

# Simplifying User Experiences with Single Registration Playbook

Requirements and Specifications for Single Registration Web to Workstation Deployment

<b>Single Registration Introduction</b>	<b>2</b>
<b>Workstation to Web Single Registration</b>	<b>2</b>
Facts	2
Pre-Requisites	2
Configuration	3
<b>Web to Workstation Single Registration</b>	<b>4</b>
Facts	4
Pre-Requisites	4
Configuration	4
HYPR Enrollment Service - Facts	5
HYPR Enrollment Service - Installation Requirement	5
Web To WS Single Registration Sequence Diagram	6
<b>Testing the Workflow</b>	<b>9</b>
<b>Deployment Strategy</b>	<b>9</b>
<b>Logs and Audit Trail</b>	<b>9</b>

## Single Registration Introduction

Passwordless Authentication using Mobile devices as authenticator enhances application security and simplifies user experiences. The users can register their mobile devices to the desktop using HYPR WFA client for passwordless login to their desktop and to the protected browser web applications. The authentication user experiences can be taken to the next level by allowing the user to register their mobile device only one time using HYPR single registration mechanism and users can have passwordless login to their desktop and protected web applications without having to register their mobile devices additionally.

Single registration could be achieved from **workstation to web** or from **web to workstation** or both directions.

## Workstation to Web Single Registration

### Facts

- Workstation to Web Single Registration is a one way registration traffic which allows the user to initiate and complete the registration ceremony one time using HYPR WFA Client. The user doesn't have to register explicitly to the configured web applications. Post this single registration ceremony, the user would be able to login to desktop and web applications.
- From the user's perspective, it is a one time registration experience, however from the backend's perspective, HYPR Server creates both desktop and web profiles.
- This single registration process doesn't stop the user from registering explicitly to the web application and in this case, the web registered profile is not linked with the desktop profile.
- The user could create multiple desktop profiles for the same user from multiple desktop machines, however all these desktop profiles would be linked with only one web profile.
- Desktop profile deregistration initiation from any desktop machine would delete that desktop profile and the associated web profile. Post this operation, the user would NOT be able to login to the web profile.

### Pre-Requisites

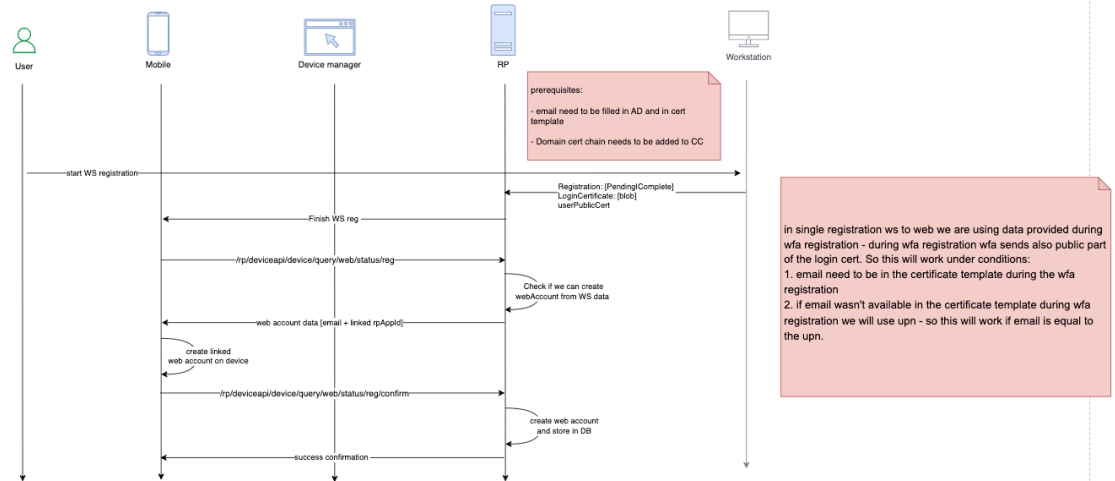
1. Create and configure rpApp for Workstation.

2. Create and configure rpApp for all web applications which users would need to login without having to register explicitly for the web.
3. HYPR WFA Client is required to be installed.

