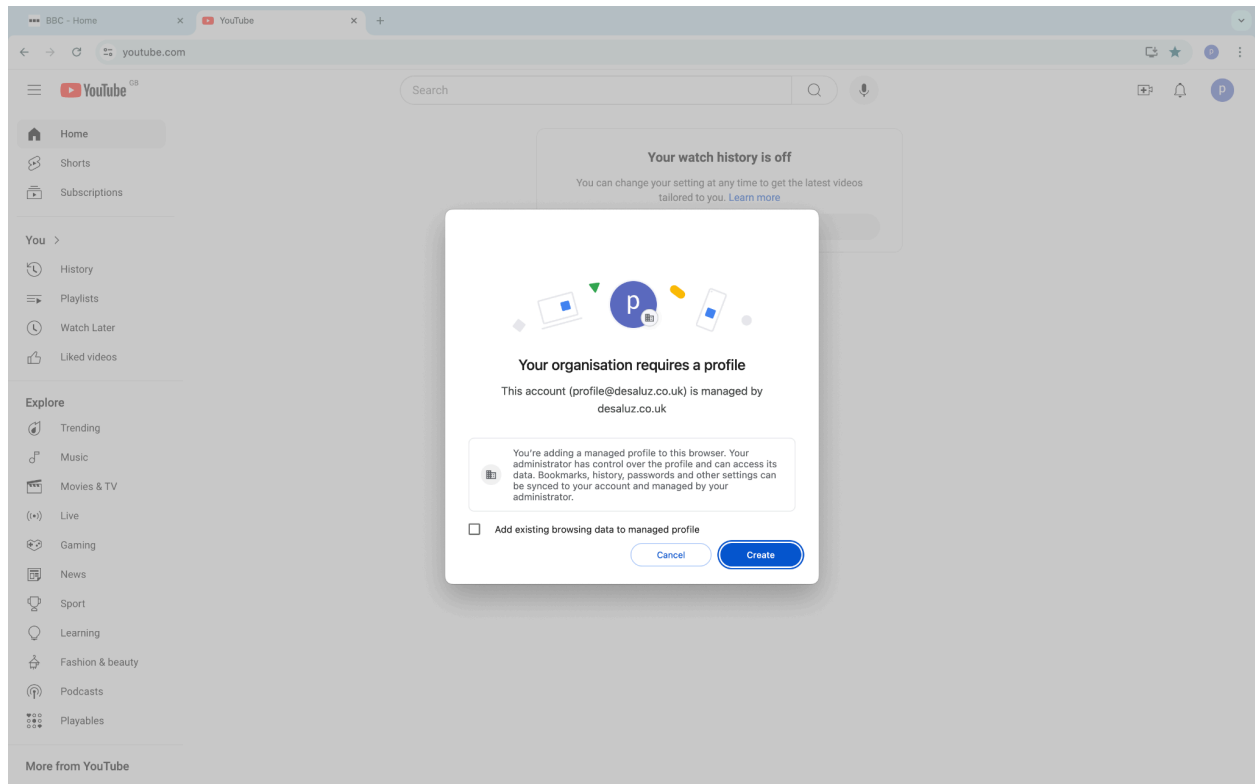


Figure 13

End user experience: Personal Profile to Work Profile

When a user is already signed into an existing account and attempts to add a work account, they will be required to create a new profile but they won't be able to migrate the data over to the new profile. This is because migration options are offered only when the user is signing in for the first time into the content area.

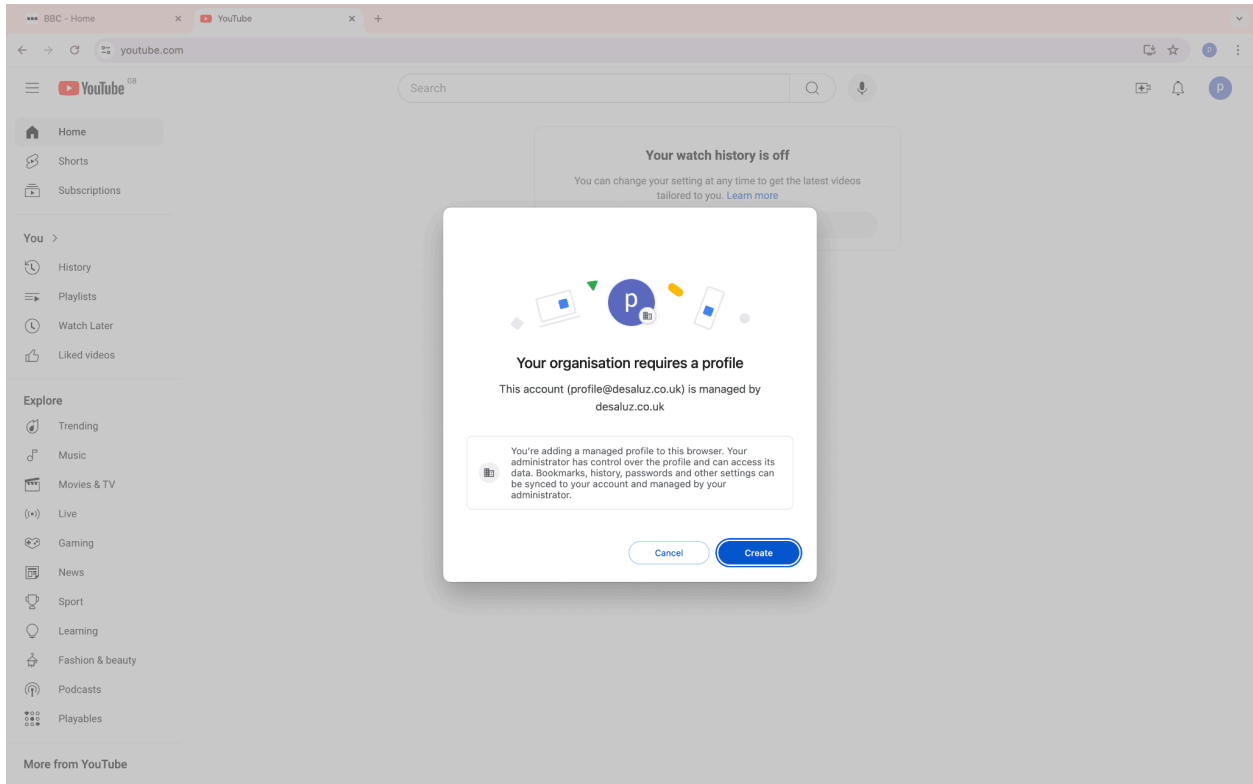


Figure 14

End user experience: Add profile

When signing into Chrome directly from the profile picker, users will not see data migration options. They will be prompted for their email address and password, followed by a profile creation notification.

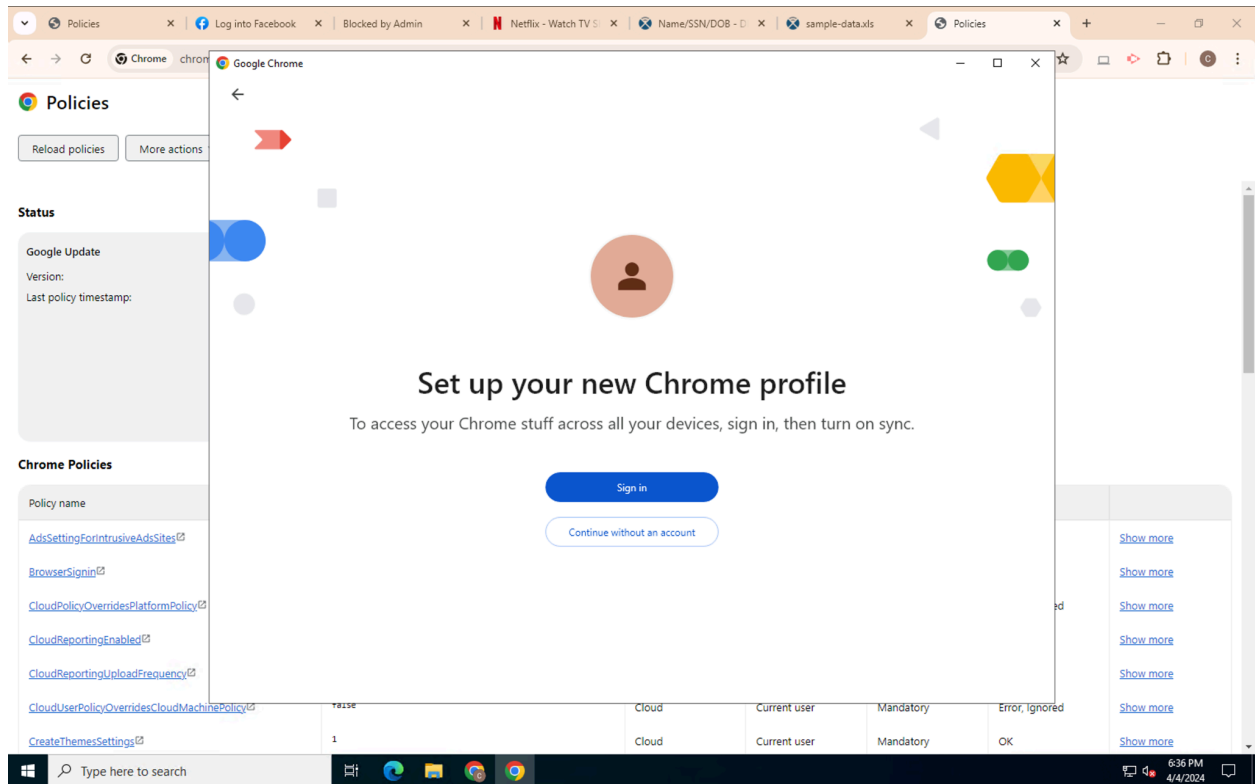


Figure 15

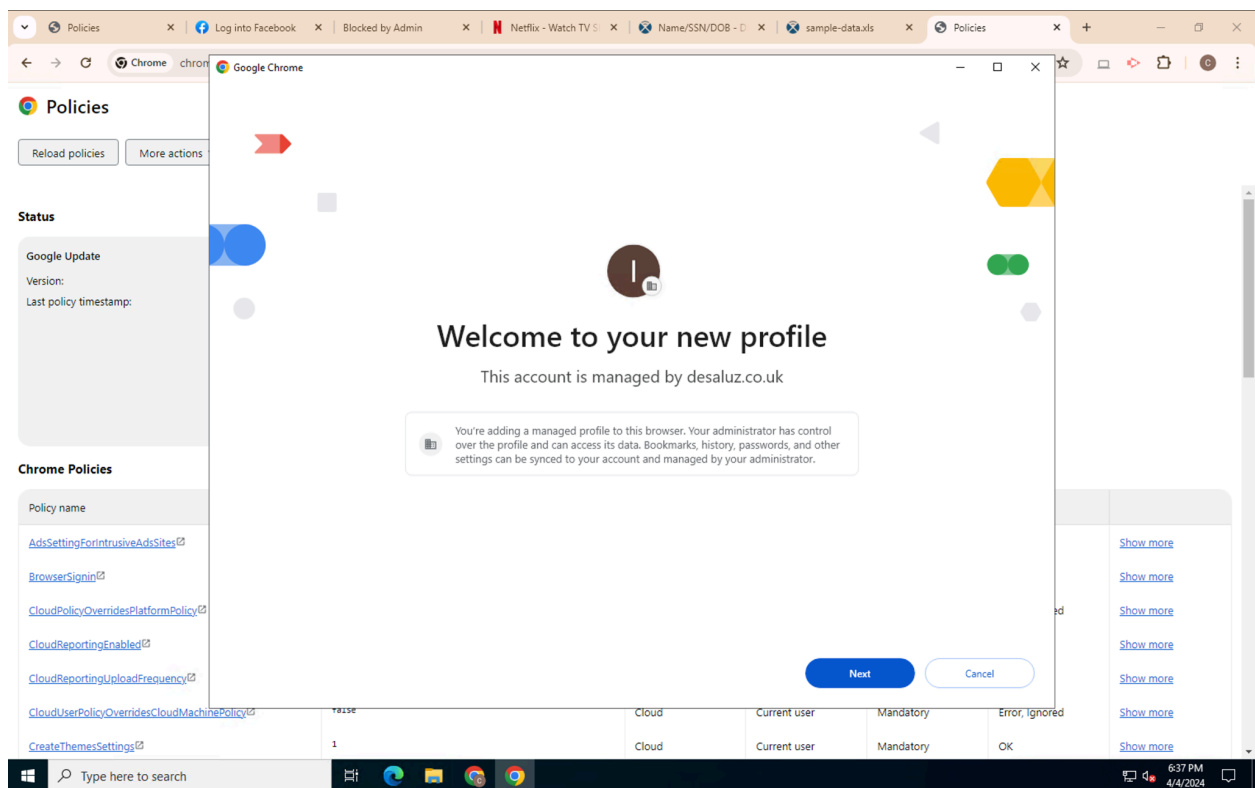


Figure 16

Scenario 1.3 [Example.com](#) wants to force end-users to sign-in to a separate work profile and prevent them from automatically importing browser data from their Local Profile.

