# Signed Workflows

Last Modified on 09/26/2019 7:11 am EDT

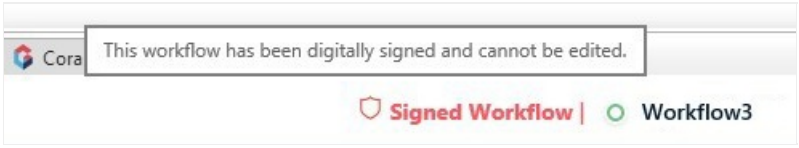
## Overview

You can protect your workflow with a digital certificate to verify the authenticity of the workflow. Signing a workflow is useful to ensure that the workflow is executed as it was originally designed, and that it cannot be modified.

To sign a workflow, you need to obtain or create a digital certificate. Digital certificates enable you to securely exchange digital data, protect the authenticity of a file, and verify its ownership. When you protect your workflow with a digital certificate, only someone with the matching certificate's public key can import and execute the signed workflow.

**NOTE**
All certificates must be issued by a certificate authority (CA).
For more details on how to obtain a valid certificate, contact your IT Department.

Signed workflows display a "Signed Workflow" label next to their name, and open in read-only mode.




When you open a signed workflow, you can only make the following changes:

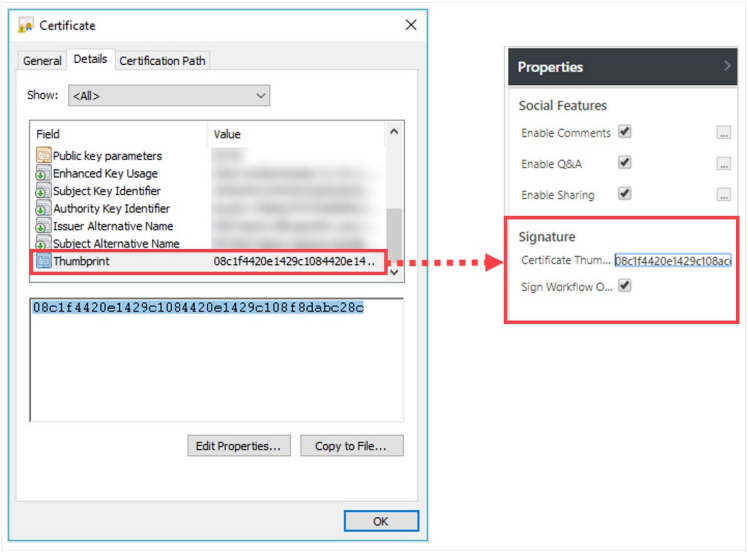
- Change permissions
- Edit lookup tables

**IMPORTANT**
If the workflow is tampered with, that is, changes are applied not through the App Studio, the signature breaks and **workflow execution fails**.

## Signing a workflow

1. Configure the signature properties.
    a. In the App Studio, click anywhere on the workflow canvas, and in the Properties pane, under **Signature**, select **Enable Signature on Export**.
    b. Enter the digital certificate's *thumbprint*.
    Make sure that the copied thumbprint does not include hidden characters, such as spaces, and other paragraph tags.

    **Example**




**NOTE**
The signature applies to a specific workflow version. If you duplicate the workflow, the signature properties are not duplicated.

## Exporting the workflow

The digital signature takes effect *only* when the workflow is exported. You can make any changes to the workflow before you export it, but not after it has been exported.

Before you export the workflow, make sure that:

- The Application Pool Account user that accesses the Administration site has *read* rights for the certificate's private key.
  For details, see this page.
- You have entered the correct certificate's thumbprint.
- The server where the workflow is created has a valid certificate located in the *Personal* folder of the Certificate store and contains the certificate's private key.

If one or more of the conditions above are missing, the export process fails.

## Importing and executing the signed workflow

When you import a signed workflow, make sure that the server to which the workflow is imported includes the public key of the same certificate that was used to sign the workflow.

The certificate should be located in the Certificate's store Personal folder.

If a matching certificate is missing, you cannot import, open, or execute the signed workflow on the server.

**IMPORTANT**
In case the workflow signature breaks as a result of changes made to the originally signed workflow, and the authenticity of the workflow cannot be verified, the **runtime execution of the workflow fails**. In such cases, you need to import or restore the originally signed workflow.

If you need to make changes to a signed workflow, it is **highly recommended** to create a new version of the workflow, and import it as a new workflow.