FIDO Pre-reg with Okta

Yubico

Nov 02, 2026

INTEGRATION GUIDE

1 Introduction **1**
- 1.1 Enrollment Options . . . 1

2 How it Works **3**
- 2.1 Process Flow . . . 3
- 2.2 Workflow integration . . . 4
  - 2.2.1 Action: Create Shipment Request . . . 5
  - 2.2.2 Action: Get Shipment Details . . . 7
  - 2.2.3 Action: Build Shipment Item . . . 9
  - 2.2.4 Action: Get Public Transport Keys and Signing Certificate . . . 11

3 Installation and Deployment **13**
- 3.1 Prerequisites . . . 13
- 3.2 Implementation Steps . . . 13

4 Configuring Okta Policies **15**
- 4.1 Creating User Groups . . . 15
- 4.2 Configuring Global Session Policy . . . 15
- 4.3 Configuring Authenticator Enrollment Policy . . . 15

5 Adding the Workflow Template **17**

6 Configuring Workflow Connections **19**
- 6.1 Creating an API Token . . . 19
- 6.2 Creating Connection from Okta Org . . . 19
- 6.3 Creating Connection from Yubico Org . . . 20
- 6.4 Updating the Create Shipment - Group Add Flow . . . 21

7 Creating Shipment Requests **25**
- 7.1 Adding New Users to Directory . . . 25
- 7.2 Creating the Shipment Request . . . 26
  - 7.2.1 Initial Authentication . . . 29
- 7.3 Troubleshooting . . . 30
  - 7.3.1 Template Errors . . . 30
  - 7.3.2 Okta Workflows Table Errors . . . 30
  - 7.3.3 Missing User Object Fields . . . 31
  - 7.3.4 Custom Okta Domain/Vanity URLs . . . 31

8 Managing Shipments **33**

9 Copyright **35**

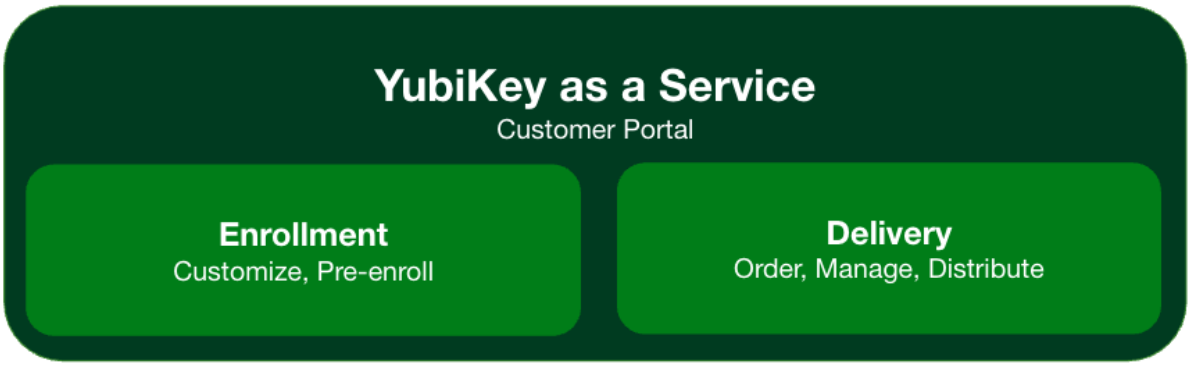
9.1 Trademarks 35
9.2 Disclaimer 35
9.3 Contact Information 35
9.4 Getting Help 36
9.5 Feedback 36
9.6 Document Updated 36

CHAPTER

ONE

INTRODUCTION

YubiKey as a Service – Enrollment provides different options for organizations to pre-enroll credentials on a YubiKey, allowing their end users to instantly start using their key to authenticate with their identity providers, without first having to register the key.



The YubiKeys are pre-programmed and shipped to end users using the *Yubico Delivery service*. Customer's can monitor and manage shipment of YubiKeys in the *Yubico Customer Portal*.

1.1 Enrollment Options

The following pre-enrollment options are available:

- **FIDO Pre-reg integration:** With this option, the keys are factory-programmed by Yubico and shipped globally, from Yubico facilities directly to the end user. The service is available through API integrations with IdPs (identity providers).

  Yubico provides integrations with the following IdPs:

  - Microsoft Entra ID, see FIDO Pre-reg with Microsoft Integration Guide.
  - PingOne (PingID/AIC), see FIDO Pre-reg with PingOne Integration Guide.
  - Okta, FIDO Pre-reg with Okta Integration Guide (this guide).

- **YubiEnroll CLI tool:** Using this option, an IT administrator with access to the organization's IdP, can pre-program credentials onto a YubiKey on-site, on behalf of an end user. The key is then provided to the end user. See YubiEnroll User Guide.

CHAPTER

TWO

HOW IT WORKS

With FIDO Pre-reg the IT administrator (IT admin) for an organization can use the YubiKey as a Service API together with the WebAuthn API of an Identity Provider (IdP) and automated workflows to order pre-enrolled YubiKeys for end users. The YubiKeys are pre-enrolled and shipped directly to the specific end user who received a randomly generated PIN separately.

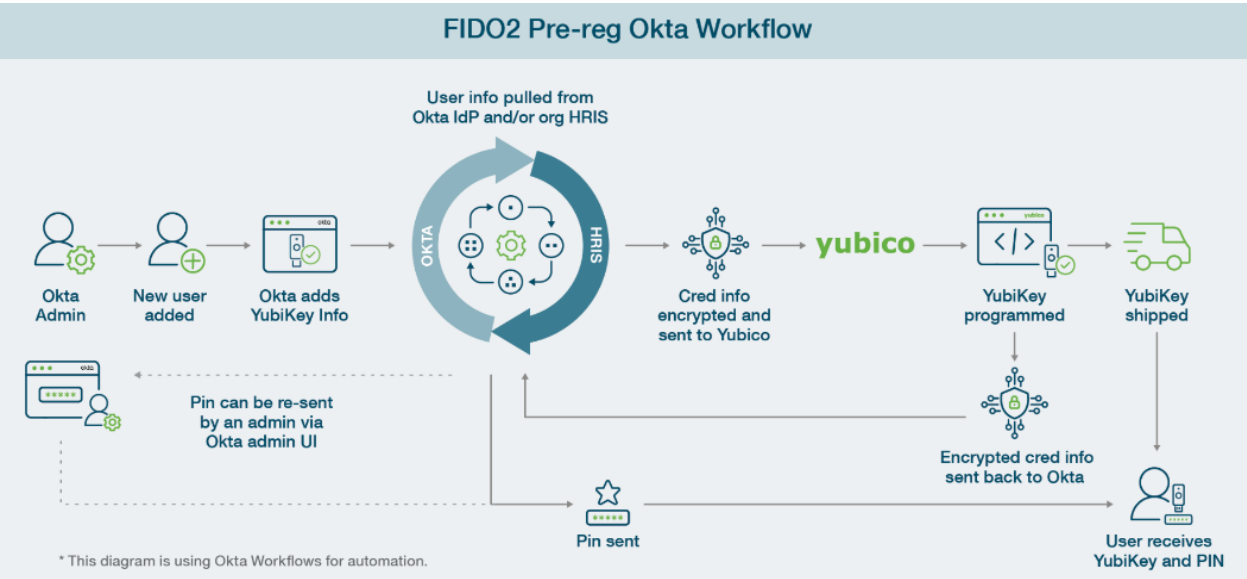
The following sections describe how to integrate FIDO Pre-reg with Okta. The instructions are intended for IT admins who are setting up shipments of pre-enrolled YubiKeys for their organization's end users in an environment using SSO and Okta as IdP.

