imprivata®

Product Documentation

Temporary Codes

Imprivata Enterprise Access Management 24.2

NOTE:
Beginning with 24.2, Imprivata OneSign and Imprivata Confirm ID have been renamed to Imprivata Enterprise Access Management.

Some interfaces in the Imprivata Admin Console, Imprivata Appliance Console, and documentation may retain the older Imprivata OneSign and Imprivata Confirm ID product names.

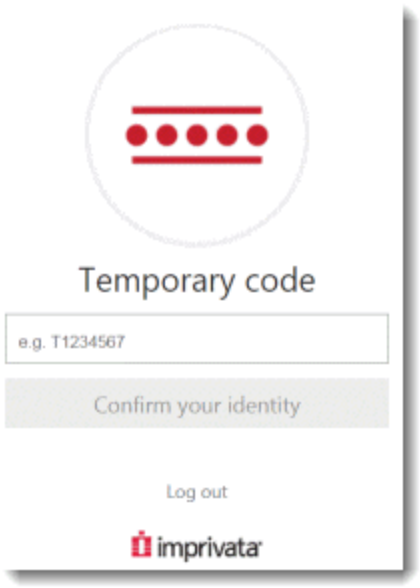
When Imprivata ID authentication is required to log in, but the user doesn't have his device or OTP token, Imprivata has made it easy for your enterprise to issue a temporary code allowing your user to continue their work virtually uninterrupted. Temporary codes can also be used when you need to provide remote access to a temporary user such as a contractor.

This document contains the following sections:

About Temporary Codes

In a typical Imprivata two-factor authentication workflow, the user must enter his password, then complete a second factor authentication via Imprivata ID, SMS code, or OTP token. If he doesn't have his device or token, he cannot log in. If he contacts your enterprise's helpdesk, you can issue him a temporary code:

1. The user contacts your help desk to report his device or OTP token was misplaced or stolen.
2. Your helpdesk verifies the user's identity and generates a temporary code with an expiration date.
3. The user logs in, using the temporary code when prompted (see image below).



He can use the temporary code until:

- The code expires
- He enrolls an Imprivata ID, phone number, or OTP token via the Imprivata agent
- He resumes using his typical second factor: Imprivata ID, SMS code, or OTP token authentication.

When Temporary Codes Can Be Used

Temporary codes are only available for Remote Access and Imprivata ID for Windows Access. Temporary codes cannot be used for order signing or any other Imprivata workflow.

Set Up Administration

By default only a superadministrator can:

- Enable or disable the temporary code feature for all eligible users in your enterprise
- Generate or revoke a temporary code for a user

To enable these for other administrators:

1. In the Imprivata Admin Console, go to the **gear icon** > **Administrator roles**.
2. Select an administrator role or add a role that will be allowed to generate and revoke temporary codes.
3. In the section **Properties**, select **Enable/disable temporary codes**.
4. In the section **Users**, select **Generate/revoke temporary codes**.
5. Complete configuration of this administrator role as needed.
6. Click **Save**.

For more information on Administrator roles, see "Administrator Roles (Delegated Administration)" in the Imprivata Online Help.

BEST PRACTICE: Imprivata has no role in verifying the identity of persons who contact your helpdesk to report their device has been misplaced or stolen. It is your enterprise's prerogative to ensure people who contact your helpdesk are who they say they are before you issue them a temporary code.

Enable Temporary Codes for Your Enterprise

Temporary codes are disabled for your enterprise by default:

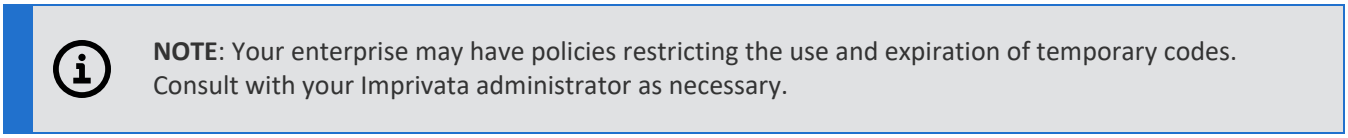
1. In the Imprivata Admin Console, go to the **gear icon** > **Settings**.
2. In the **Temporary Codes** section, click the checkbox **Allow Temporary Codes**.
3. Click **Save**.