## WS To Web Single Registration Sequence Diagrams

### 1. New Web Profile Scenario - The user doesn't have any existing web profile.

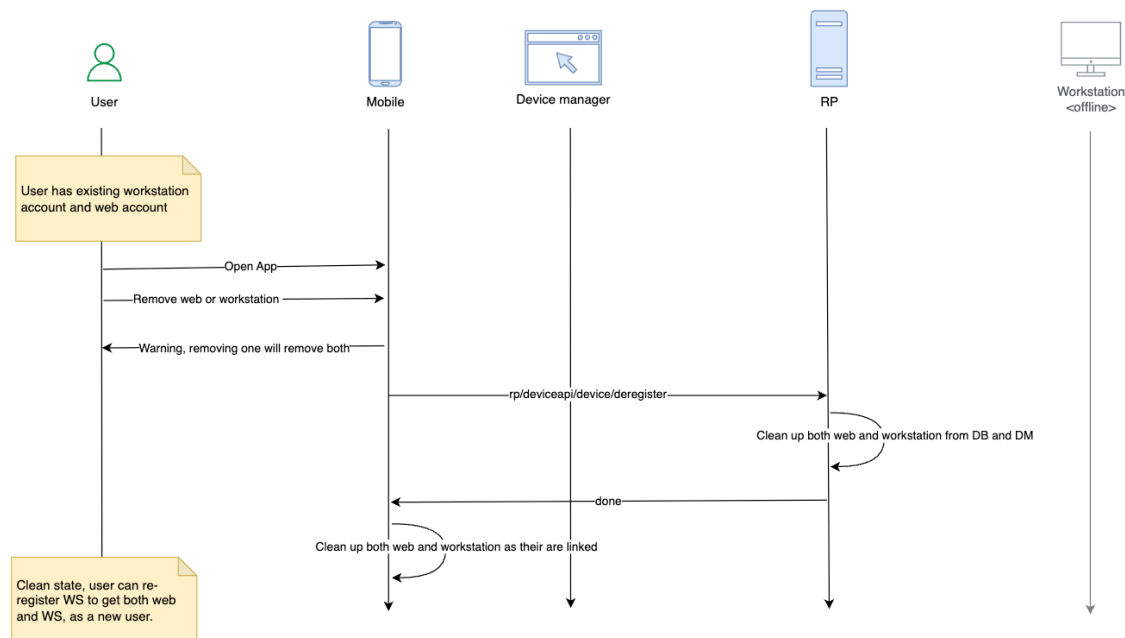
WS -> Web, new user





## 4. Deregistration Scenario

WS -> Web, user remove Web or Remove Workstation under SingleReg



## Configuration

1. Enable below listed FFs on Workstation rpApp level
  - a. WEB\_LOGIN\_WITH\_WFA\_REGISTRATION
2. Enable below listed FFs on Web apApp level
  - a. WEB\_TO\_WS\_SINGLE\_REGISTRATION\_TRANSLATION
  - b. RP\_APP\_WORKSTATION\_ENABLED
3. Upload AD CS domain CA certificate to HYPR CC
  - a. Login to AD CS and export the domain certificate in DER format (base64-encoded).
  - b. Make HYPR CC API Call to upload the certificate
    - i. API URL - `https://<HOST>/rp/api/domaincertificate`
    - ii. Request Type - POST
    - iii. Request Payload - `{"domainCertificate": "<Base64Encoded>"}`
    - iv. Authorization - Bearer <AdminToken>

```

None
curl
--location
--request POST "https://HOST/rp/api/domaincertificate"
--header "Authorization: Bearer hypap-edba607b-b400-4c57-9d3d-839a6e07a6f1"
--header "Content-Type: application/json"
--data '{
  "domainCertificate":
"MIIDczCCAlugAwIBAgIQS0n13f/8s5Np+dFMzF++0TANBgkqhkiG9w0BAQsFADBM-RMwEQYKCZImiZ
PyLGBGRYDdmV0MRcwFQYKCZImiZPyLGBGRYHaHlwcmxhYjEjEcMBoGA1UEAxMTaHlwcmxhYi1BRFNFU
lZFUi1DQTAeFw0yMjA4MTEyMzQ4MTZaFw0zMjA4MTEyMzU4MTVaMEwxEzARBgoJkiaJk/IsZAEZFgNu
ZXQxZzAVBgoJkiaJk/IsZAEZFgdoeXBybGFjMRwwGgYDVQQDEXNoeXBybGFjLUFUEU0VSVkVSLUNBMTI
BIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuDnPO/GZ1HeNMj1X+yDu46oK1x4mnC8aBDUwVl
pzcEv4heLuAWZT/dFVFKKZSNQxbAMubuNwFepySrgp7ThBVP4BGBq7b/LmjZJD9oeqpBhKnryIfYSqL
bxY3J2h5YtjQiR7nRr9iNyft+8I91yyhn95sdtNEyeENlyI+dz41bAj/PksJVtdxhI/ClnJTVSCHFid
42jcta0VKgfnmRfvvobX2r0pgmKhAYr9fNZ67TlZTTjji8Hz4vpQGm/9fiLKim4idAksTo1x/w0m0LS
baHTZ/qAUdType6aDDw1g9xap3cXPRX82Lstq/4CbhNZRHg1QfFMamghb6siX9KXOhQIDAQABo1EwTz
ALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUG9I0pL+oXX7m1k0KNqFPWb/hm
p0wEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQELBQADggEBAEGU/5V1evJKwTFaac6MnA02Pgwv
maer8Gycun4cAJbd9HUtenKcw8+oryojouniJ7Bm7NTrGPHDFgTxg1P9fdA8DE8nVCidCYiN3iJ0zQ5
v593eK08SxExEG0IcFve0Zf0uAXgtr2UkqTbP2K8RYUT5nTpjBXUMcQdH01fXYJ/cKqH25CiGqMwUQx
+aNWzc7/LT4nX9A9zMiwALD1IbTZ01zU7R8mt0A3IZCLJJvC19PdAcpqiHqAUnq8ojJN0neeANJyiXi
xedrTp6gxEpGWV7tR2NuYesnwjFtV2jV0VdcYVmDQVtqdpkxbx93re2IGhNq0+H0Pujtie2TTv7J4kE
="
}'