The instructions assume you have IT administration skills and knowledge of the YubiKey as a Service API and Okta Workflows. Listed tasks include steps performed both in the Customer Portal and Okta. Refer to the Okta documentation for more details.

The FIDO Pre-reg integration streamlines the deployment process with improved ease of use and enhanced security. The diagram below illustrates the process. The FIDO Pre-reg template developed specifically for Okta Workflows, helps orchestrate the process steps. The Yubico Connector and the FIDO Pre-reg Workflow templates are both integrated with the Okta Workflows console.

2.1 Process Flow

The workflows are designed to ensure each request via Okta to Yubico contains all information needed to have the keys shipped to the end user. A secure and encrypted transfer process mitigates any risk of exposing sensitive information.



Workflow: IT Admin and End User

1. The IT admin initiates a shipment request for a pre-enrolled key from the IdP (Okta) tenant. This triggers the FIDO Pre-reg Okta Workflows template. All information needed to program and ship a key for an individual user is sent to Yubico through a Delivery service API request. Note that only one key per shipment can be requested.
2. The IT admin receives updates based on the shipping status, and can monitor shipments of pre-enrolled keys using the Customer Portal.
3. The end user receives an email containing their YubiKey PIN and their FIDO Pre-reg YubiKey is shipped to them directly. No IdP password or IdP registration is required. The YubiKey PIN is only communicated to the end user and is encrypted and obscured from Okta, the IT admin, and Yubico.
4. The end user can immediately use the YubiKey and PIN to authenticate into Okta where they have Single Sign-On (SSO) access to applications to which they have access provided through the Okta.

Workflow: Credential and PIN Provisioning

1. The IT admin initiates a shipment request for a pre-enrolled YubiKey from the Okta tenant.
2. Yubico receives the shipment request from Okta through the YubiKey as a Service API. Yubico programs a YubiKey with the information provided in the request. The information contains the credential and PIN requests, end user shipping information, and YubiKey form factor.
3. After the YubiKey is programmed, a response is sent back to the YubiKey as a Service API including the randomly generated PIN, serial number, and firmware version. This response is retrieved by the Okta workflows.
4. When the Okta workflows receive the response from the YubiKey as a Service API, the YubiKey is enabled for usage. This triggers an email to the end user containing the PIN for the YubiKey.
5. After the programming of the YubiKey the credential data, including the PIN, is purged from Yubico systems.

Additionally, the YubiKey can be used as a recovery tool for the IdP's complementary passwordless feature such as Okta FastPass. For example, if an end user loses their phone and gets a replacement one, they can re-enroll in the IdP service using the YubiKey without needing to call their support services.

2.2 Workflow integration

The following describes the integration between the Yubico Connector in Okta and the Okta Workflows. The integration provides the Yubico action cards used to set up the workflows in Okta for requesting shipments and retrieving shipment information. The Yubico workflow integration includes the action cards described below.

Action	Description
Create Shipment Request	Create a new shipment request to provision a YubiKey that will contain a pre-enrolled WebAuthn credential.
Get Shipment Details	Get details about a specific shipment request, including the shipment state, and shipment items used for the pre-enrolled of a WebAuthn credential.
Build Shipment Item	Helper action card that builds a "shipment item" used in the "Create shipment request" action card.
Get Public Transport Keys and Signing Certificate	Pull the current public Yubico transport and signing keys used to encrypt the PIN and credential request payloads.

The input and output parameters for each action card are described in more detail in the following. For more information, see *Configuring Workflow Connections*.

When you add a Yubico card to a flow for the first time, you will be prompted to authorize the connection using an API token generated from the Customer Portal. Once you have configured this connection and saved the API token information to it, you can reuse the connection for other YubiKey as a Service API-related actions. For more information, see *Creating an API Token*.

2.2.1 Action: Create Shipment Request

Action card to create a new shipment request to provision a YubiKey that contains a pre-enrolled WebAuthn credential.

Note: Product ID and Inventory Product list can be found in the Product inventory type mapping table.

Input - Create Shipment Request

Field	Definition	Type	Req'd
Company	Company name of shipment recipient	Text	TRUE
Email	Email address of shipment recipient	Text	FALSE
First Name	First name of shipment recipient	Text	FALSE
Last Name	Last name of shipment recipient	Text	FALSE
Phone Number	Telephone number of shipment recipient The limit is 40 of the alphanumeric characters "0-9+-( )" unless the country code is IN, in which case the limit is 255. Any format is acceptable, with or without spaces.	Text	TRUE
Address	Street address of shipment recipient Note: This field can also include the apartment or unit number.	Text	TRUE
Apt or Unit Number	The apartment or suite or unit number or designation of shipment recipient.	Text	FALSE
City	City of shipment recipient	Text	TRUE
Region	2-letter region or state code of shipment recipient. Mandatory for recipients in the US or Canada.	Text	FALSE
Postal Code	Zip code or postal code of shipment recipient.	Text	TRUE
Country Code		Text	TRUE

Output - Create Shipment Request

Field	Definition	Type
Shipment ID	The shipment ID of the newly created shipment. Value is null for non-successful API response.	Text
Shipment State ID	The shipment state of the newly created shipment. For values, see Shipment State Codes. Value is null for non-successful API responses.	Number

2.2.2 Action: Get Shipment Details

Action card to get details about a specific shipment including the shipment state and the shipment items used for the pre-registration of a WebAuthn credential.

Input - Get Shipment Details

Field	Definition	Type	Req'd
Shipment ID	ID for a specific shipment.	Text	TRUE

Output - Getting Shipment Details

Field	Definition	Type
Shipment State ID	The shipment state of the newly created shipment. For values, see Shipment Status Codes in the Customer Portal User Guide. Value is null for non-successful API responses	Number
Shipment Items	List of items included in the shipment. Underlying objects include details for each item.	List of objects
	product_data: Details about a shipment item. Includes: - serial - version - fido_pin_response - fido_credential_response	List of objects
	serial: Serial number of the item	Text
	version: Firmware version of the item	Text
	fido_pin_response: PIN for the item. Is encrypted as a JWE string. This string should be provided to Okta's WebAuthn pre-registration activate endpoint.	Text
	fido_credential_response: List of FIDO credentials for the item. Is encrypted as a JWE string. This string should be provided to	List of strings

2.2.3 Action: Build Shipment Item

Action card that builds a `shipment item` used in the `Create shipment request` action card.