Admin experience

In this case, you'll have to configure the [ProfileSeparationSettings](#) policy and the [ProfileSeparationDataMigrationSettings](#) policy as set below:

Enterprise profile separation = Enforce profile separation


Chromium name ProfileSeparationSettings 	Supported on Chrome (Windows, Mac, Linux) since version 119
Inheritance	Locally applied ▼
Configuration	Enforce profile separation ▼ Controls whether a user is required to create a browser profile after signing in to the content area. This policy overrides the 'Separate profile for managed Google identity' policy.

Figure 17

Profile separation data migration = Users cannot bring existing browsing data in their managed profile

Inheritance	Locally applied ▼
Configuration	Users cannot bring existing browsing data in their managed profile ▼

Figure 18

End user experience: Local Profile to Work Profile

When a user signs into a Google service for the first time, the profile separation dialog will appear and the user will **not** be able to keep local browsing data. Their existing data will remain in the initial profile they were in.

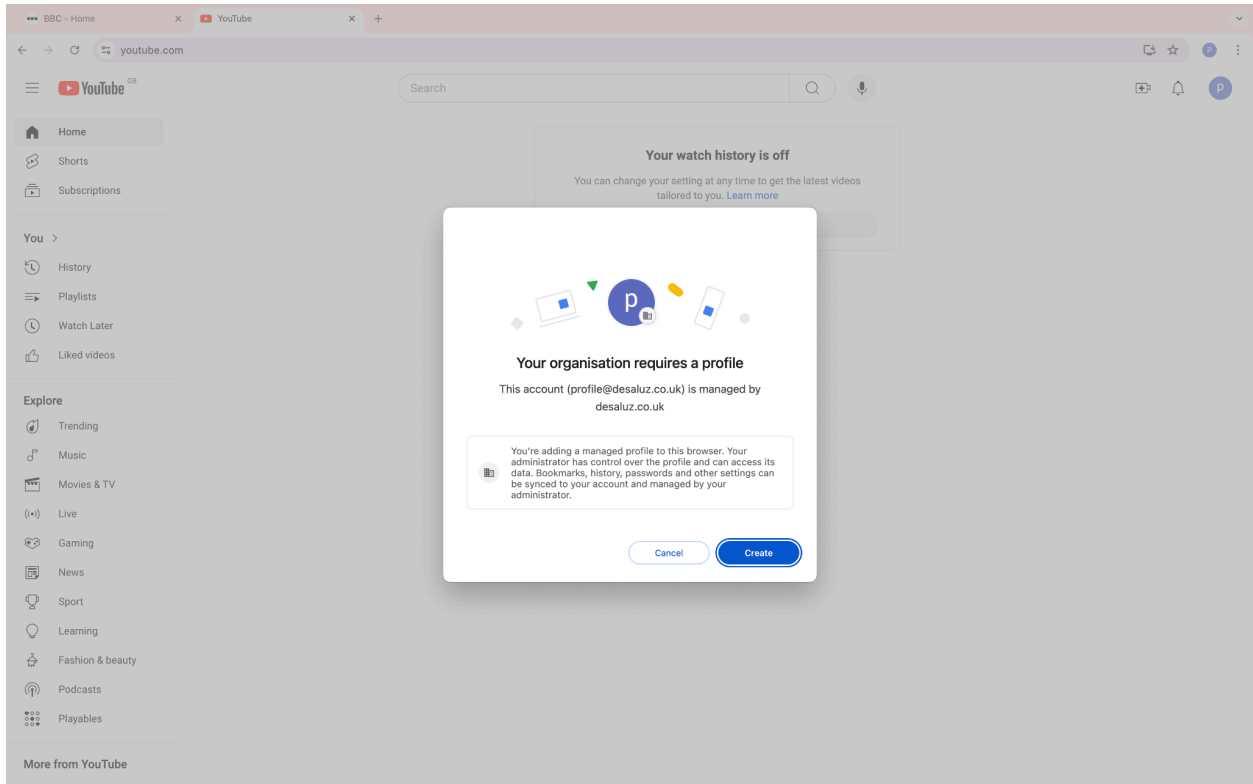


Figure 19

End user experience: Personal Profile to Work Profile

When a user signs into a Google service for the first time, the profile separation dialog will appear and the user will **not** be able to keep local browsing data. Their existing data will remain in the initial profile they were in.

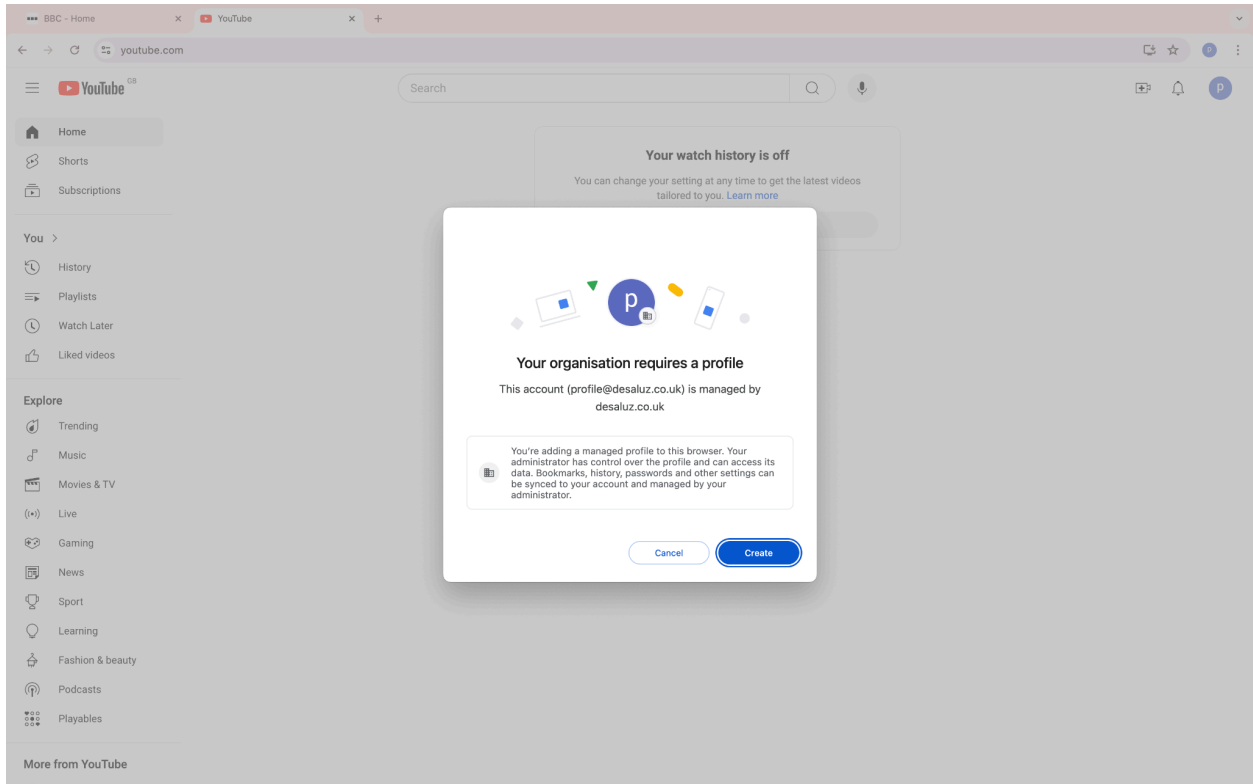


Figure 19

End user experience: Add profile

When signing into Chrome directly from the profile picker, users will not see data migration options. They will be prompted for their email address and password, followed by a profile creation notification.