```

## Web to Workstation Single Registration

### Facts

- Web to Workstation Single Registration is a one way registration traffic which allows the user to initiate and complete the registration ceremony one time using browser web application interface. The user doesn't have to register explicitly to the desktop using HYPR WFA Client. Post this single registration ceremony, the user would be able to login to desktop and web applications.
- From the user's perspective, it is a one time registration experience, however from the backend's perspective, HYPR Server creates both desktop and web profiles.

## Pre-Requisites

1. Create and configure rpApp for Workstation.
2. Create and configure rpApp for all web applications which users would need to login without having to register explicitly for the web.
3. HYPR Enrollment Service Deployment and Configuration
4. HYPR WFA Client Installation (Optional)

## Configuration

1. Enable below listed FF on Global level
  - a. WINDOWS\_WEB\_ENROLLMENT
2. Enable below listed FFs on Web rpApp level
  - a. ASYNC\_REGISTRATION
  - b. WINDOWS\_WEB\_ENROLLMENT
  - c. RP\_APP\_WORKSTATION\_ENABLED
  - d. WEB\_TO\_WS\_SINGLE\_REGISTRATION\_TRANSLATION
  - e. VIRTUAL\_DESKTOP\_INFRASTRUCTURE
  - f. ENDPOINT\_API\_SECURITY\_TOKEN\_DEVICE (Enabled by Default)
  - g. ENDPOINT\_API\_SECURITY\_TOKEN\_WORKSTATION (Enabled by Default)
3. Enable below listed FFs on Workstation rpApp level
  - a. WINDOWS\_WEB\_ENROLLMENT
  - b. RP\_APP\_WORKSTATION\_ENABLED
  - c. VIRTUAL\_DESKTOP\_INFRASTRUCTURE
  - d. ENDPOINT\_API\_SECURITY\_TOKEN\_DEVICE (Enabled by Default)
  - e. ENDPOINT\_API\_SECURITY\_TOKEN\_WORKSTATION (Enabled by Default)

## HYPR Enrollment Service - Facts

- HYPR Certificate Enrollment Service is designed to manage authentication certificates for end users enrolling with the web application registration interface or Device Manager.
- When users add a new mobile device to the web application using the registration interface, HYPR CC Server queues up the certificate request.
- Enrollment Service is expected to interact with HYPR CC Server in terms of polling for pending cert requests and it sends back the encrypted certificate to the CC server.
- CC Server transports the certificate to the user's mobile device.

- Interaction of the Enrollment Service with the HYPR CC Server is controlled by FF (WINDOWS\_WEB\_ENROLLMENT).