Best Practice: When A User Misplaces Their Device

When a user reports she's misplaced her device, issue a temporary code and select an expiration that allows her sufficient time to recover the device:

1. Ask the user if she uses her device to log in remotely or access Windows (Temporary codes can't be used to sign orders.)
2. Look up the user in the Imprivata Users list: In the Imprivata Admin Console, go to **Users** > **Users** and find the user on the list.
3. On the User details page go to **Temporary Code** > **Generate Code**.
4. Talk to the user and determine how long it will take her to recover her misplaced device.
5. Select **Use Multiple times** and select an **expiration** that allows her to log in with the temporary code until she recovers her device.
6. Click **Generate code**.

7. Communicate the temporary code to the user, and tell her:
   - The code expires on (read the date and time off the screen)
   - The code only works for her Imprivata account. It won't work for any other users.
   - The code cannot be used to sign orders.
   - Log in and enter the temporary code where prompted onscreen.
   - After she recovers her device, she can begin using it again to log in immediately. She does not have to contact the helpdesk again.
8. After you click **Done**, the code is hidden from view and cannot be viewed again.



NOTE: Your enterprise may have policies restricting the use and expiration of temporary codes. Consult with your Imprivata administrator as necessary.

Best Practice: When A User's Device Is Stolen

When a user reports her device is lost or stolen, you must delete their enrollment in Imprivata ID and SMS code authentication to prevent unauthorized use of their credentials. Issue a temporary code, and select an expiration that allows her sufficient time to replace her device and enroll Imprivata ID or her phone number again:

1. Ask the user if she uses her device to log in remotely or access Windows (Temporary codes can't be used to sign orders.)
2. Look up the user in the Imprivata Users list: In the Imprivata Admin Console, go to **Users** > **Users** and find the user on the list.
3. In the section **Authentication Methods**, select **Delete Enrollment** for her Imprivata ID and SMS code.

   > **CAUTION**: If the user is a clinician who also uses her Imprivata ID to sign orders: after you click **Save** in the next step, she will not be able to use her Imprivata ID to sign orders until she acquires a device and re-enrolls Imprivata ID.

4. Click **Save**.
5. Go to **Temporary Code** > **Generate Code**.
6. Talk to the user and determine how long it will take her to replace her device and re-enroll her Imprivata ID and/or phone number.
7. Select **Use Multiple times** and select an **expiration** that allows her to log in with the temporary code until she replaces her device and re-enrolls.
8. Click **Generate code**.
9. Communicate the temporary code to the user, and tell her:
   - The code expires on (read the date and time off the screen)
   - The code only works for her Imprivata account. It won't work for any other users.
   - The code cannot be used to sign orders.
   - Log in and enter the temporary code where prompted onscreen.
   - After she acquires a new device, she must install the Imprivata ID app and enroll it, or re-enroll her phone number for SMS code authentication.
   - If she recovers the device that was stolen, she won't be able to use Imprivata ID again until she enrolls again, or she must re-enroll her phone number for SMS code authentication.
10. After you click **Done**, the code is hidden from view and cannot be viewed again.

> **NOTE**: Your enterprise may have policies restricting the use and expiration of temporary codes. Consult with your Imprivata administrator as necessary.

Best Practice: Provide Remote Access To Users With Password Only

There are some cases where you want to provide a temporary code to a user who will never enroll an Imprivata ID:

- The user is a temporary worker who should not enroll an Imprivata ID; and
- The user is logging in remotely, and Confirm ID Remote Access requires Imprivata ID authentication; and/or
- The user is logging into a workstation on premises that requires Imprivata ID for Windows Access.

In one of these scenarios, you can issue her a temporary code to use as her second factor.

BEST PRACTICE: Because this user will only ever authenticate with her password and a temporary code, place her in a user policy separate from your permanent employees. Temporary contractors should not be allowed to enroll any authentication methods.

1. Look up the user in the Imprivata Confirm ID Users list: In the Imprivata Admin Console, go to **Users** > **Users** and find the User on the list.
2. On the User details page go to **Temporary Code** > **Generate Code**.
3. Select **Use Multiple times** and select an **expiration** after she no longer needs to log in remotely. The maximum is **14 days**, after which the code will expire and the user would need to enroll a second authentication method or request a new temporary code.
4. Click **Generate code**.
5. Communicate the temporary code to the user, and tell her:
   - The code expires on (read the date and time off the screen)
   - The code only works for her Imprivata account. It won't work for any other users.
   - The code cannot be used to sign orders.
   - Log in and enter the temporary code where prompted onscreen.
6. After you click **Done**, the code is hidden from view and cannot be viewed again.