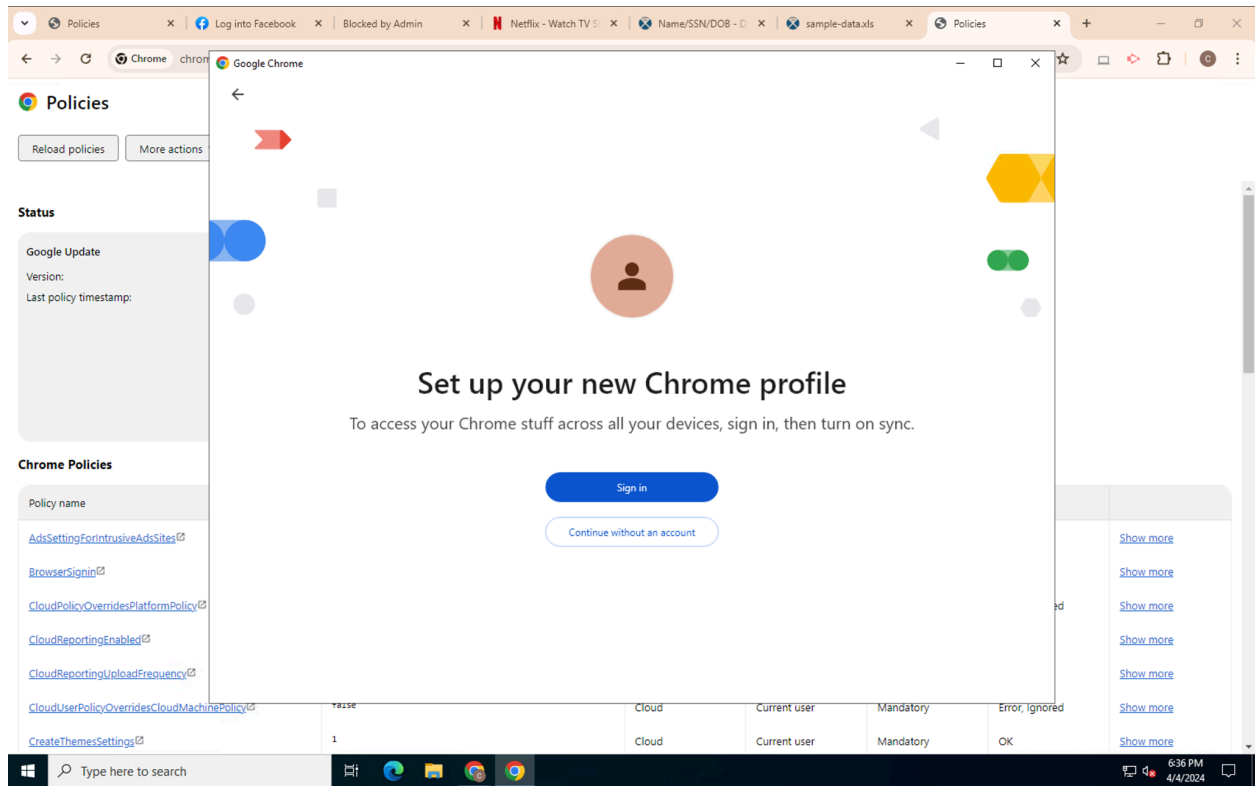


Figure 21

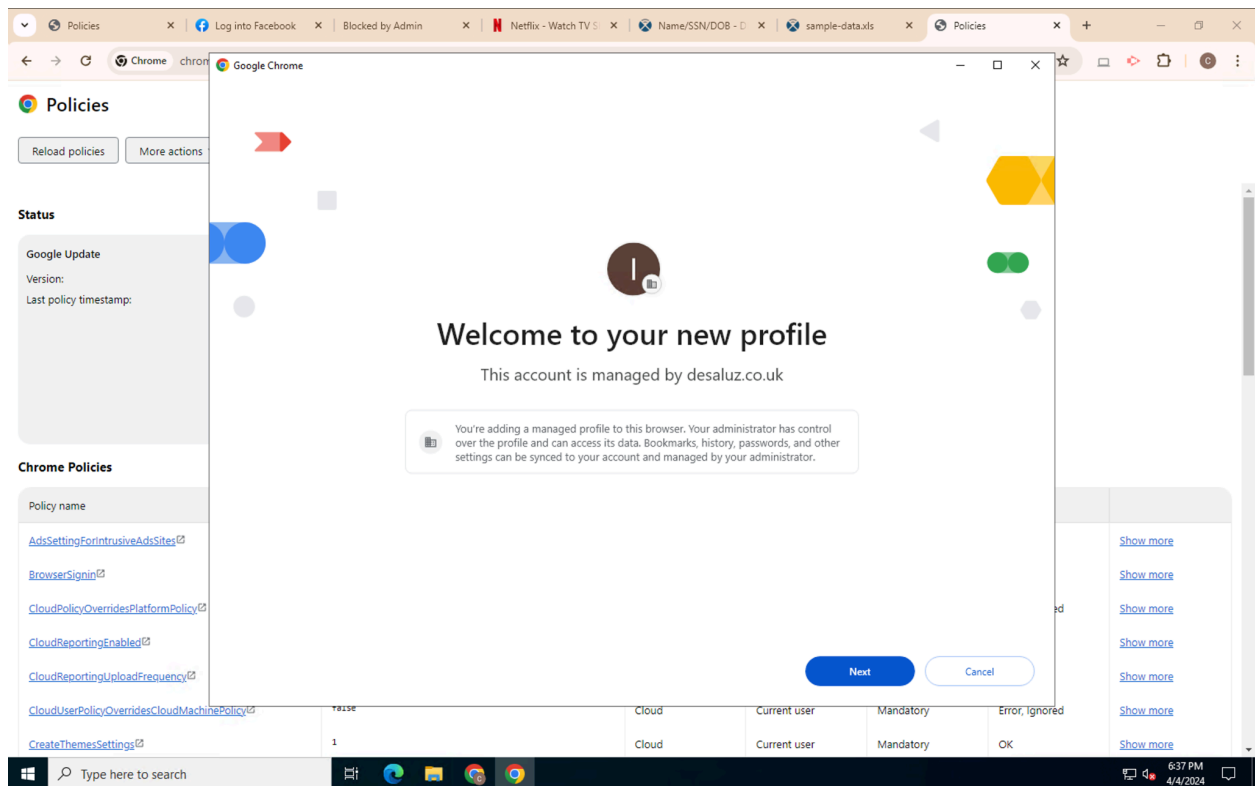


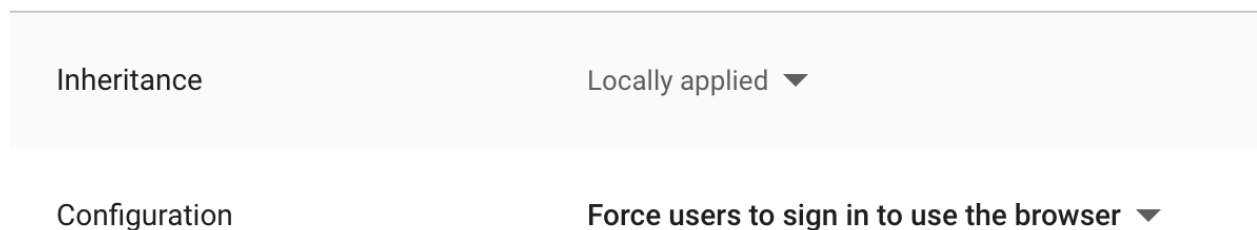
Figure 22

Scenario 2. Example.com wants to force end-users to sign-in to Chrome with their work account. Non [example.com](#) accounts are blocked from signing-in.

Admin experience

In this case, you'll have to configure the [BrowserSignin](#) policy, the [RestrictSigninToPattern](#) policy and [AllowedDomainsForApps](#) policy as set below:

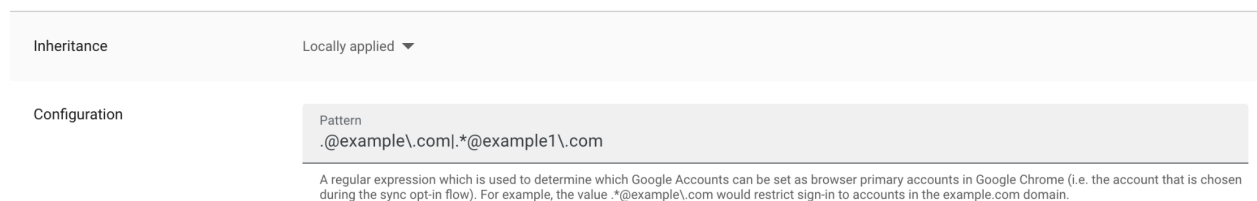
Browser Sign-in settings = Force users to sign in to use the browser



The screenshot shows the 'Browser Sign-in settings' policy configuration in the Google Admin console. The 'Inheritance' section shows 'Locally applied'. The 'Configuration' section shows the policy is set to 'Force users to sign in to use the browser'.

Figure 23

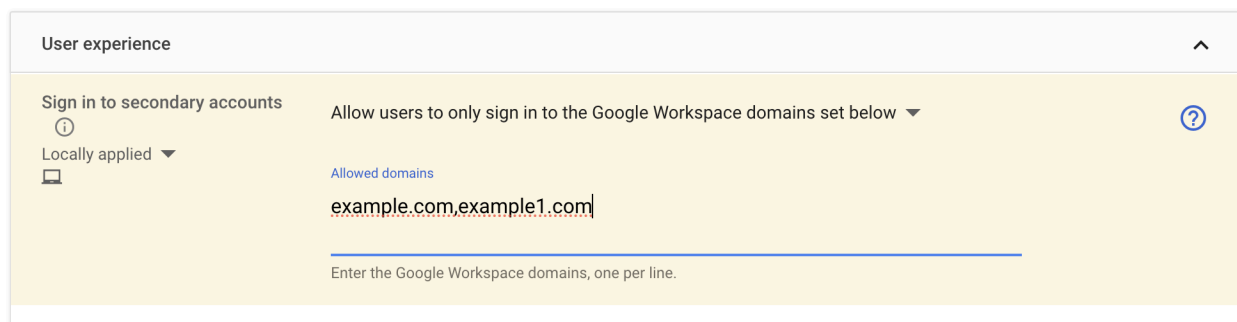
Restrict Sign-in To Pattern = Sign-in pattern. **Sample Values** = [.example.com](#) | [.example1.com](#)



The screenshot shows the 'Restrict Sign-in To Pattern' policy configuration in the Google Admin console. The 'Inheritance' section shows 'Locally applied'. The 'Configuration' section shows the 'Pattern' is set to `.example.com|.example1.com`. A note below the pattern field states: 'A regular expression which is used to determine which Google Accounts can be set as browser primary accounts in Google Chrome (i.e. the account that is chosen during the sync opt-in flow). For example, the value .example.com would restrict sign-in to accounts in the example.com domain.'

Figure 24

Sign in to secondary accounts = Allow users to only sign in to the Google Workspace domains set below. **Sample Values** = [example.com](#), [example1.com](#)



The screenshot shows the 'Sign in to secondary accounts' policy configuration in the Google Admin console. The 'Inheritance' section shows 'Locally applied'. The 'Configuration' section shows the policy is set to 'Allow users to only sign in to the Google Workspace domains set below'. The 'Allowed domains' field contains the text `example.com,example1.com`. A note below the field states: 'Enter the Google Workspace domains, one per line.'

Figure 25

Note 6: Changes to the [BrowserSignin](#) policy require a Chrome restart to take effect.

Note 7: When the [RestrictSigninToPattern](#) and [AllowedDomainsForApps](#) policies are configured, your end-users are blocked from sign-in into a Google service with an account that doesn't match the Sign-in pattern.

End user experience:

If the [BrowserSignin](#) policy is set to 'force' while a user is actively using Chrome, the change will not take effect immediately. The user must restart Chrome for the policy to be enforced. Upon restart, they will be required to sign in. Any existing profiles used without signing in will become locked.

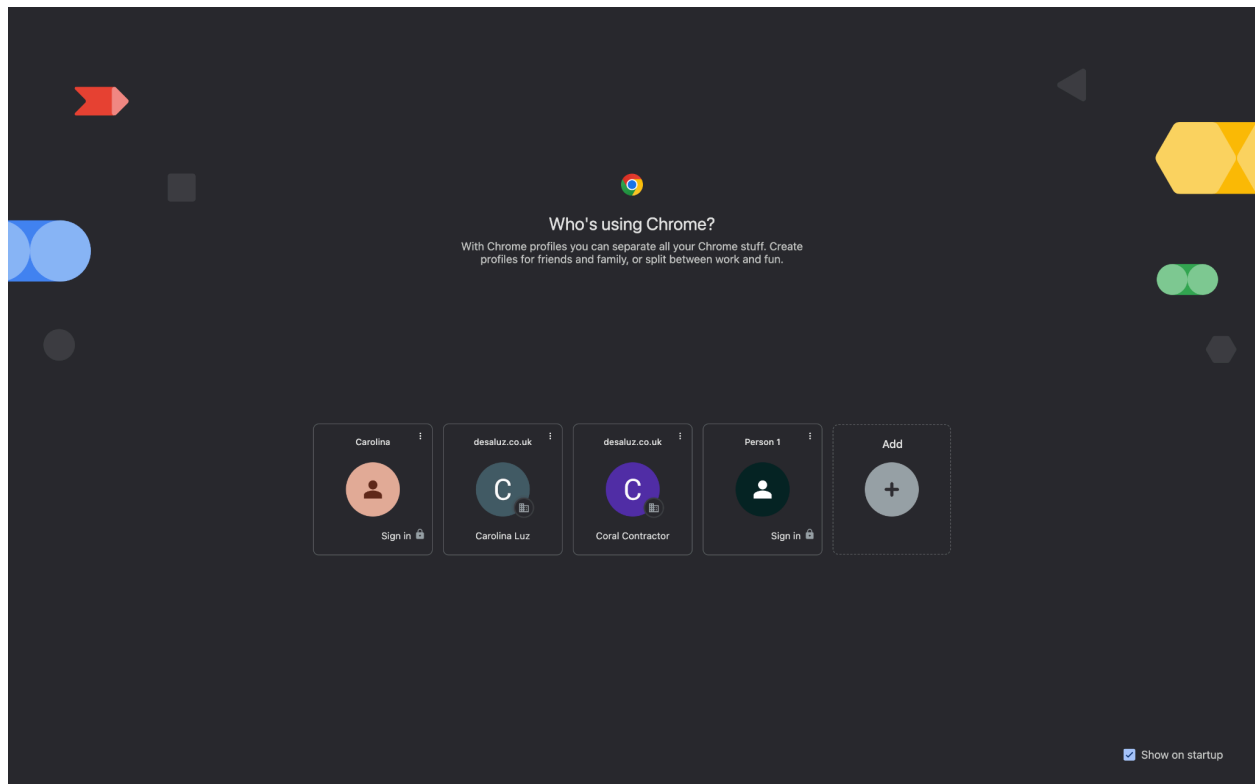


Figure 26

Note 8: The data associated to the locked profiles is not lost and can be accessed locally if needed.

If the [BrowserSignin](#) policy is set to 'force' while Chrome is closed, the change will not take effect immediately.

To continue using Chrome, the user will need to create a new profile by signing in.