## **HYPR Enrollment Service - Installation Requirement**

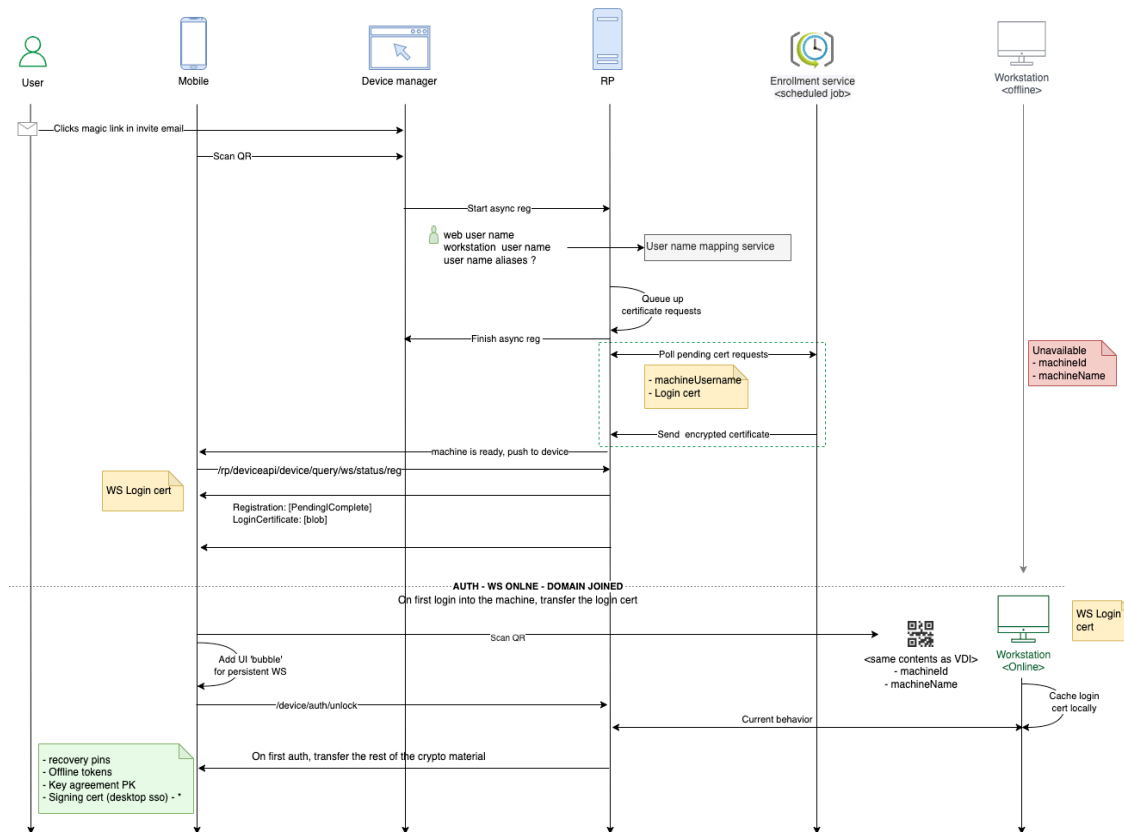
1. The Enrollment Service is distributed as an MSI installer package which has no user interface (HyprEnrollmentService\_x64.msi).
2. It can be installed on a Windows Server with network connectivity to Active Directory Certificate Services (AD CS).
3. Windows Server is required to have .NET Framework enabled.
4. It can't be installed on the Domain Controller or the AD CS server.
5. [HYPR Public Documentation Guide](#) could be referred for the steps to be followed for installation of the enrollment service.

## **Web To WS Single Registration Sequence Diagrams**

1. **New Web Profile Scenario - The user doesn't have any existing web profile.**