Input - Build Shipment Item

Field	Definition	Type	Req'd
Customization ID	ID associated with the specific Yubico customization assigned to an organization.	Text	TRUE
Product ID	ID associated with the specific YubiKey format.	Number	TRUE
Inventory Product ID	ID for the "bucket" containing credits for YubiKey ordering.	Number	TRUE
Quantity	Number of keys to include in this shipment (current limitation is 1).	Number	TRUE
PIN Request - Encrypted	Customization options for YubiKey PIN generation, wrapped as a JWE string. This string is the output provided by Okta's WebAuthn pre-registration enroll endpoint.	Text	TRUE
Credential Requests - Encrypted	PublicKeyCredentialCreatic for WebAuthn credential creation, wrapped as a JWE string. This string is the output provided by Okta's WebAuthn pre-registration enroll endpoint. Note: This input item is noted as a as list. This is due to YubiKey as a Service's	List of strings	TRUE

Output - Build Shipment Items

Field	Definition	Type
Shipment Item	Object that contains configuration details for an item to include in a shipment.	Object

2.2.4 Action: Get Public Transport Keys and Signing Certificate

Action card to pull the current public Yubico transport and signing keys used to encrypt the PIN and credential request payloads.

Input - Get Public Transport Keys and Signing Certificate

No input required.

Output - Get Public Transport Keys and Signing Certificate

Field	Definition	Type
Transport Keys - JWKS	Yubico JWKS (JSON Web Key Set) used for deriving an ECDH shared secret. Primarily used for encrypting the PIN and credential requests for the YubiKey as a Service API.	Object
Signing Public Keys - JWKS	Yubico JWKS (JSON Web Key Set) containing signing certificates used for signing PIN and credential responses from the YubiKey as a Service API.	Object

CHAPTER

THREE

INSTALLATION AND DEPLOYMENT

The following provides an overview of the prerequisites and steps to install, deploy, and verify the components used for the FIDO Pre-reg integration with Okta as IdP.

3.1 Prerequisites

Ensure you have the items listed below before starting the implementation procedure.

Provided by Yubico:

- A Yubico subscription plan. For questions about Yubico subscription services, contact your Yubico sales representative.
- Yubico Customer Portal access with FIDO Pre-reg enabled. This is provided during onboarding of your organization.
- Customization ID (CID), Product ID, and Inventory ID for the YubiKey delivery.

Provided by customer:

- An Okta Identity Engine (OIE) tenant with Adaptive MFA and Okta Workflows entitlements.
- In order for users to be able to authenticate with a security key, ensure that FIDO2 WebAuthn is enabled in your Okta tenant. In the **Okta Admin Console**, configure **User verification** to use the **Preferred** option as described in Add the Passkey (FIDO2 WebAuthn) authenticator (Okta documentation).

Note: The FIDO Alliance recommends `UV=Required`. However, you will need to assess the impact of `UV=Required` based on your organization's current settings, as it may impact users across operating systems and browser types if a PIN is not set. `Preferred` is an option, if you are concerned about blocking other users.

3.2 Implementation Steps

The FIDO Pre-reg workflow template for Okta is flexible and you can request a pre-enrolled YubiKey using the following methods:

- **MFA initiated** - trigger shipments using Pre-enrolled authenticators in Okta Workflows console for an individual user.
- **Group Add** - trigger shipments using the Group Add flow in the Okta Workflows console (individual or multiple users). Lets you request shipments based on group membership.

- **Batch requests** - use the API to order YubiKeys for multiple users. For more information, see Order pre-enrolled YubiKeys in a batch (Okta documentation).

The following steps lets you set up the FIDO Pre-reg integration and create a shipment request for a pre-enrolled YubiKey:

1. *Create user groups and configure Okta policies*
2. *Add the FIDO Pre-reg Workflow template*
3. *Configure the workflow connections*
4. *Create a shipment request*

The sections in the following describe each step in detail.

CHAPTER

FOUR

CONFIGURING OKTA POLICIES

This section describes how to create user groups and configure phishing-resistant authentication policies in Okta to support the FIDO Pre-reg integration.

4.1 Creating User Groups

Create groups for new and existing users in Okta. For information on how to do this, see Create groups for new and existing users (Okta documentation).

4.2 Configuring Global Session Policy

Create a Global Session Policy that is configured to establish the user session with any factor that is *not a password*. For information on how to do this, see Configure a global session policy (Okta documentation).

4.3 Configuring Authenticator Enrollment Policy

Authenticator enrollment policies let you manage how and when your end users enroll authenticators, for example to use "WebAuthn Only". For more information, see Configure an authenticator enrollment policy (Okta documentation).

CHAPTER

FIVE

ADDING THE WORKFLOW TEMPLATE

The FIDO Pre-reg Okta workflow template includes flows for example for shipment triggers, shipment processing, and credential mapping.

To add the workflow templates to your Okta instance, do the following:

1. Go to the **Okta Workflows Template** catalog.
2. Locate the **Yubico FIDO Pre-reg Workflow** template by searching for "Yubico FIDO Pre-reg" in the search bar within the Okta Workflows console.
3. Click **Add Template**.

CHAPTER

SIX

CONFIGURING WORKFLOW CONNECTIONS

In this step you will authorize and configure the **Create shipment** workflow connections.

6.1 Creating an API Token

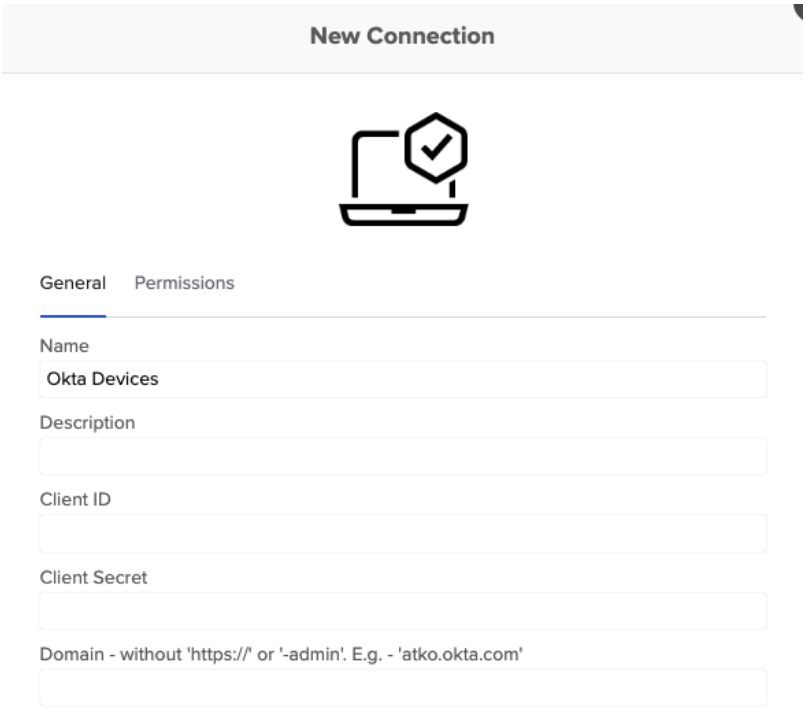
When you add a Yubico card to a flow the first time you are prompted to authorize the connection using an API token for your organization.

To create an API token, sign in to the Customer Portal with the account for the application that will be calling the YubiKey as a Service API. Click the organization name on the top of the left menu and select **Manage API token**. In the token dialog that appears, click **Create API token** and save the token for later use. For more information, see Creating API Tokens (Customer Portal User Guide).

6.2 Creating Connection from Okta Org

Do the following to create the connection from the *Okta org*:

1. In the **Okta Admin** console, open **Workflows** and click **Connections > New Connection**.
2. Locate and select the **Okta** connector icon.
3. Add a display name for the connection in the **Name** field, and provide a description.