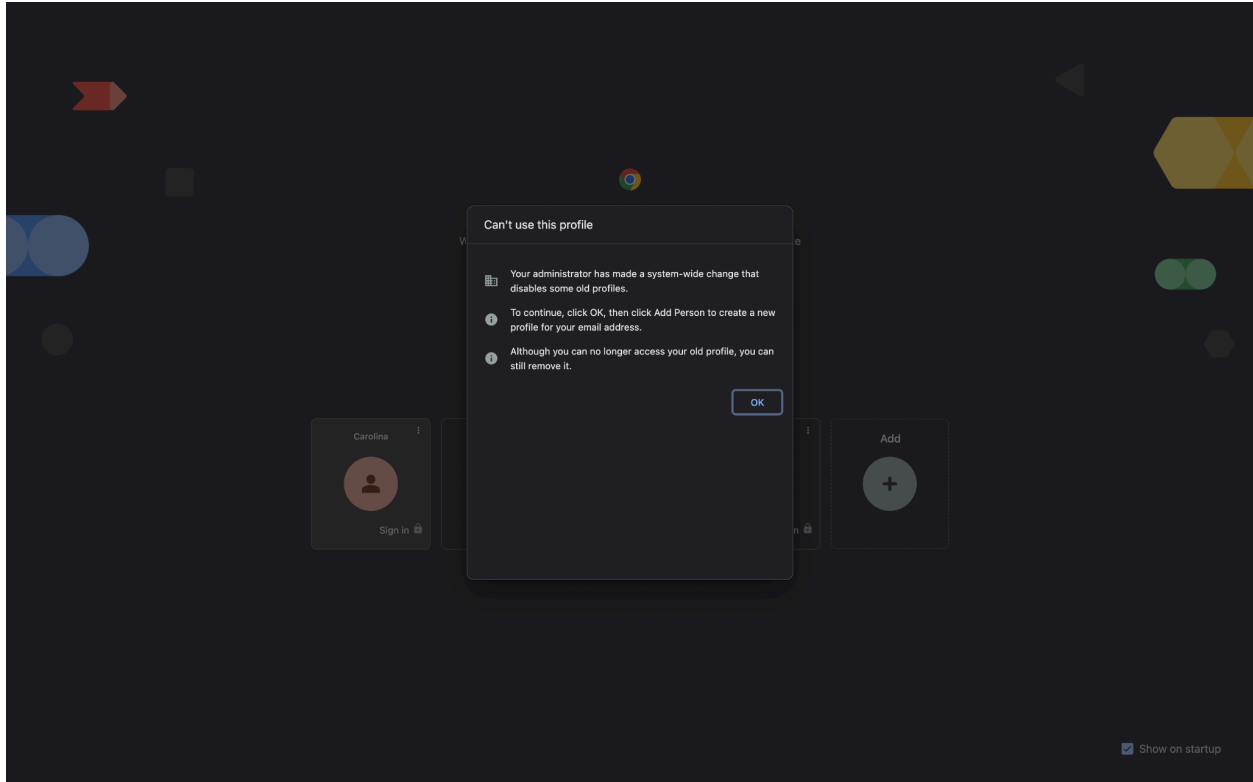


Figure 27

The user will only be able to sign in the profile with an account from a domain specified on the [RestrictSigninToPattern](#) and [AllowedDomainsForApps](#) policies. If the user tries to sign in the profile with an account from a domain that is not specified on the [RestrictSigninToPattern](#) and [AllowedDomainsForApps](#) policies the user will get the error message below.

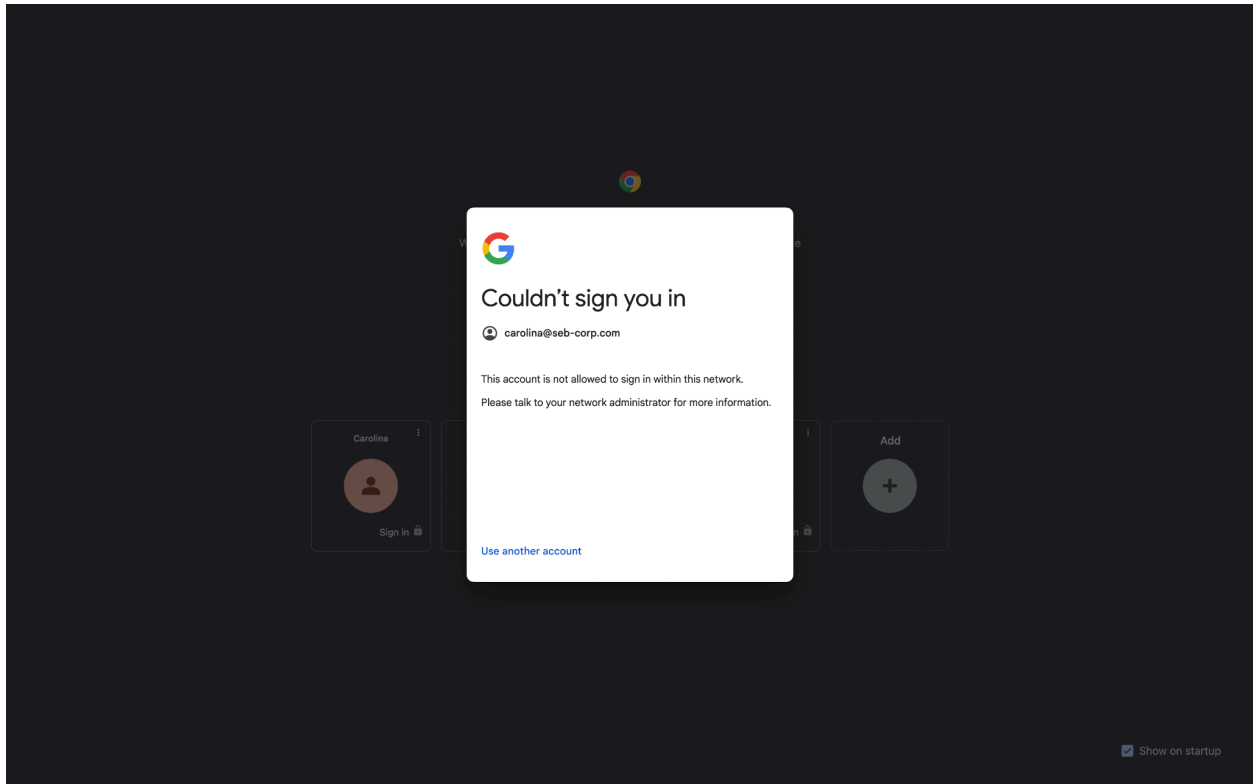


Figure 28

Scenario 2.1 [Example.com](#) wants to force end-users to sign-in to a separate work profile and suggest that they automatically import browser data from their Local Profile.

Admin experience

In this case, you'll have to configure the [ProfileSeparationSettings](#) policy and the [ProfileSeparationDataMigrationSettings](#) policy as set below:

Enterprise profile separation = Enforce profile separation


Chromium name ProfileSeparationSettings 	Supported on Chrome (Windows, Mac, Linux) since version 119
Inheritance	Locally applied ▼
Configuration	Enforce profile separation ▼ Controls whether a user is required to create a browser profile after signing in to the content area. This policy overrides the 'Separate profile for managed Google identity' policy.

Figure 29

Profile separation data migration = Suggest to users to bring their existing data in the managed profile and give them a choice not to

Chromium name ProfileSeparationDataMigrationSetti...	Supported on Chrome (Windows, Mac, Linux) since version 119
Inheritance	Locally applied ▼
Configuration	Suggest to users to bring their existing data in the managed profile and give them a choice not to ▼

Figure 30

End user experience: Local Profile to Work Profile

When a user signs into a Google service for the first time, the profile separation dialog will appear and the migration data box will be **checked**. If the user clicks on the continue a new profile is generated with the user's browsing data.

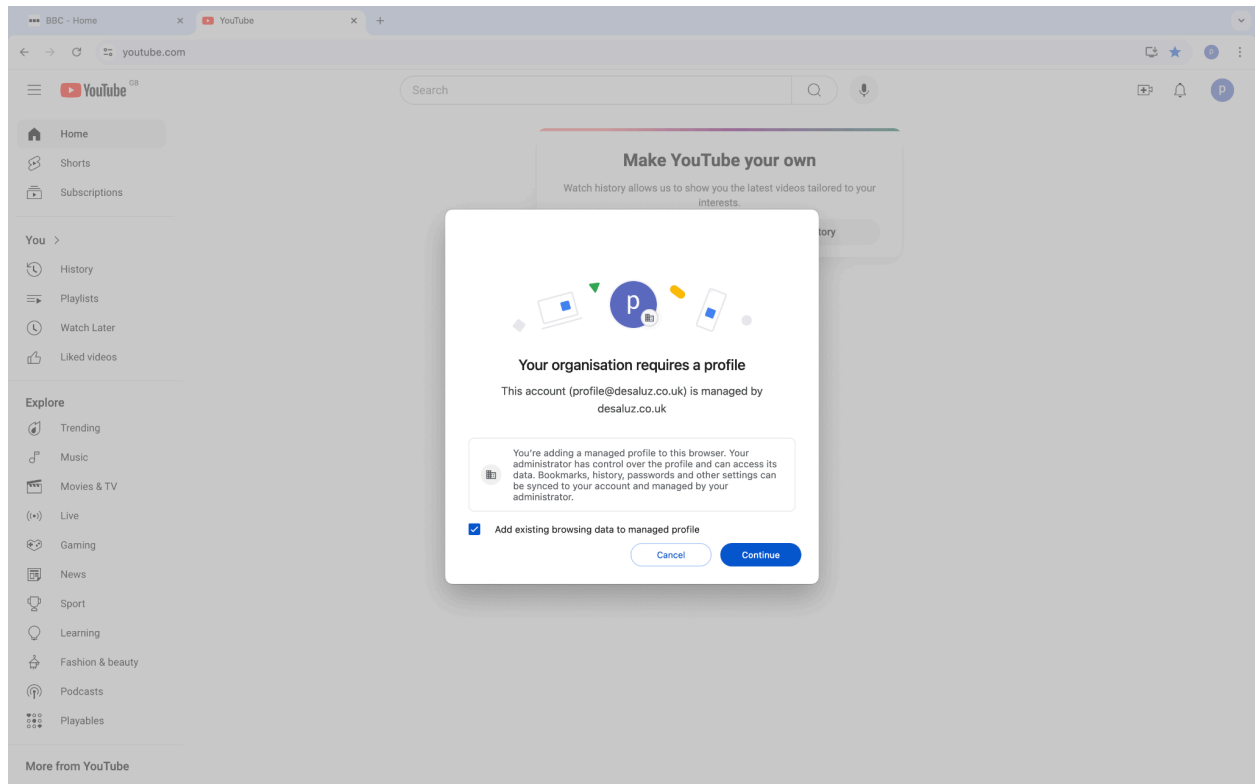


Figure 31

End user experience: Personal Profile to Work Profile

When a user is already signed into an existing account and attempts to add a work account, they will be required to create a new profile but they won't be able to migrate the data over to the new profile. This is because migration options are offered only when the user is signing in for the first time into the content area.

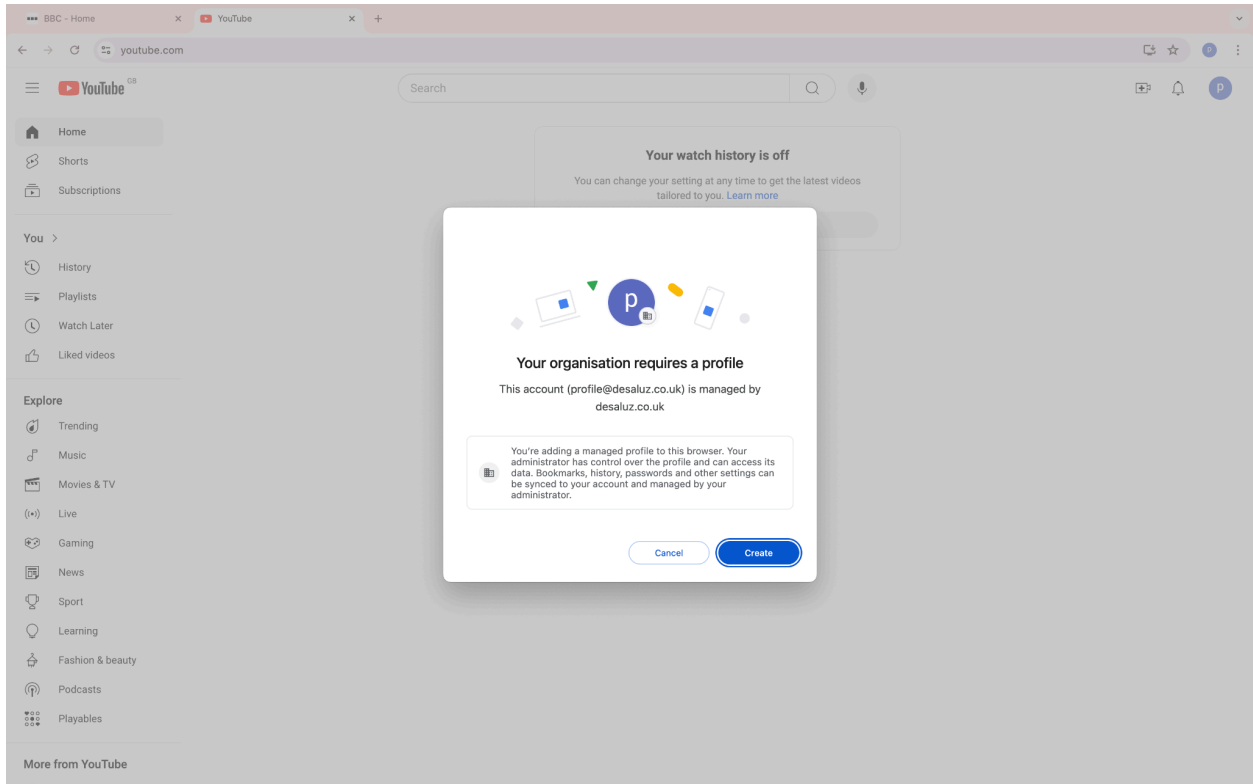


Figure 32

End user experience: Add profile

When signing into Chrome directly from the profile picker, users will not see data migration options. They will be prompted for their email address and password, followed by a profile creation notification.