## Web -&gt; WS, new user



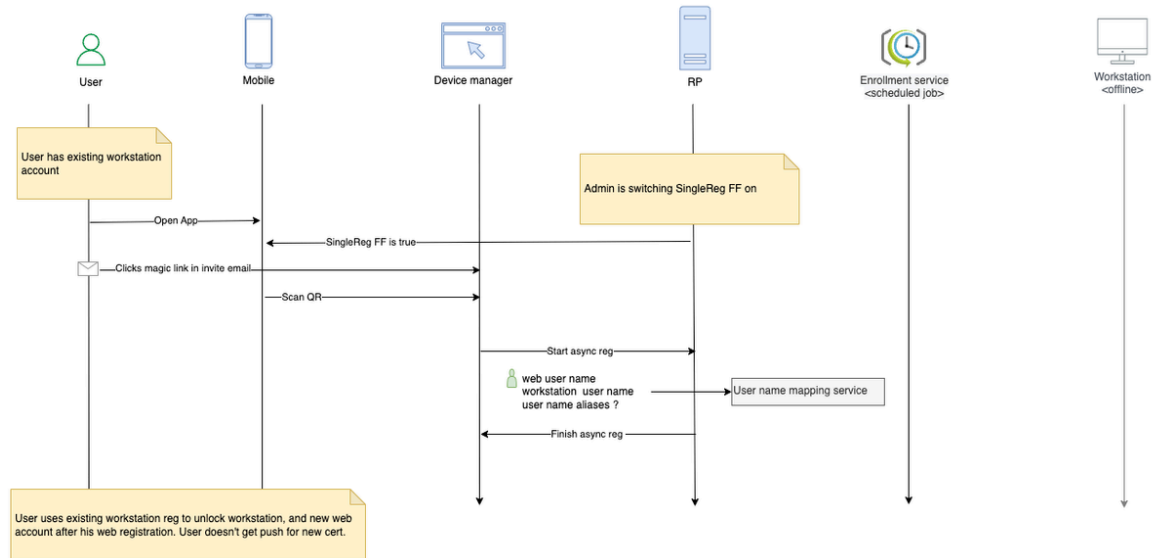
## 2. Existing Web Profile Scenario

```

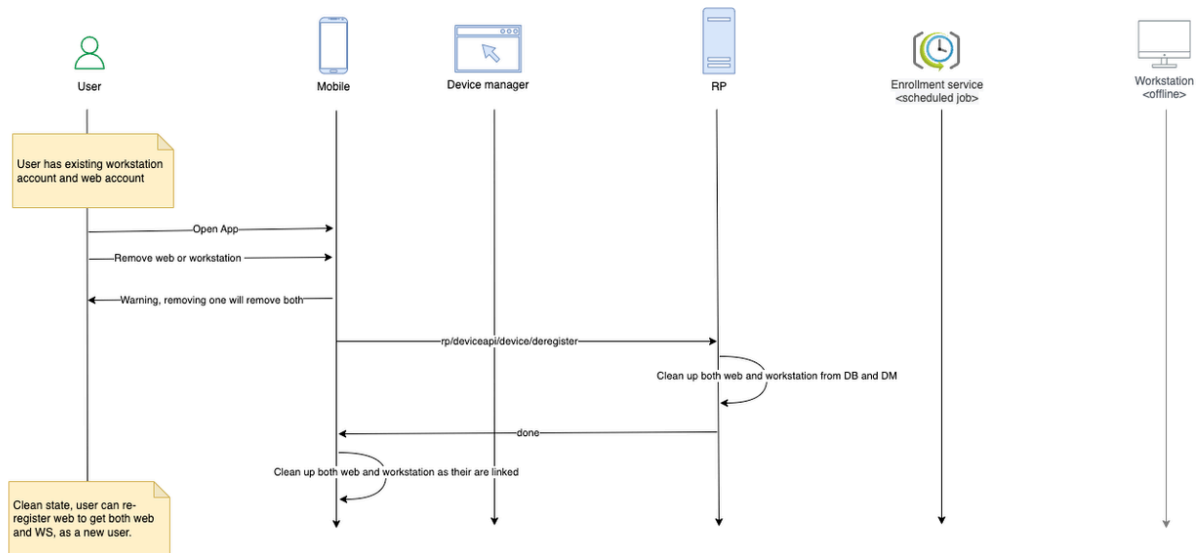
sequenceDiagram
    participant User
    participant Mobile
    participant Device manager
    participant RP
    participant Enrollment service as Enrollment service<br><scheduled job>
    participant Workstation as Workstation<br><offline>

    Note over User: User has existing web account
    User->>Mobile: Open App
    Note over Mobile: SingleReg FF is true
    Mobile->>RP: /p/deviceapi/device/query/ws/status/reg
    Note over RP: Admin is switching SingleReg FF on
    Note over RP: Queue up certificate requests
    Note over RP: Poll pending cert requests
    Note over RP: - machineUsername  
- Login cert
    Note over RP: Send encrypted certificate
    RP->>Mobile: Push to Device - Certificate is ready
    Note over Mobile: WS Login cert
    Mobile->>Device manager: Registration: [Pending/Complete]  
LoginCertificate: [blob]
    Note over Device manager: AUTH - WS ONLINE - DOMAIN JOINED  
On first login into the machine, transfer the login cert
    Device manager->>Workstation: Scan QR
    Note over Workstation: WS Login cert
    Note over Workstation: <same contents as VDI>  
- machineId  
- machineName
    Note over Workstation: Workstation<br><Online>
    Note over Workstation: Cache login cert locally
    Note over Mobile: Add UI 'bubble'  
for persistent WS
    Mobile->>RP: /device/auth/unlock
    Note over RP: Current behavior
    Note over Mobile: On first auth, transfer the rest of the crypto material
    Note over Mobile: - recovery pins  
- Offline tokens  
- Key agreement PK  
- Signing cert (desktop sso) - *
  