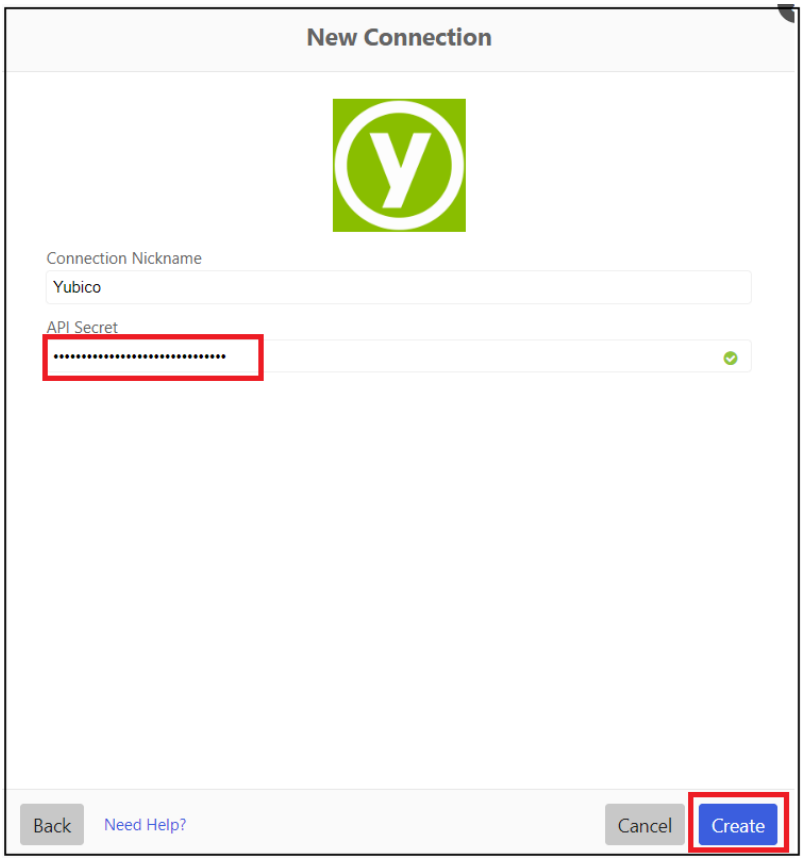


4. Enter the **Client ID** and **Client Secret** values provided in Okta Workflows OAuth.
5. In the **Domain** field, enter your Okta org domain without `https://`, for example, company.okta.com. If your org uses a custom domain, enter the custom domain.
6. Click **Create**.

6.3 Creating Connection from Yubico Org

Do the following to create a connection from the *Yubico org*:

1. If not already done, generate an API token as described in *Creating an API Token*. Save the API token in a location from where you can easily copy and paste it.
2. In the **Okta Admin** console, open **Workflows** and click **Connections > New Connection**.
3. Locate and select the **Yubico** connector icon.
4. Provide a display name for the connection in the **Connection Nickname** field, paste the previously generated API token into the **API Secret** field.

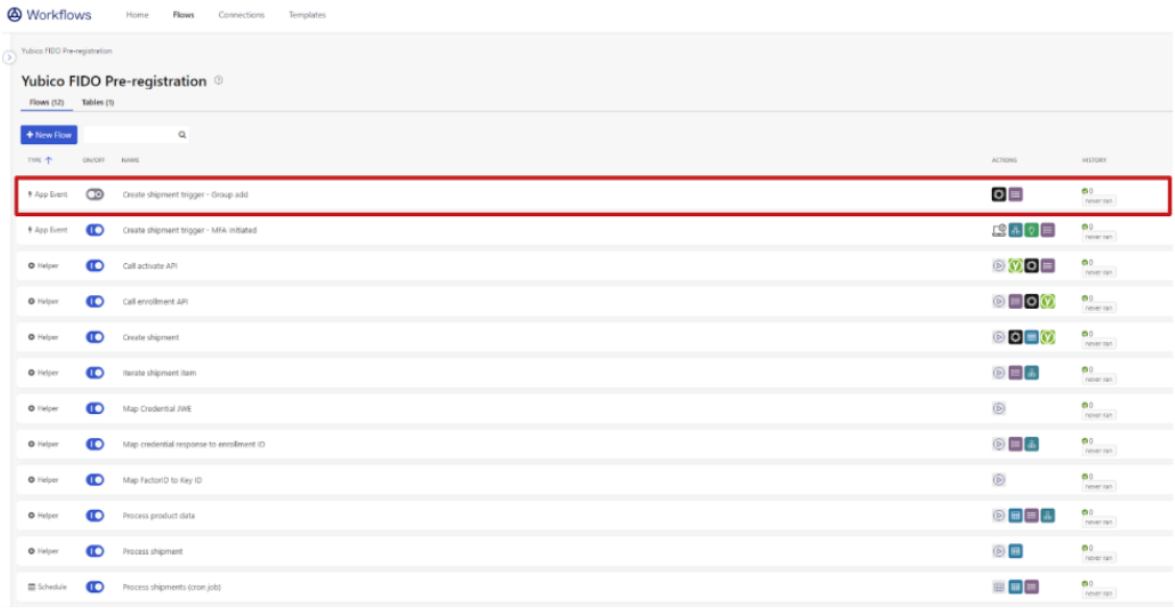


5. Click **Create**.

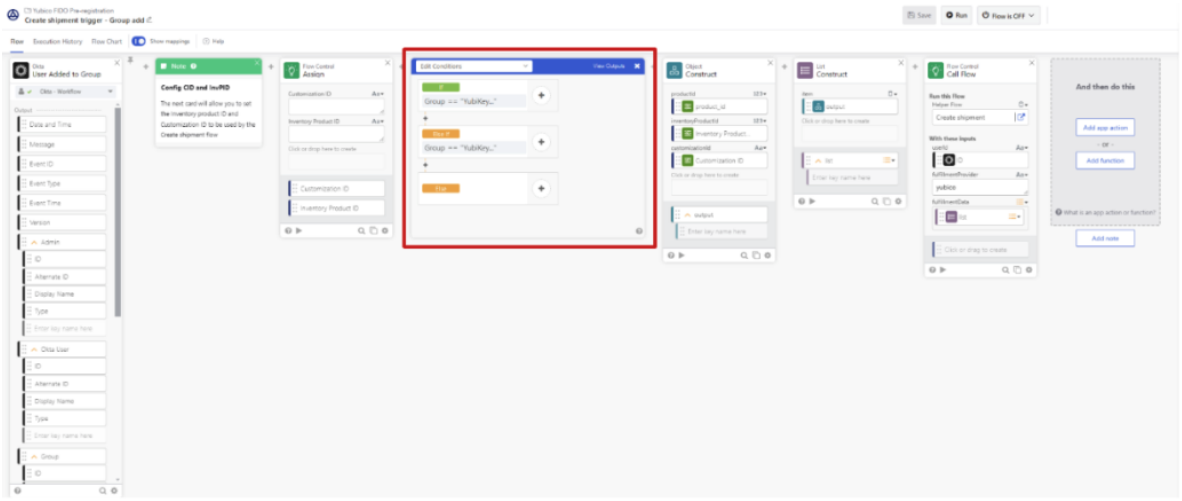
6.4 Updating the Create Shipment - Group Add Flow

If requesting a pre-enrolled YubiKey via the *Group Add* flow, you will need to add customization and product IDs to the Create shipment - Group Add flow as described in the following:

1. In the **Okta Admin** console, open **Workflows**, select **Flows** and open the **Create shipment trigger - Group add** workflow.