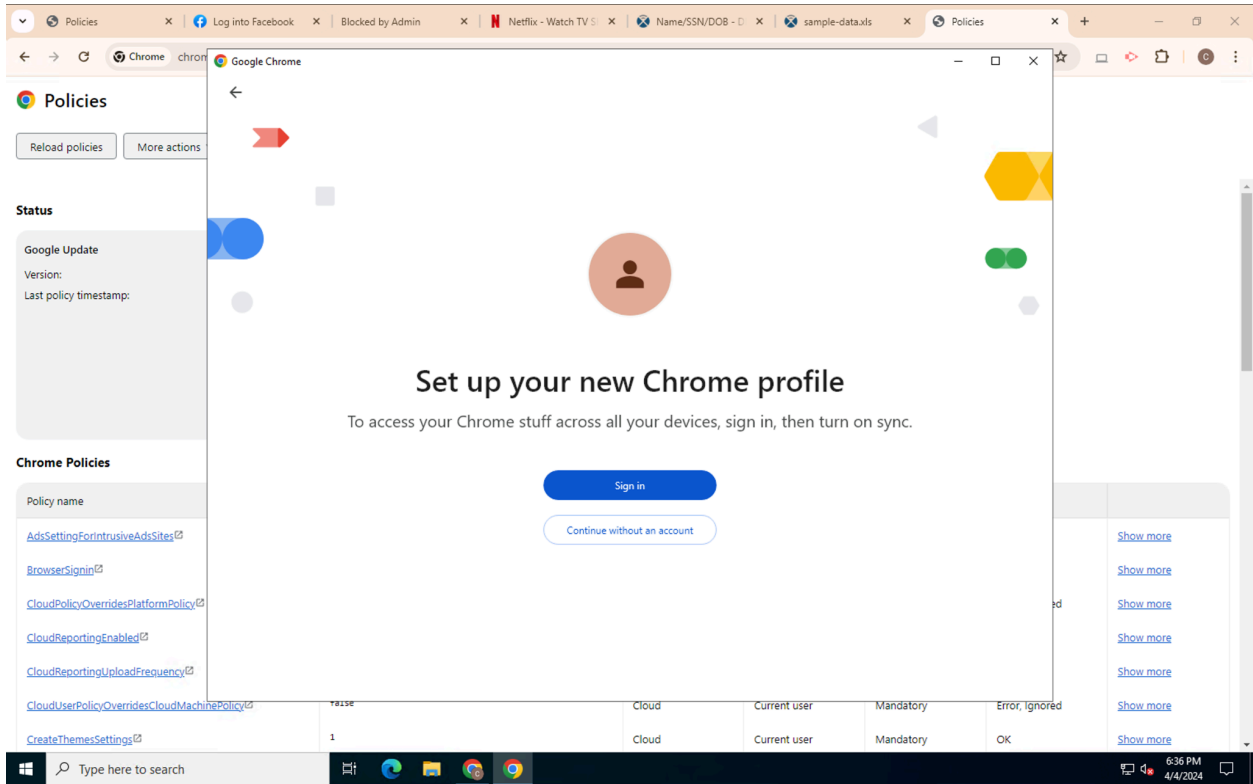


Figure 33

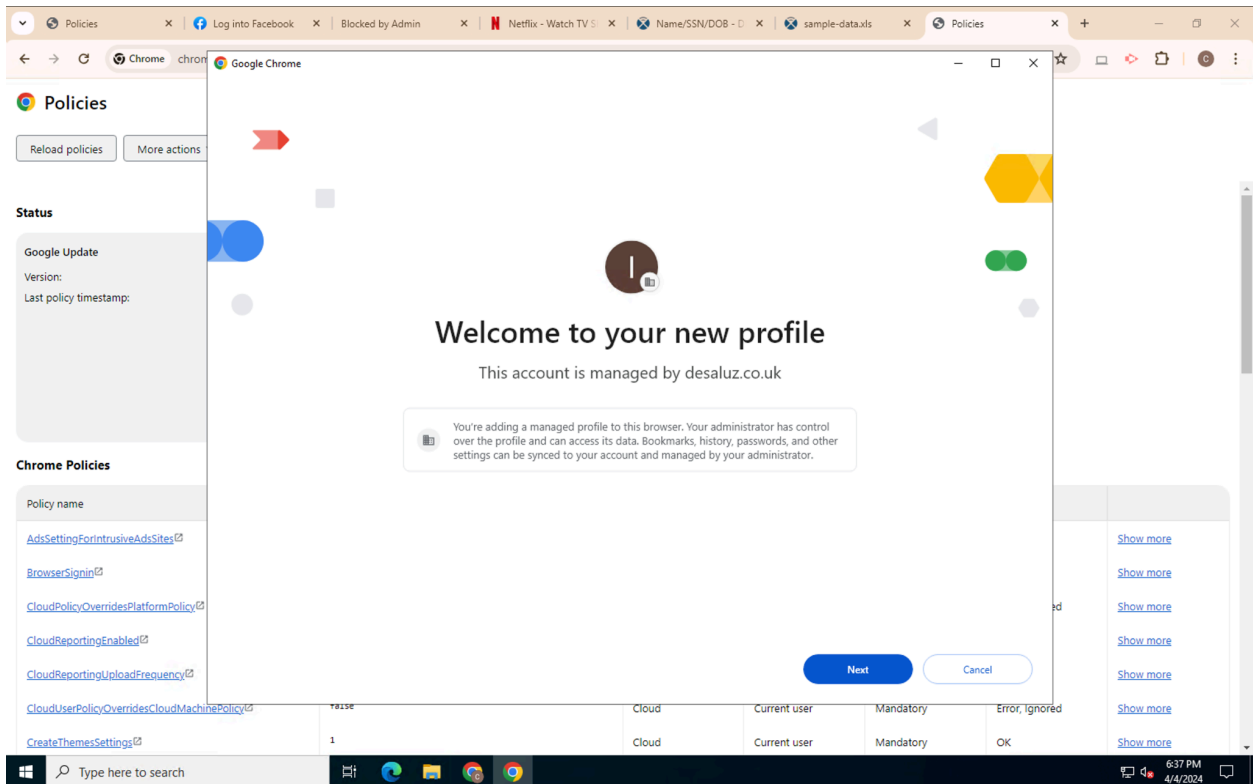


Figure 34

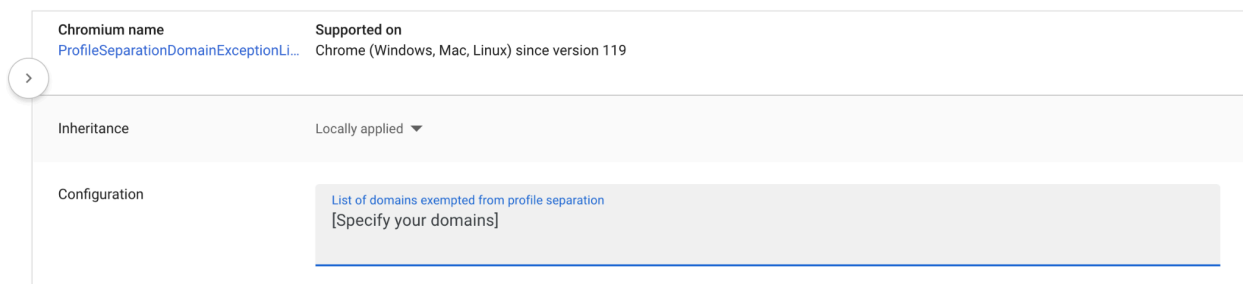
Scenario 2.1.1 [Example.com](#) wants to allow specific domains to coexist in the same work profile

It is common for organizations to own multiple work domains, especially as a result of mergers or acquisitions. Consequently, users may have multiple work accounts that they use to sign in to Google services. To streamline the user experience, organizations may want to exempt users from having to create a new profile every time they sign in to Google services with a different work account.

Admin experience

In this case, you'll have to configure the [ProfileSeparationDomainExceptionList](#) policy as set below:

Profile separation exemptions = [Specify your domains]



The screenshot shows the configuration page for the `ProfileSeparationDomainExceptionList` policy in the Google Admin console. The page has a left sidebar with a navigation menu containing 'Chromium name', 'Supported on', 'Inheritance', and 'Configuration'. The main content area is divided into sections corresponding to these menu items. The 'Supported on' section indicates the policy is supported on Chrome (Windows, Mac, Linux) since version 119. The 'Inheritance' section shows the policy is 'Locally applied'. The 'Configuration' section contains a text input field with the placeholder text 'List of domains exempted from profile separation' and '[Specify your domains]'. A blue underline is visible at the bottom of the configuration field.

Figure 35

End user experience: Sign-in with an account from a domain on the `ProfileSeparationDomainExceptionList` Policy

If a user attempts to sign into a Google service within a work profile using an account whose domain is specified in the [ProfileSeparationDomainExceptionList](#) policy, they will not be prompted to create a new profile. They will however get a suggestion to create a profile, but they can choose not to.