NOTE: Your enterprise may have policies restricting the use and expiration of temporary codes. Consult with your Imprivata administrator as necessary.

Frequently Asked Questions

The Temporary Code section is absent from the user details page!

If the **Temporary Code** section is absent, then this user is not eligible to use a temporary code. They may not be configured for the Remote Access workflow or Imprivata ID for Windows Access: ask the user if she uses her device to log in (Temporary codes can't be used to sign orders.)

The Temporary Code section is present but I cannot generate a code!

If the **Temporary Code** section is visible but the **Generate Code** link is absent, then your administrator role is not enabled to generate them. Contact your Imprivata administrator.

How do I know if a user is eligible for a temporary code?

Temporary codes are available for users in user policies associated with the Imprivata Confirm ID Remote access workflow or Imprivata ID for Windows Access. Find the user in the Imprivata Admin Console database and view the user details page:

- If the **Temporary Code** — **Generate code** link is available, the user is eligible to use a temporary code.
- If you see the message **Temporary codes are disabled for this enterprise**, they must be enabled for the whole enterprise before a code can be generated for a user. Contact your Imprivata administrator.
- If the **Generate Code** section is visible but the **Generate Code** link is absent, your administrator role is not enabled to generate temporary codes. Contact your Imprivata administrator.

What do I do if a user reports they've misplaced their device?

Generate a temporary code for the user. See Best Practice: When A User Misplaces Their Device.

What do I do if a user reports their device is lost or stolen?

Delete their Imprivata ID enrollment and phone number, and generate a temporary code for the user. See Best Practice: When A User's Device Is Stolen.

What happens when a user finds their misplaced device?

The user can resume using Imprivata ID or SMS codes at any time. They don't need to contact your helpdesk again. If you generated a temporary code for the user, it is automatically deleted.

What happens when a user finds their lost/stolen device?

You cannot "undo" a deleted enrollment. If her device wasn't lost or stolen after all, she must still re-enroll Imprivata ID and/or her phone number. If the user is a clinician who also uses Imprivata ID for order signing, she must complete identity proofing and re-enroll Imprivata ID.

What happens when a user replaces their lost/stolen device?

The user must re-enroll Imprivata ID and/or their phone number. If the user is a clinician who also uses Imprivata ID for order signing, they must complete identity proofing and re-enroll Imprivata ID.

What happens when the user begins using Imprivata ID or SMS codes again?

The user can resume using Imprivata ID or SMS codes at any time. They don't need to contact your helpdesk again. If you generated a temporary code for the user, it is automatically deleted.

How do I enroll a contractor for one day?

Generate a temporary code as described above and set the expiration for **24 hours**. See Best Practice: Provide Remote Access To Users With Password Only.

How do I revoke a temporary code?

If for any reason you want to stop a user from using their temporary code, go to their user details page and click **Revoke code**, and **Save**.

What if a user forgets their temporary code? How do I replace/re-generate a new code?

A temporary code can be replaced with a new one at any time. Go to their user details page and click **Replace code**.

How do I enroll a remote person securely?

Imprivata Confirm ID users can enroll Imprivata ID and their phone number remotely by providing their username and password only. For added security during remote enrollment, you can generate a temporary code for each user and place them in a user policy that allows remote enrollment but requires two-factor authentication when logging in remotely. In this scenario, they would enter their username, password, and temporary code before they could remotely enroll Imprivata ID or their phone number. See "Configuring Imprivata Confirm ID Remote Access" in the Imprivata Online Help.

My Remote Access users are logging in with password only.

If you delete the Imprivata ID or phone number enrollment of a Remote Access user, you may inadvertently return them to a state where they can log in remotely with password only **and** delay enrolling indefinitely.

Review your Remote Access workflows and Enroll Delay options. After a user replaces a stolen device, move them to a user policy where they cannot delay enrolling. See "Configuring Imprivata Confirm ID Remote Access" in the Imprivata Online Help.