2. In the **Create shipment** page, open the dropdown menu on the **Edit Conditions** card.



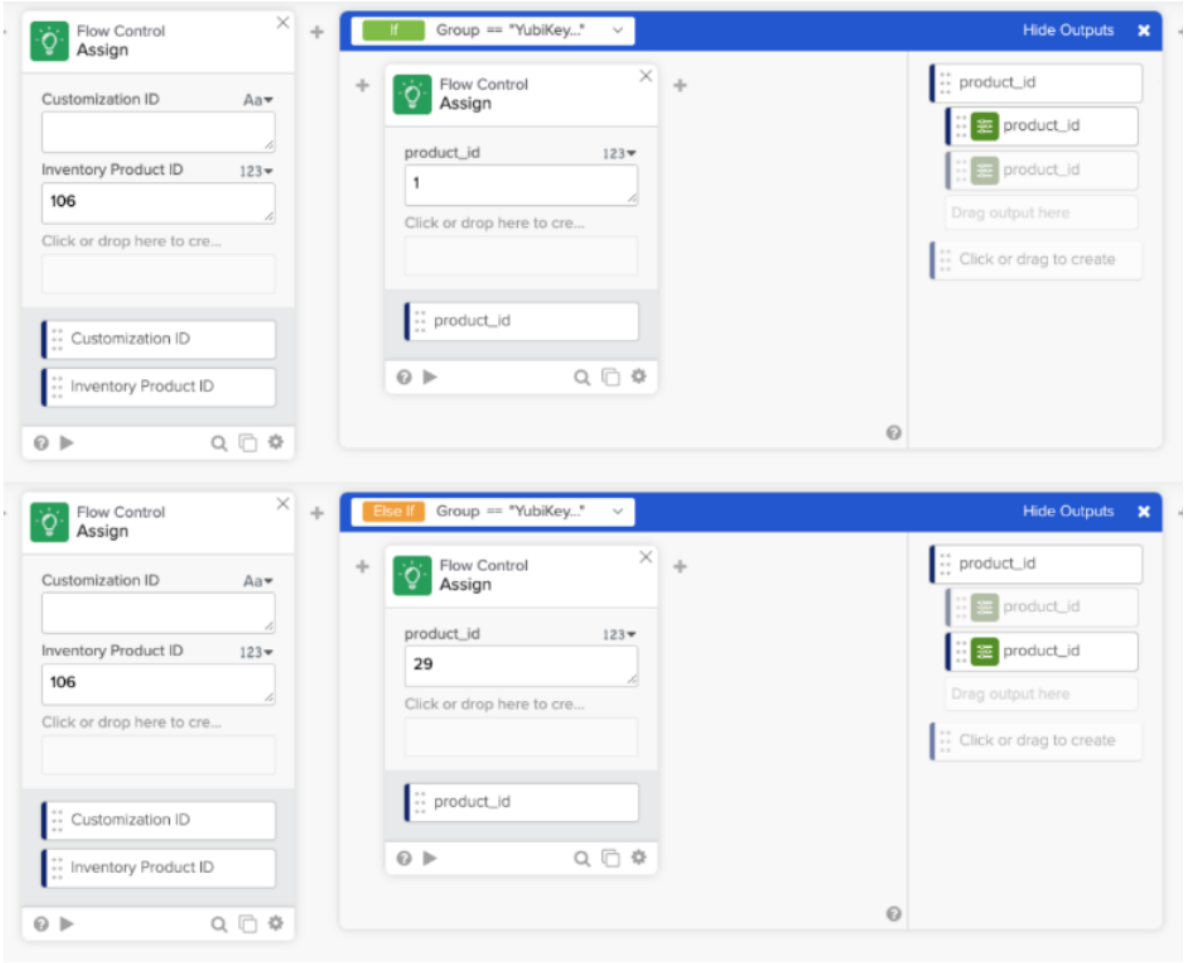
3. Update the fields as described below using input values provided by Yubico during onboarding of your organization. Note that in this example, the `product_id` is "1" for key model *YubiKey 5 NFC* and "29" for key model *YubiKey 5C NFC*. For more information, see Product ID and Inventory Product ID (Customer Portal User Guide).

    a. **If product_id** (for *YubiKey 5 NFC*): Your Customization ID.

    b. **If inventory_product_id**: Your Subscription ID.

    c. **Else if product_id** (for *YubiKey 5C NFC*): Your Customization ID.

    d. **Else if inventory_product_id**: Your Subscription ID.


Flow Control
Assign
Customization ID
Aa
Inventory Product ID
123
106
Click or drop here to cre...
Customization ID
Inventory Product ID
If
Group == "YubiKey..."
Hide Outputs
Flow Control
Assign
product_id
123
1
Click or drop here to cre...
product_id
product_id
product_id
product_id
Drag output here
Click or drag to create
Flow Control
Assign
Customization ID
Aa
Inventory Product ID
123
106
Click or drop here to cre...
Customization ID
Inventory Product ID
Else If
Group == "YubiKey..."
Hide Outputs
Flow Control
Assign
product_id
123
29
Click or drop here to cre...
product_id
product_id
product_id
product_id
Drag output here
Click or drag to create

4. Click **Save**.

CHAPTER

SEVEN

CREATING SHIPMENT REQUESTS

Important: Before you start creating shipment requests, ensure you have the Customization IDs and Product IDs for the YubiKey models you will be shipping to end users. These IDs are provided by Yubico during onboarding of your organization. For more information, see *Prerequisites*.

In this step you will add new users for shipments and create a shipment request. In order to make a shipment request, the following information is required for the user, either from the Okta Universal Directory (UD) or from your organization's HRIS (Human Resources Information System):

- First Name
- Last Name
- Street Address
- City
- State/Province/Territory (2-letter format codes)
- Postal Code
- Country Code
- Primary email
- Secondary email (for onboarding *new* users to receive a PIN)
- Primary phone number
- Organization

7.1 Adding New Users to Directory

The following describes how to add a *new* user with status "Staged" in Okta. For more information, see Create staged user (Okta documentation).

To add a new user, do the following:

1. In the **Okta Admin** console, go to **Directory > People** and click **Add person**.
2. In the **Add Person** dialog, enter information as follows:
    - **First name**, **Last name**, and **Username**.
    - **Primary email** (work email) for active users.
    - **Secondary email** (personal email used prior to activation for new users).

- Do not assign the user to any YubiKey groups, this is done later.
- Set **Activation** to "Activate later". This creates the user in status "Staged".

3. Click **Save**.
4. On the **People** page, go to **Staged > User > Profile > Edit**.
5. Enter the following information required for key shipment: **Primary phone**, **Street address**, **City**, **State**, **Zip code**, **Country code**, and **Organization**.
6. Click **Save**.

7.2 Creating the Shipment Request

You can create shipment requests either through the Okta Admin console using Okta Groups, or using the API for batch shipment requests, see *Implementation Steps*.