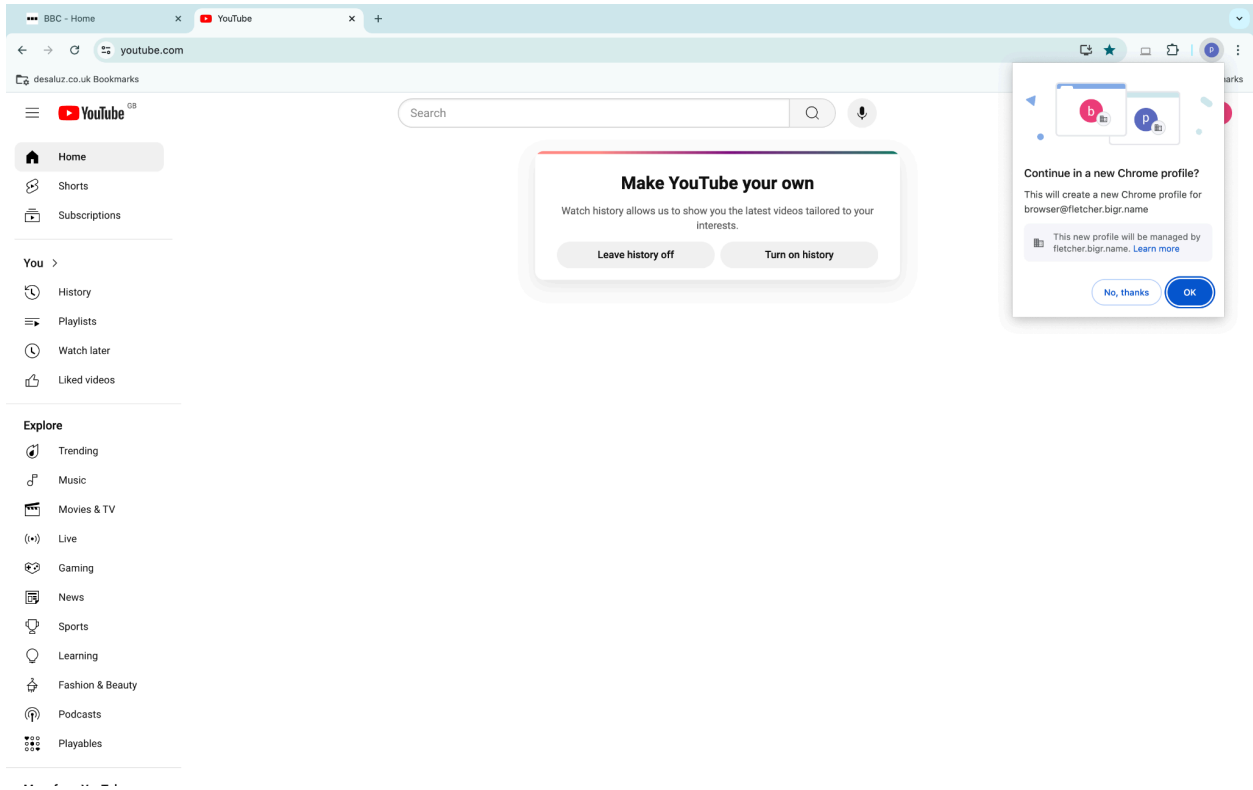


Figure 36

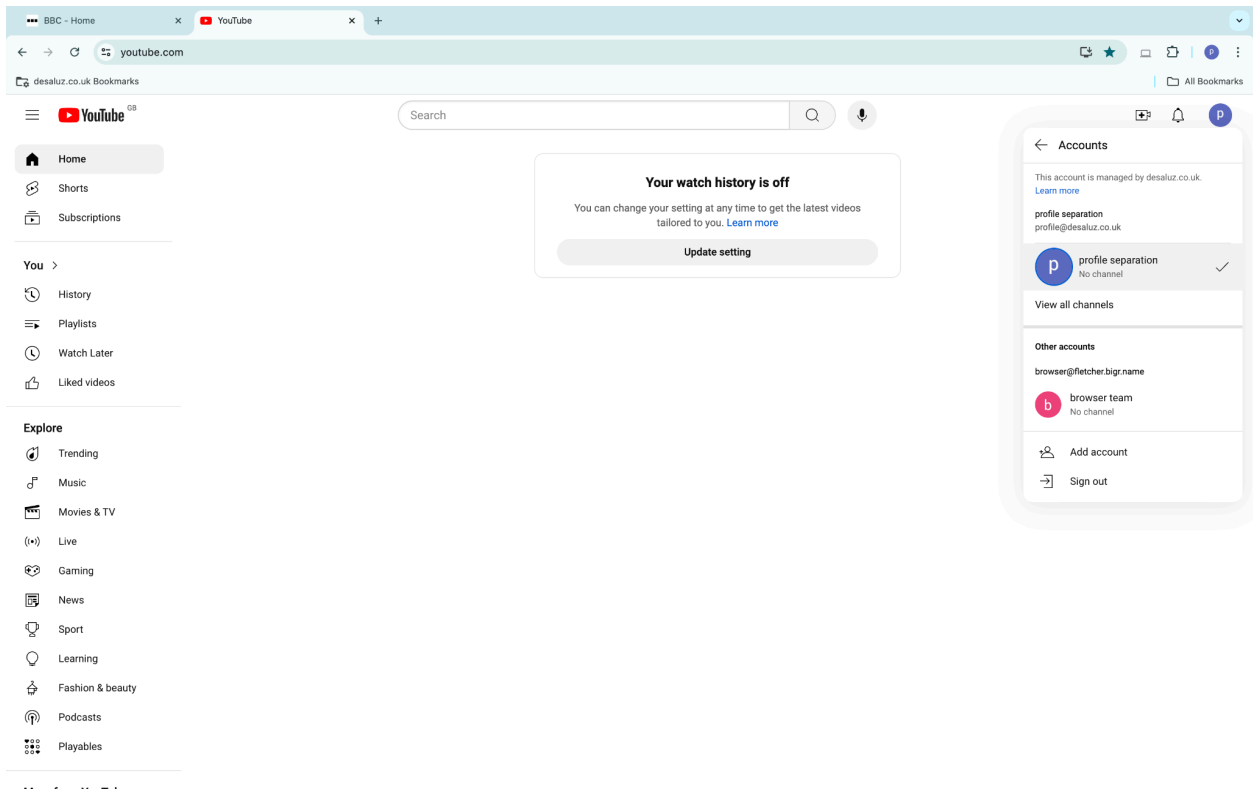


Figure 37

End user experience: Sign-in with an account from a domain not on the ProfileSeparationDomainExceptionList Policy

If a user attempts to sign into a Google service within a work profile using an account whose domain is not specified in the [ProfileSeparationDomainExceptionList](#) policy, a new profile will be created.

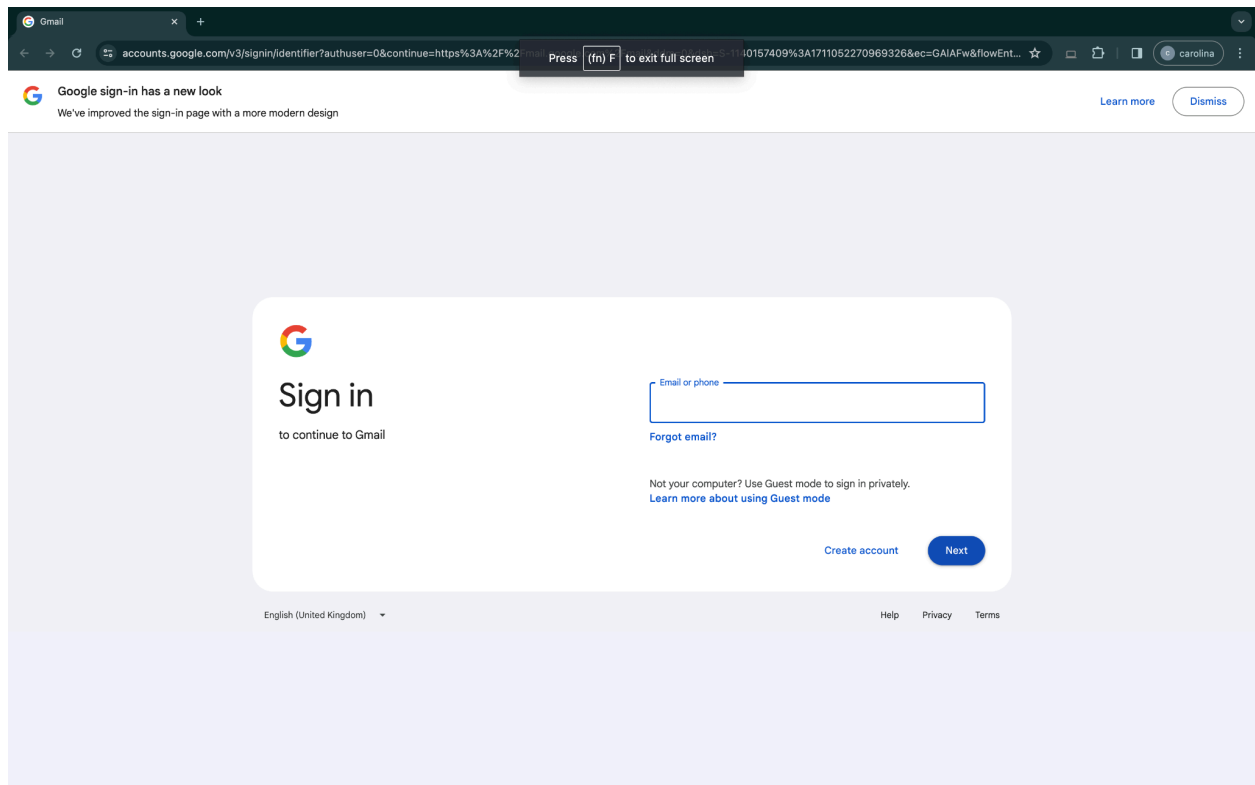


Figure 38

Note 4: If the account the user attempts to sign into a Google service within a work profile is targeted by the ProfileSeparationSettings policy and the policy is enforcing profile separation, the user will be forced to create a new profile. This behavior occurs even if the domain is specified in the ProfileSeparationDomainExceptionList policy.

Scenario 2.2 [Example.com](#) wants to force end-users to sign-in to a separate work profile and allow them to automatically import browser data from their Local Profile.

Admin experience

In this case, you'll have to configure the [ProfileSeparationSettings](#) policy and the [ProfileSeparationDataMigrationSettings](#) policy as set below:

Enterprise profile separation = Enforce profile separation


Chromium name	Supported on
ProfileSeparationSettings 	Chrome (Windows, Mac, Linux) since version 119
Inheritance	Locally applied ▼
Configuration	Enforce profile separation ▼ Controls whether a user is required to create a browser profile after signing in to the content area. This policy overrides the 'Separate profile for managed Google identity' policy.

Figure 39

Profile separation data migration = Let users decide whether to bring existing browsing data into their managed profile

Inheritance	Inherited from Google default
Configuration	Let users decide whether to bring existing browsing data into their managed profile ▼

Figure 40

End user experience: Local Profile to Work Profile

When a user signs into a Google service for the first time, the profile separation dialog will appear and the migration data box will be **unchecked**. If the user clicks on the continue button, a new profile is generated and their existing data remains in the initial profile they were in. If the users wants to migrate their browsing data to the new profile they will have to manually check the migration data box.

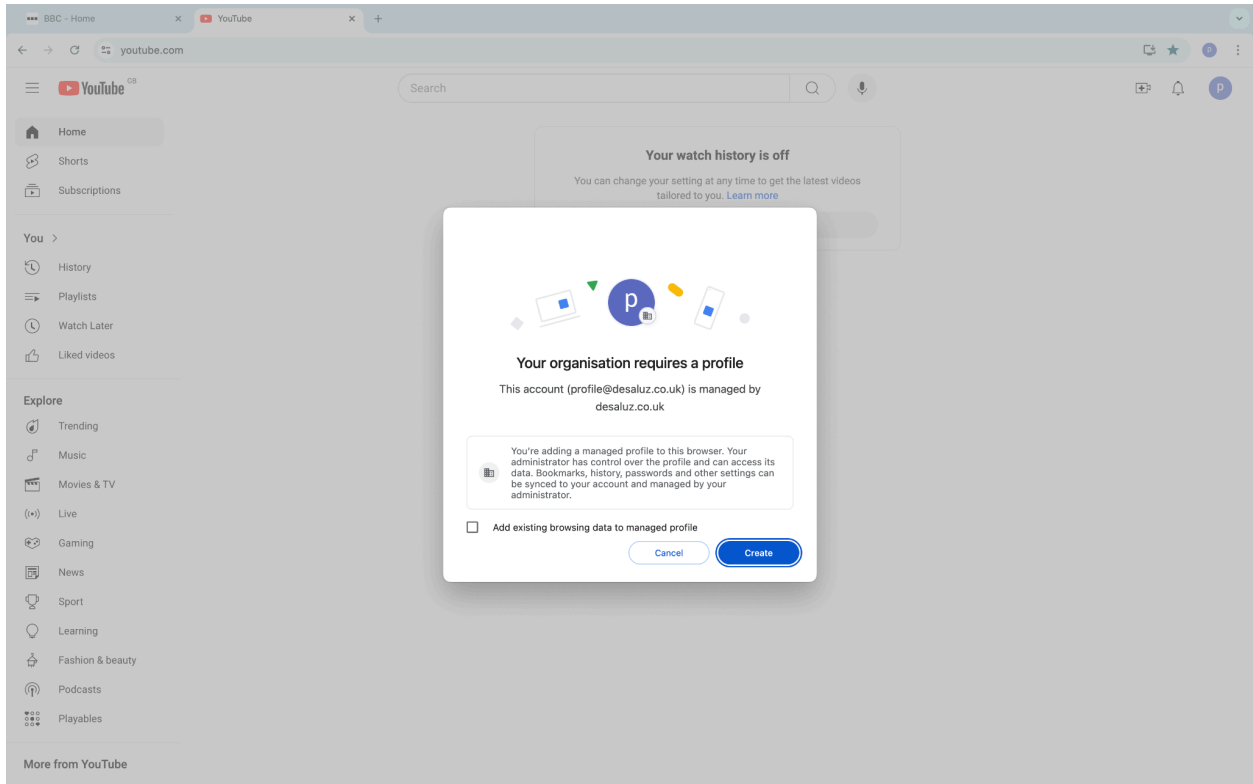


Figure 41

End user experience: Personal Profile to Work Profile

When a user is already signed into an existing account and attempts to add a work account, they will be required to create a new profile but they won't be able to migrate the data over to the new profile. This is because migration options are offered only when the user is signing in for the first time into the content area.