```

### 3. Existing Workstation Profile Scenario

**Web -> WS, user has existing workstation reg**

## 4. Deregistration Scenario

**Web -> WS, user remove Web or Remove Workstation under SingleReg**

## Testing the Workflow

1. HYPR CC Console could be leveraged to create a magic link for the web application.
  - a. Enter the user's email in the Username field. This is the same email address that is associated with the user profile on Active Directory.
  - b. Click Create Magic Link
2. The user could navigate to Magic link Web Link UR which would redirect the user to device manager.
3. The user selects 'Register mobile device' which makes a call to HYPR Server to initiate the web registration.
4. Wait a few minutes for server to process certificate
5. The User could tap on the Pending Computer bubble.
6. The user could scan QR code on the Windows lock screen to complete the WFA pairing.

## Deployment Strategy

1. **Customer has the existing footprint of passwordless login to desktop** - Workstation to Web single registration could be enabled so that web profiles would be created for all existing desktop profiles.
2. **Customer has the existing footprint of passwordless login to web application** - Web to Workstation single registration could be enabled so that workstation profiles would be created for all existing web profiles.
3. **Customer has no footprint - Both** Workstation to Web and Web to Workstation single registration could be enabled.

## Logs and Audit Trail

1. HYPR CC Console provides administrators with an Audit Trail mechanism for tracking events that flow through the HYPR components. [HYPR Public Documentation](#) could be referred for the details.
2. The Audit Trail events are stored in the HYPR database for a limited time. Customers can integrate their existing SIEM footprint with HYPR Server for permanent storage of these audit events.

AUDIT TRAIL

09:51:51 05 Feb 2024 - 10:51:51 05 Feb 2024

Type to search for Users, Machine IDs, Session IDs, Device IDs, and Trace IDs.

8

Show:

Results

20

Audit Trail data for Highlands Bank WS, HYPR Default Web Application, HYPR Default Workstation Application, Highlands Bank Web, Central Center Admin, HB0ktointAffirm001

<input type="checkbox"/>	Time	Username	Event	SubEvent	Status	Trace ID	Logged By
<input type="checkbox"/>	10:33:52 2/05/24	grace.hop...	AFFIRM APPLICATION CONFIGURATION CHANGED	/cc/ui/idv/configuration	Success	0a8c813c2...	RELYING_PART...
<input type="checkbox"/>	10:33:52 2/05/24	grace.hop...	AFFIRM APPLICATION CONFIGURATION CHANGED	/cc/ui/idv/configuration	Success	0a8c813c2...	RELYING_PART...
<input type="checkbox"/>	10:16:40 2/05/24	grace.hop...	AFFIRM APPLICATION CONFIGURATION CHANGED	/cc/ui/idv/configuration	Success	4405f9ac8...	RELYING_PART...
<input type="checkbox"/>	10:16:40 2/05/24	grace.hop...	AFFIRM APPLICATION CONFIGURATION CHANGED	/cc/ui/idv/configuration	Success	4405f9ac8...	RELYING_PART...
<input type="checkbox"/>	10:16:27 2/05/24	grace.hop...	AFFIRM APPLICATION CONFIGURATION CHANGED	/cc/ui/idv/configuration	Success	ea847e3e9...	RELYING_PART...