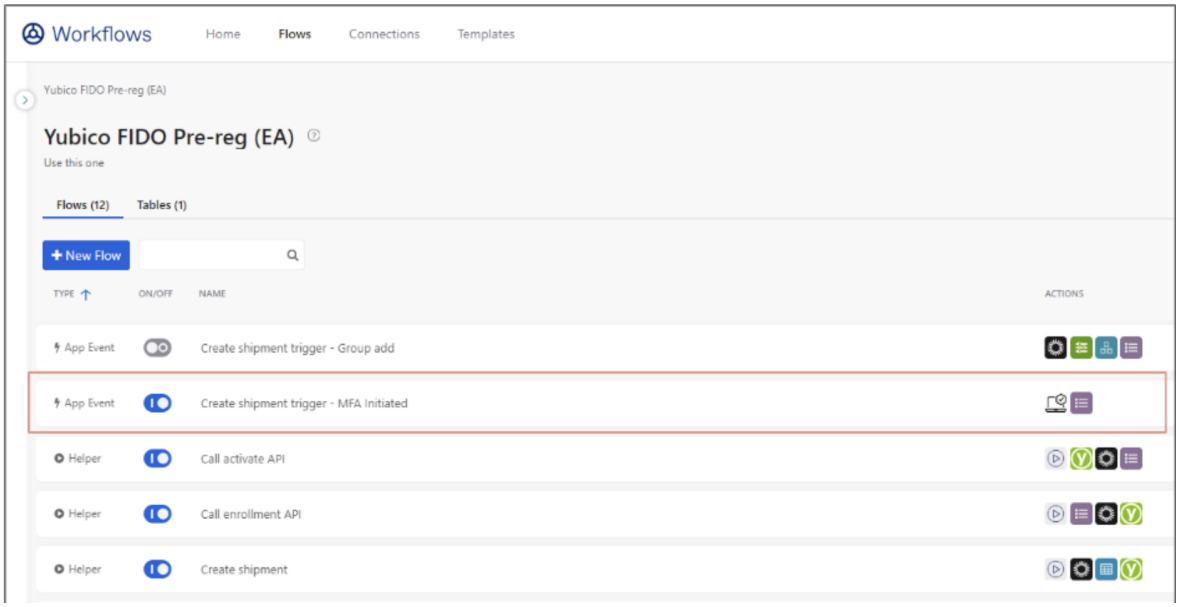
In this example we will use the **Pre-enrolled authenticators** option in the **Okta Workflows** console to create a shipment request.

Note: Only one FIDO Pre-reg YubiKey at a time can be requested for an Okta tenant.

To create a shipment request, do the following:

1. In the **Okta Workflows** console, ensure the **Create shipment trigger - MFA initiated** flow is *enabled*.

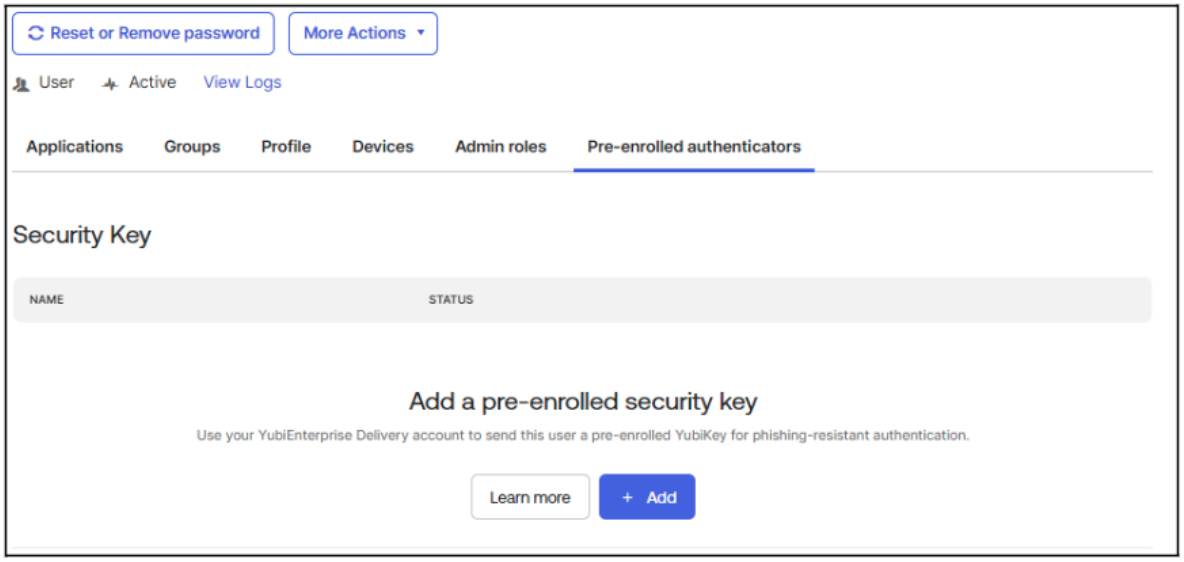
   Note: It is recommended that only one flow at a time be enabled: either the **Group Add** or the **MFA Initiated** flow.



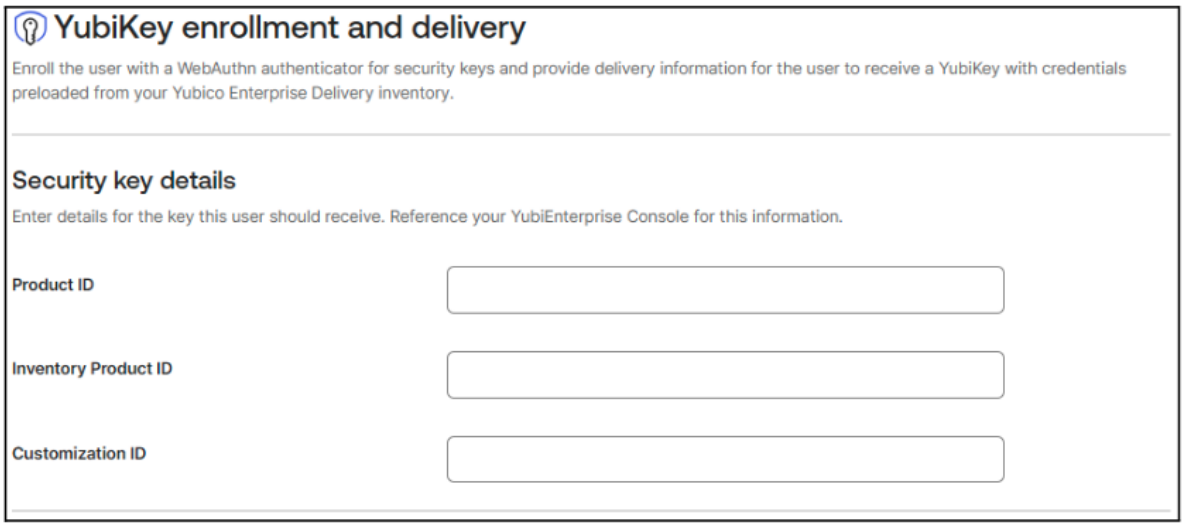
2. In the **Okta Admin** console, ensure the user to whom you want to ship the key has a profile in the user directory. If not, create a new user as described in *Adding New Users to Directory*.
3. Click the profile of the desired user and do the following:

- If using the Okta Universal Directory (UD) to source the shipping information, ensure this is populated in the user profile.
- Alternatively, confirm the user's shipping information is being sourced from an HRIS or other source of truth.