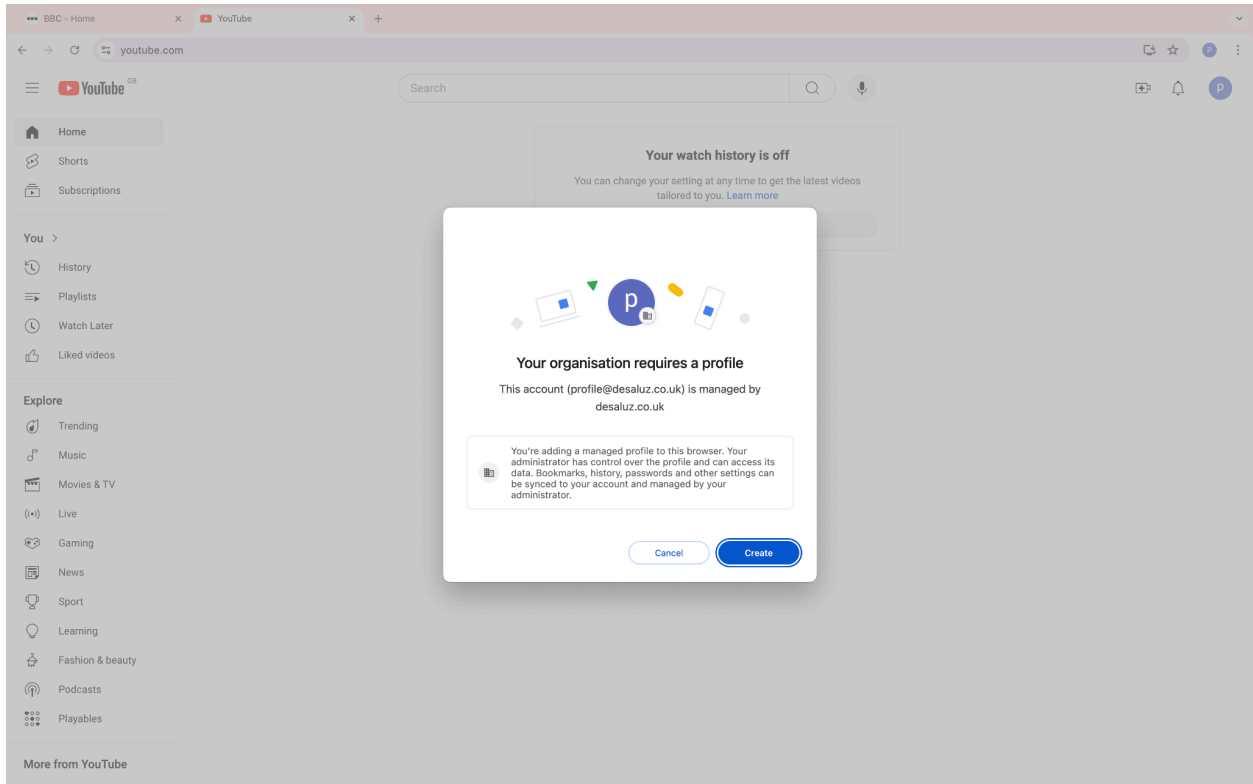


Figure 42

End user experience: Add profile

When signing into Chrome directly from the profile picker, users will not see data migration options. They will be prompted for their email address and password, followed by a profile creation notification.

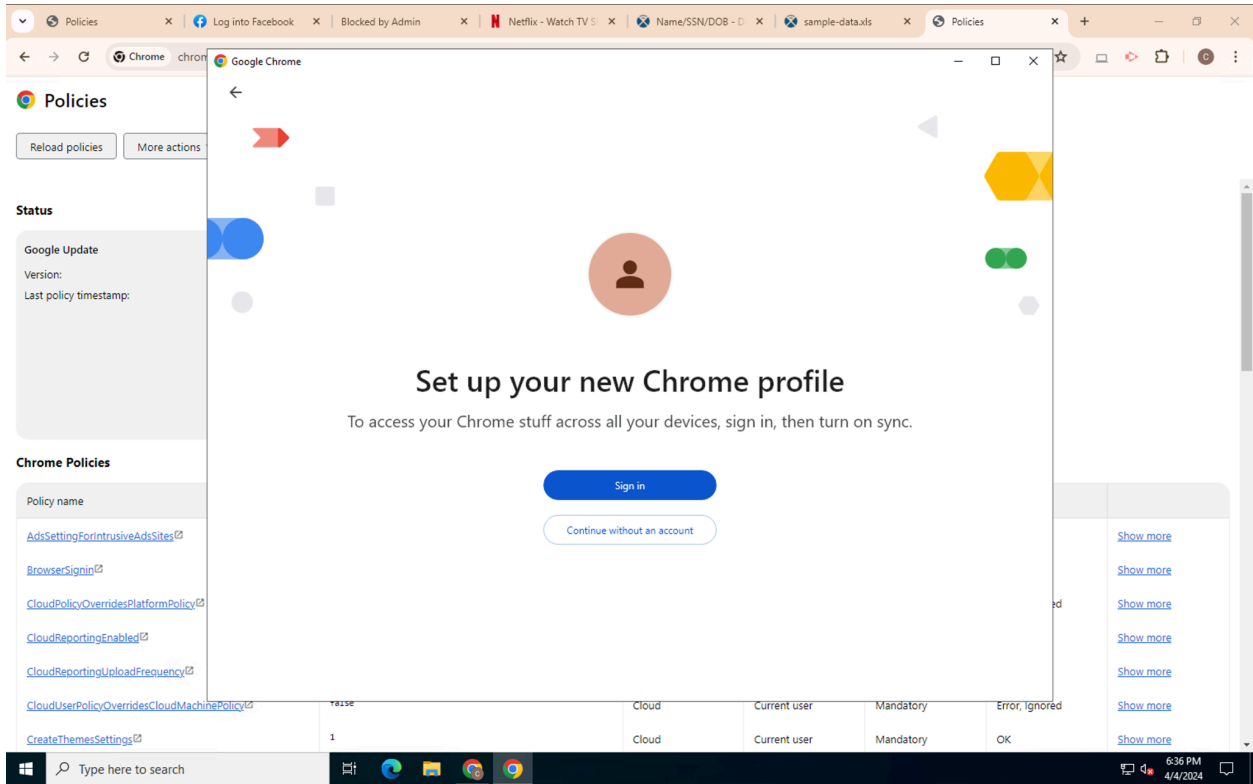


Figure 43

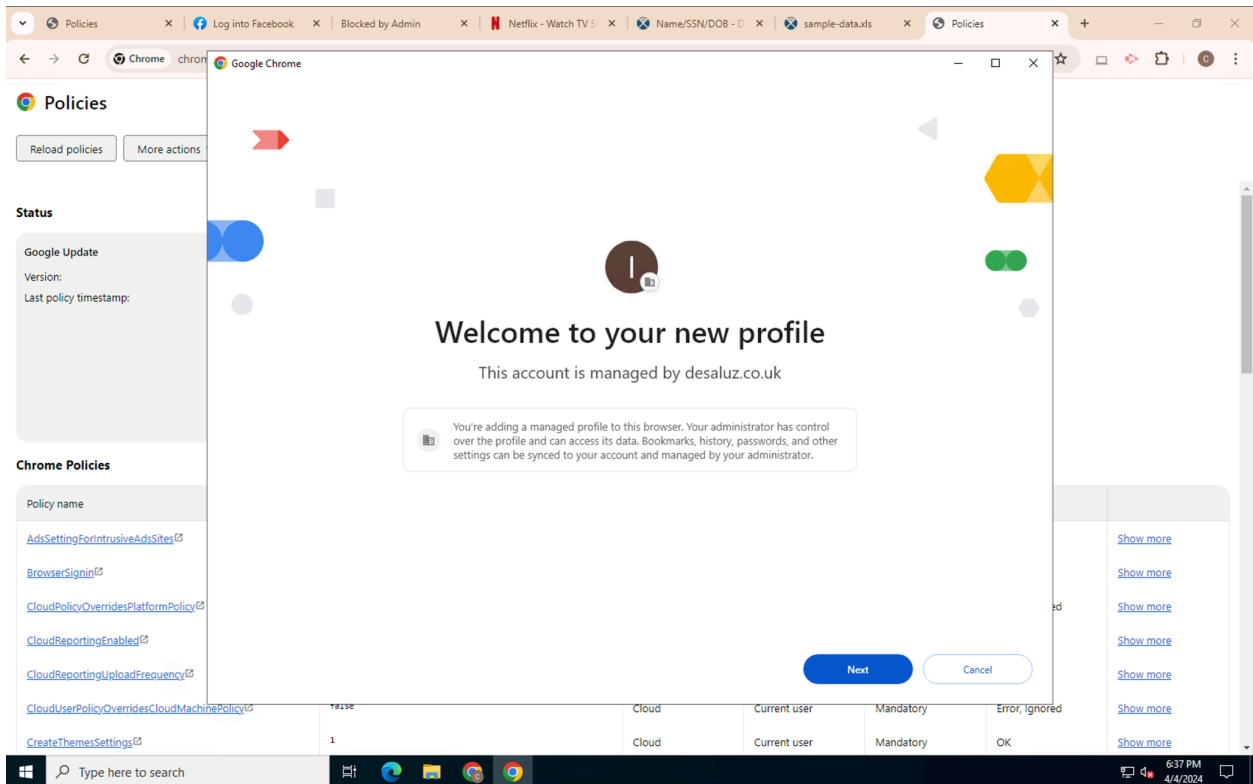


Figure 44

Scenario 2.3 [Example.com](#) wants to force end-users to sign-in to a separate work profile and prevent them from automatically importing browser data from their Local Profile.

Admin experience

In this case, you'll have to configure the [ProfileSeparationSettings](#) policy and the [ProfileSeparationDataMigrationSettings](#) policy as set below:

Enterprise profile separation = Enforce profile separation


Chromium name	Supported on
ProfileSeparationSettings 	Chrome (Windows, Mac, Linux) since version 119
Inheritance	Locally applied ▼
Configuration	Enforce profile separation ▼ Controls whether a user is required to create a browser profile after signing in to the content area. This policy overrides the 'Separate profile for managed Google identity' policy.

Figure 45

Profile separation data migration = Users cannot bring existing browsing data in their managed profile

Inheritance	Locally applied ▼
Configuration	Users cannot bring existing browsing data in their managed profile ▼

Figure 46

End user experience: Local Profile to Work Profile

When a user signs into a Google service for the first time, the profile separation dialog will appear and the user will not be able to keep local browsing data. Their existing data will remain in the initial profile they were in.

