

Swish Online Payment Integration Guide with Wallmob

Swish Online Integration

Overview

This guide provides step-by-step instructions for setting up, configuring, and testing the **Swish Online** payment integration with Wallmob.

Swish Online enables merchants to accept online payments through Swish. The integration uses a secure merchant certificate issued by Swish to authenticate communication between Wallmob and the Swish payment service.

1. Prerequisites

Before configuring Swish Online, make sure you have the following:

- An active **Swish Handel / Swish e-commerce** agreement.
- Your **Swish merchant number (Swish Alias Number)**.
- A valid **Swish .p12 certificate**.
- The **certificate password**.
- Swish Online enabled for your Wallmob account.

2. Swish Online Configuration

Swish Online is configured through the Wallmob Backoffice.

Step 1. Enable Swish Online

Navigate to:

Master User → Configuration →

`Shared.Setting.Integrations.SwishOnline.Enabled`

Set the configuration to **Enabled**.

Step 2 – Open Integrations

1. Log in to **Wallmob Backoffice**.
2. Navigate to **Integrations**.
3. Select **Swish Online**.

Step 3 – Enter Swish Details

Enter the following information:

Field	Description
Swish Alias Number	Your Swish merchant number
Certificate File	The <code>.p12</code> certificate provided by Swish
Certificate Password	Password for the certificate

Step 4 – Upload the Certificate

Upload the `.p12` certificate provided by Swish.

The certificate is required to establish a secure connection between Wallmob and Swish.

Step 5 – Save the Configuration

After entering all required information:

1. Verify that the Swish Number is correct.
2. Verify the certificate file.
3. Verify the certificate password.
4. Save the configuration.

After successful configuration, the integration should be shown as **active/connected**.

3. Authentication

Swish Online uses **mutual TLS (mTLS)** authentication.

The merchant certificate is used to securely authenticate requests sent to Swish.

The authentication process is handled automatically after the integration has been configured.

You do not need to configure an API key or OAuth credentials.

Certificate Security

The certificate and certificate password are sensitive credentials.

Please ensure that:

- The certificate is stored securely.
- The certificate password is not shared with unauthorized users.
- Production certificates are not used in test environments.
- Test certificates are not used in production.

- Certificates are renewed before they expire.
-

4. Making a Payment

Once Swish Online has been configured, the consuming application can initiate Swish payment requests through Wallmob.

A payment request contains information such as:

- Payment reference
- Swish merchant number
- Amount
- Currency
- Payment message
- Callback URL

Example:

```
1 {  
2   "payeePaymentReference": "0123456789",  
3   "callbackUrl": "https://your-domain.com/swish/callback",  
4   "payeeAlias": "1231181189",  
5   "amount": "100",  
6   "currency": "SEK",  
7   "message": "Order #12345"  
8 }  
9
```

Callback URL

The callback URL is used to receive payment status notifications.

The callback endpoint must:

- Be publicly accessible.
 - Use HTTPS.
 - Be able to receive payment notifications from Swish.
 - Be implemented by the application consuming the payment service.
-

5. Testing

Testing should be completed using the **Swish test environment** before enabling the integration in production.

Step 1 – Configure Test Credentials

Configure the Swish Online integration using:

- Swish test merchant number.
- Swish test .p12 certificate.
- Test certificate password.

Step 2 – Verify Configuration

After saving the configuration:

1. Open the Swish Online integration.
2. Verify that the integration is active.
3. Verify that the Swish Number is correct.
4. Confirm that the certificate has been uploaded successfully.

Sensitive certificate information should not be displayed after configuration.

Step 3 – Create a Test Payment

Initiate a payment using the Swish test environment.

Verify that:

- The payment request is accepted.
- The expected payment status is returned.
- The payment callback is received.
- The payment status is correctly updated in the consuming application.

6. Test Scenarios

The following scenarios should be tested before moving to production:

Scenario	Expected Result
Valid Swish Number	Configuration is saved successfully
Valid certificate	Certificate is accepted
Valid certificate password	Integration becomes active
Valid payment request	Payment request is accepted
Payment callback	Callback is received successfully
Invalid Swish Number	Appropriate error is returned
Invalid certificate	Authentication fails

Incorrect certificate password	Authentication fails
Expired certificate	Authentication fails
Update Swish Number	Existing certificate remains configured