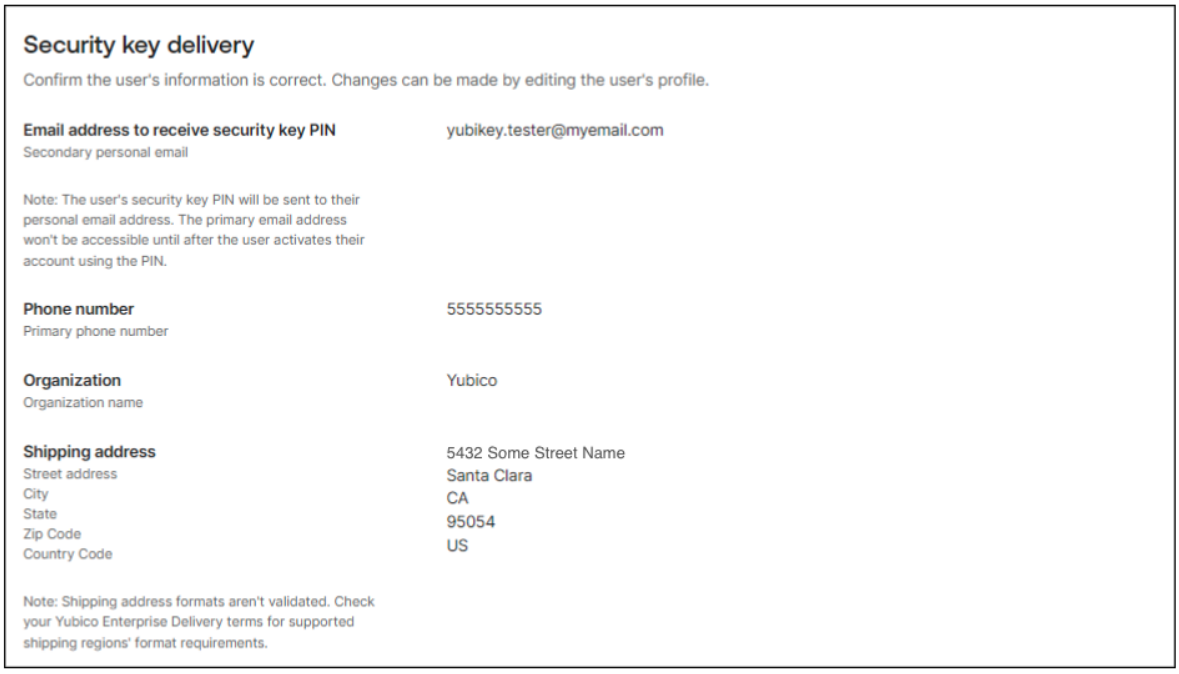
4. In the user profile, click **Pre-enrolled authenticators** and then click **+ Add**.



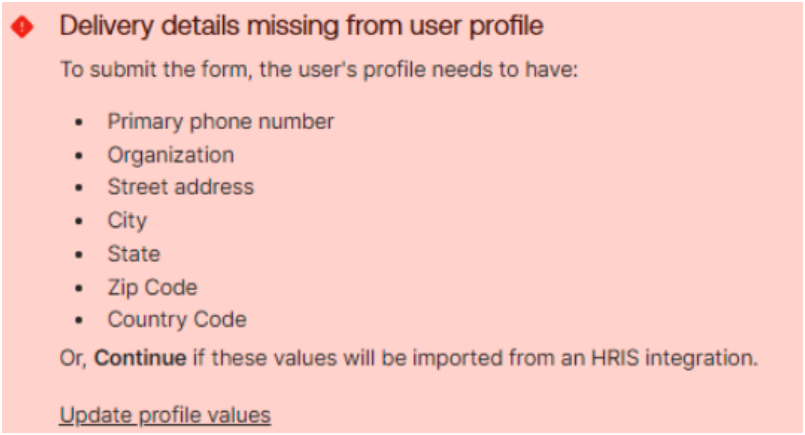
5. On the **YubiKey enrollment and delivery** page, enter the **Product ID**, **Inventory ID**, and **Customization ID** provided by Yubico during onboarding. See *Prerequisites*.



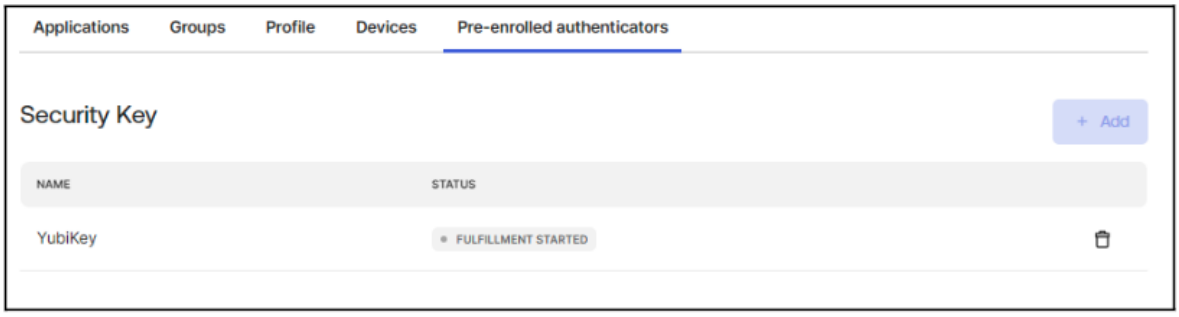
6. On the **Yubikey enrollment and delivery** page, ensure all required fields are populated: Primary and secondary **Email address** (PIN will be sent to both), primary **Phone number**, **Organization**, and **Shipping address**.



7. If the user's shipping information is being sourced elsewhere, you will receive a message stating that it is missing. Ensure that the information is retrieved from another endpoint or update the profile values before continuing.



8. Click **Continue**.
9. The FIDO Pre-reg workflow is triggered and the fulfillment starts.



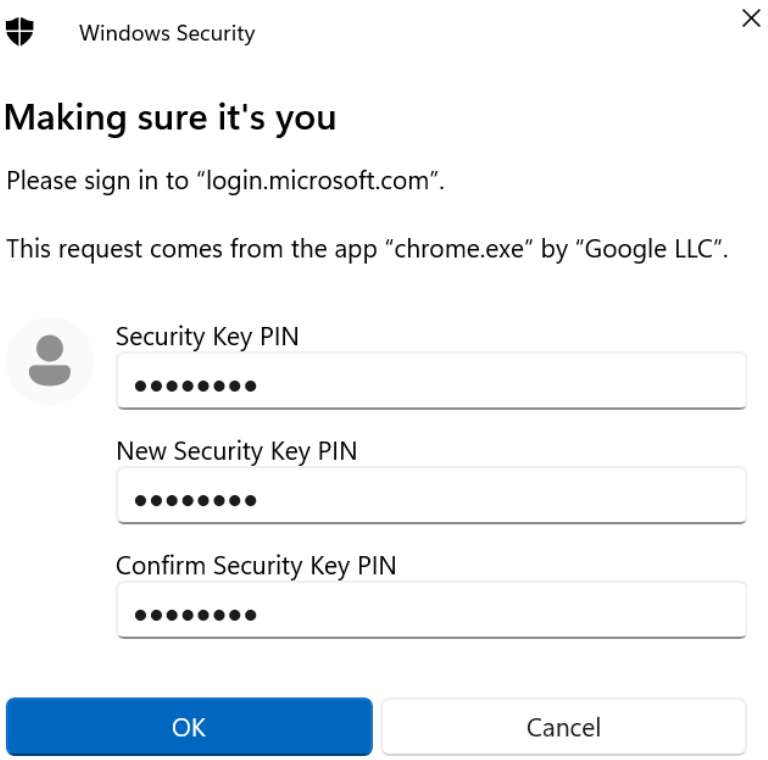
Yubico receives a request for a pre-enrolled YubiKey. The request contains all information needed to program and ship the key. When the request is fulfilled and the credential is activated by Okta, the randomly generated PIN associated

with the YubiKey is emailed to the user's secondary email address (new user). For existing users, it will be sent to their primary email address.