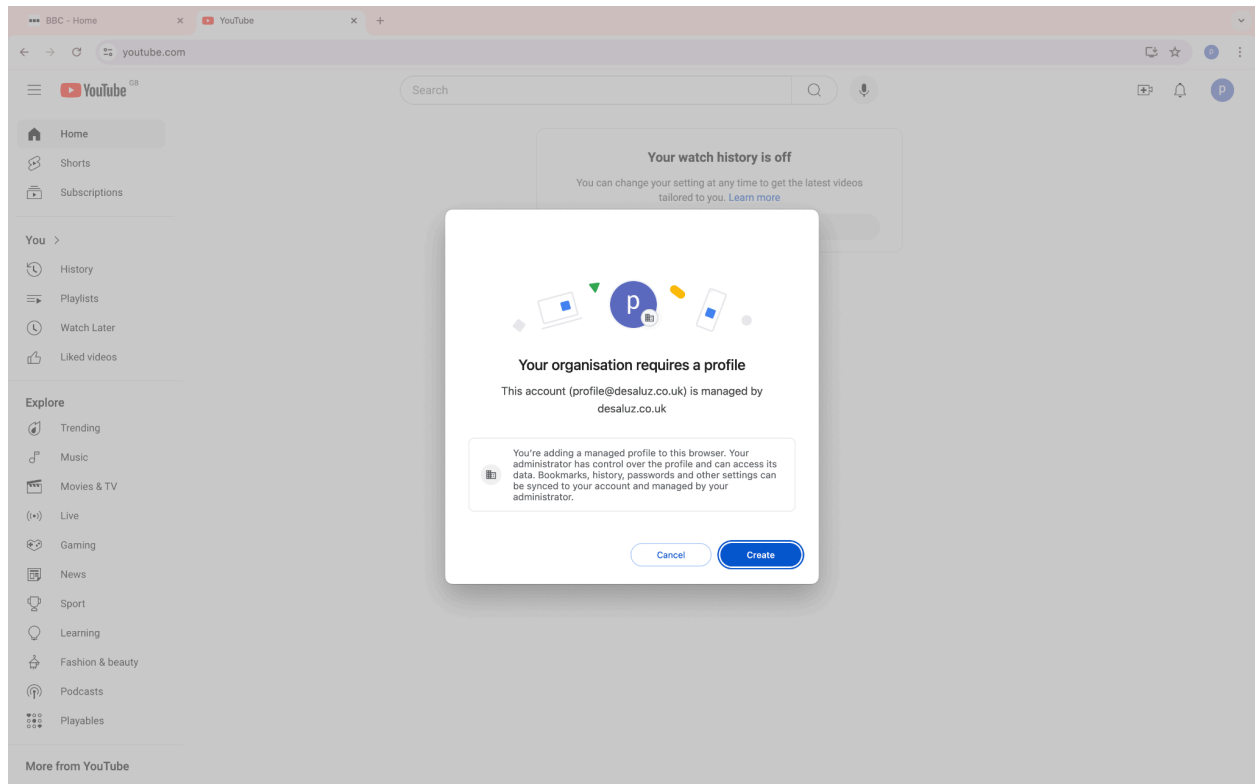


Figure 47

End user experience: Personal Profile to Work Profile

When a user signs into a Google service for the first time, the profile separation dialog will appear and the user will not be able to keep local browsing data. Their existing data will remain in the initial profile they were in.

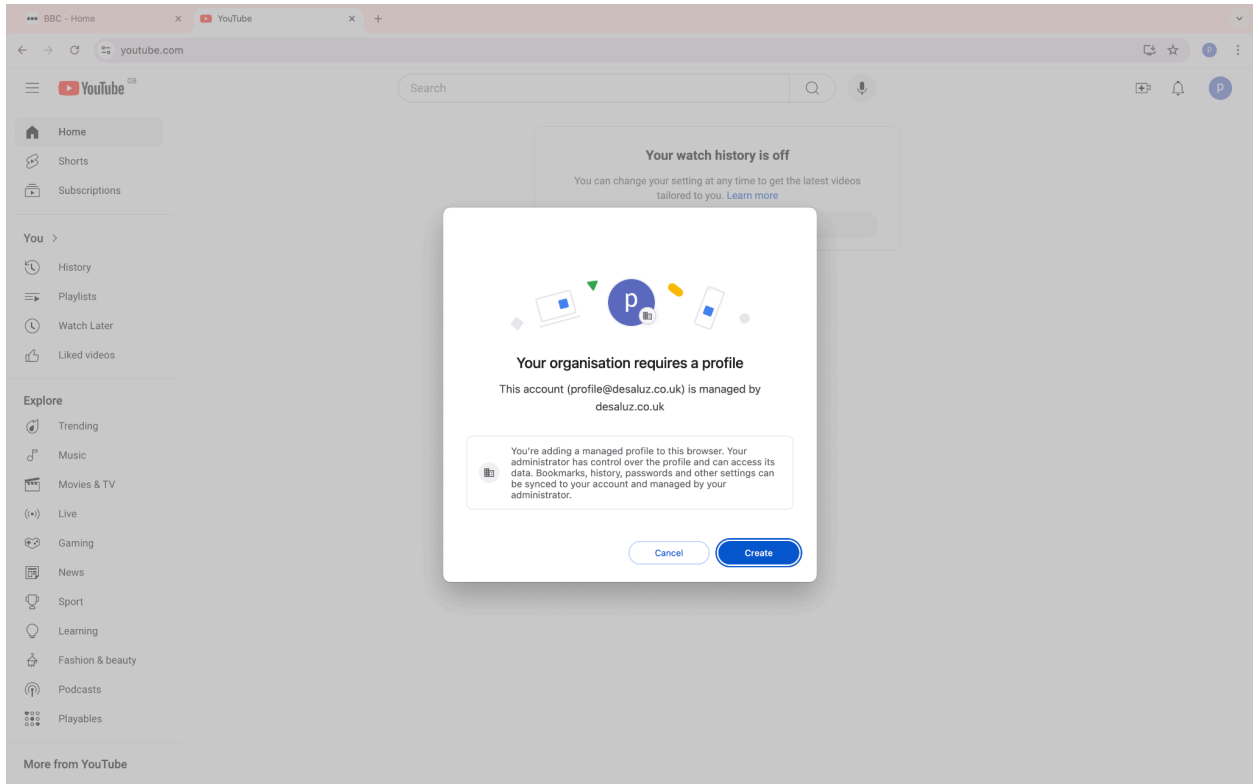


Figure 48

End user experience: Add profile

When signing into Chrome directly from the profile picker, users will not see data migration options. They will be prompted for their email address and password, followed by a profile creation notification.

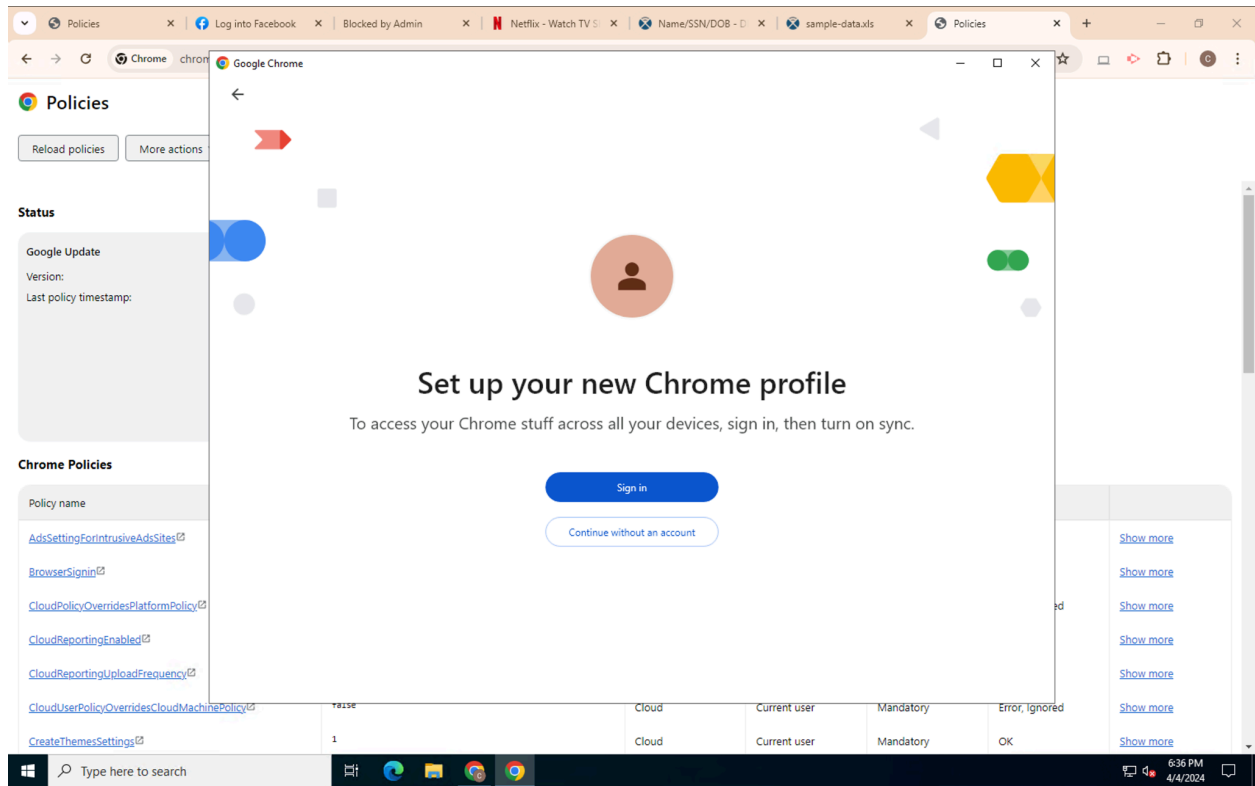


Figure 49

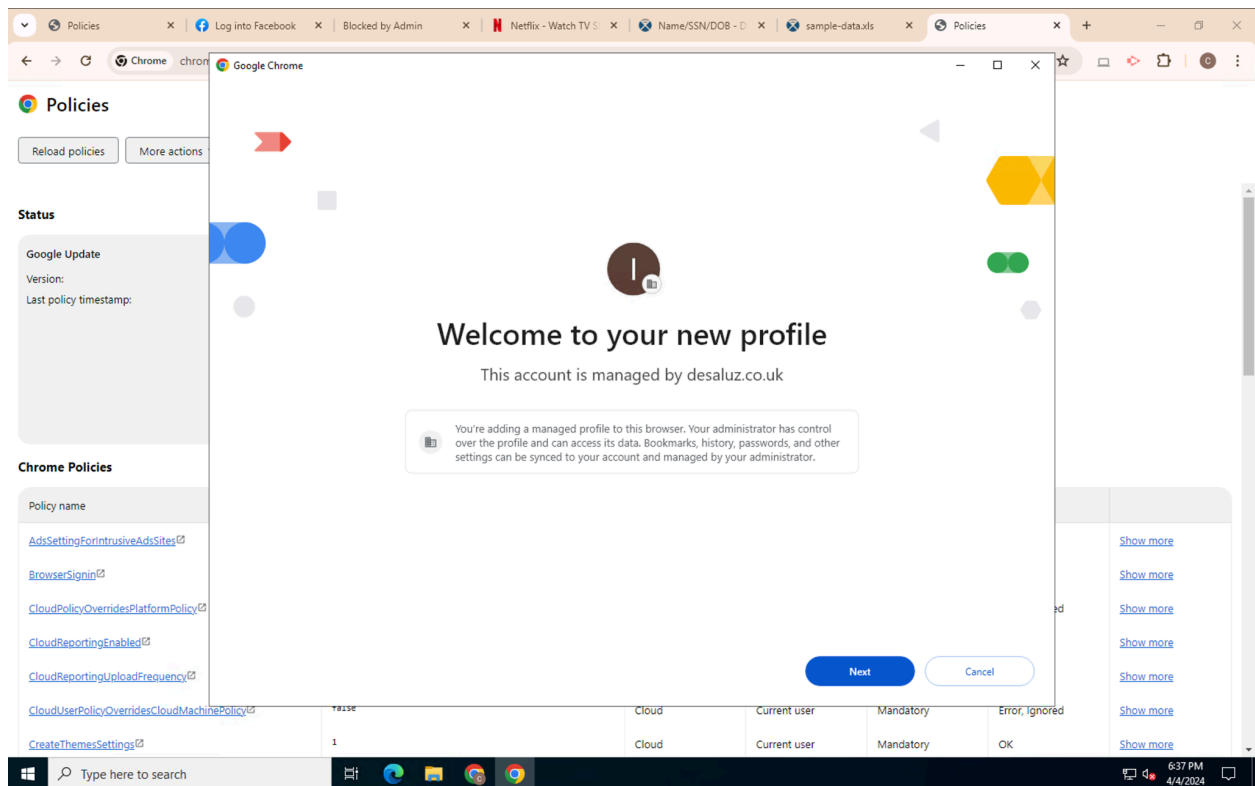


Figure 50