Note: Once the credential is programmed onto the YubiKey, the challenge and credential data, including PIN, is purged from Yubico systems.

7.2.1 Initial Authentication

To authenticate with the identity provider, the end user presents their YubiKey and enters the provided PIN. If "Force PIN change" is set (and if supported by the platform), the end user is prompted to change the PIN when using the YubiKey for the first time, as in this example.



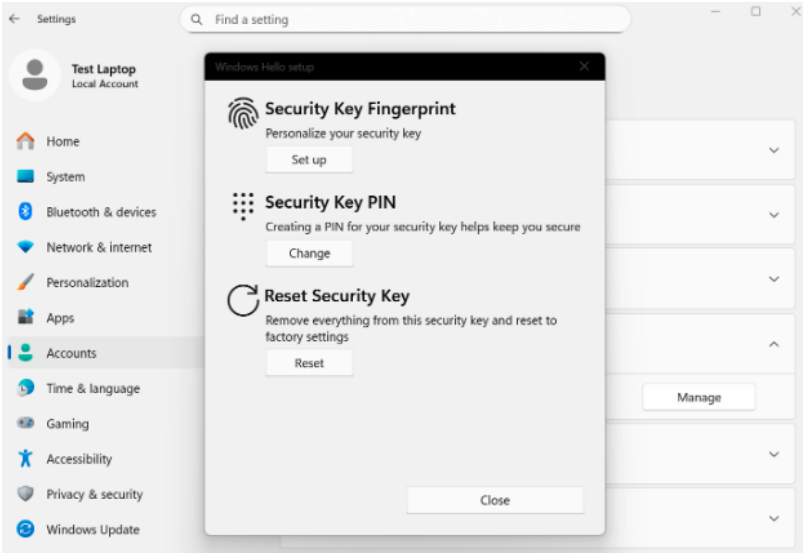
If "Force PIN change" was not set, the end user will be able to log in without changing the provided PIN, when using the YubiKey for the first time.

The previous step also applies when using a *YubiKey Bio (FIDO and Multi-Protocol Editions)* where the end user authenticates primarily using fingerprint(s) enrolled on the key (a PIN is required as fallback also when using fingerprint authentication).

Note: In most cases, the end user will *not* be automatically prompted to enroll a fingerprint when using a pre-enrolled YubiKey Bio the first time. Enrolling a fingerprint must be done by the end user in a separate step as described in the following.

Here is an example of how to enroll fingerprints when using *Windows 11*: Navigate to **Settings** > **Accounts** > **Sign-in options**, select **Security key**, and click **Manage**. Enter the PIN for the YubiKey Bio, and follow the on-screen

instructions, which will prompt you to insert the security key and touch it to enroll a fingerprint. When done, you will be prompted to provide the fingerprint (instead of the PIN) when logging in.



Different platforms (device/OS/browser) will have different flows with regards to enrolling fingerprints on YubiKeys. Refer to the account security settings information for each platform for instructions on how to enroll fingerprints. For more examples of fingerprint enrollment, see YubiKey Bio Series Specifics.

Yubico Authenticator is a convenient tool that can also be used to enroll fingerprints on a YubiKey Bio. For instructions on how to install Yubico Authenticator and enroll fingerprints, see Install the App and Enroll a fingerprint.

Select the method that is applicable to your organization's IT platform when providing recommendations for your end users on how to enroll fingerprints on their pre-enrolled YubiKey Bio.

7.3 Troubleshooting

The following provides guidelines on how to solve common issues.

7.3.1 Template Errors

As an Okta administrator, you can review errors with the FIDO Pre-reg template in the FIDO Pre-reg Workflow **Execution History**. For more information, see Check Execution History (Okta documentation).

7.3.2 Okta Workflows Table Errors

If a shipment in the Okta Workflows table is in an error state due to an invalid address (address validation failed), you can manually remove the shipment in the Yubico Customer Portal. For information on how to do this, see Editing and Deleting Shipments (Customer Portal User Guide).

If the shipment is in an error state which can be resolved (for example by correcting the address), do not duplicate or re-add the entry. Instead, manually change the state from "error" to "ongoing" in the Okta Workflows Shipments table.

7.3.3 Missing User Object Fields

If the submitted shipment request has an error due to a missing user object field, review the **Execution History** for the *Create Shipment Request card* in the Yubico FIDO Pre- reg template to identify the missing object.

Navigate to the user object in the **Okta Universal Directory (UD)** and add the missing input into the appropriate field. If using an HRIS system, ensure that the user object contains all the necessary user shipping information: Address, city, state, zip code, country code, organization, primary email, secondary email, and primary phone number. For organization, the "organization" title may need to be hardcoded in the Okta Workflow card.

Once the required information is provided, make the request again.

7.3.4 Custom Okta Domain/Vanity URLs

If your Okta organization uses a vanity or custom URL, the Okta Connector and the Okta Device Connector in the Workflows should be configured to use the custom URL. Both the Okta and Okta Devices Connectors will need the custom URL.

CHAPTER

EIGHT

MANAGING SHIPMENTS

The status for a shipment can be viewed in the Customer Portal for your organization, and in the user's Okta profile under "Pre-Enrolled Authenticators". The information in Okta is pulled from the Yubico Delivery service.

You can edit a shipment request, for example to update the recipient and address information or delivery type, as well as delete a shipment request if needed. For more information, see Managing Enrolled Shipments.

Note: A shipment request must be deleted both in the Customer Portal and in the user's Okta profile on the "Pre-enrolled authenticators" tab. Additionally, you can remove a shipment request from the Okta Workflow Pre-reg Shipments table. If not removed from that table, on the next process run, the YubiKey as a Service API will return a 404 message, set the status to "error", and not process it again.

CHAPTER

NINE

COPYRIGHT

© 2021-2026 Yubico AB. All rights reserved.

9.1 Trademarks

Yubico and YubiKey are registered trademarks of Yubico AB. All other trademarks are the property of their respective owners.

9.2 Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

All Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

9.3 Contact Information

Yubico AB
Gävlegatan 22
113 30 Stockholm
Sweden

9.4 Getting Help

Documentation is continuously updated on https://docs.yubico.com/ (this site). Additional support resources are available in the Yubico Knowledge Base.

Click the links to:

- Submit a support ticket for YubiKey as a Service and Customer Portal
- Submit other support requests
- Contact our sales team

9.5 Feedback

Yubico values and welcomes your feedback. If you think you may have discovered a flaw in our product, please submit a support request at https://support.yubico.com/s/requests and provide as much detail as you can.

9.6 Document Updated

2026-11-02 12:48:48 UTC