End users must enter this activation code in a text box of the dialog box.

- If the CT-KIP URL includes an activation code, instruct end users that they need not enter a value in the **Password or Activation Code** text box in the Install Software Token dialog box.

Create a Virtual Smart Card

To use the derived credentials feature, you must create a virtual smart card to use when you log in to a server and connect to a remote desktop. One virtual smart card can hold multiple certificates.

Prerequisites

- Verify that the client device, remote desktops, RDS hosts, Connection Server host, and other Horizon components meet the smart card authentication requirements. See Smart Card Authentication Requirements.

- Use the Purebred app to create a derived credential and provision the credential on the client device.

- Verify that the device has a passcode. A passcode is required to create a virtual smart card.

Procedure

1   Tap **Settings** at the bottom of the Horizon Client window.

2   Tap **Derived Credentials** and then tap **Create New Virtual Smartcard**.

3   Perform device authentication.

   - If either Touch ID or Face ID is enabled, authenticate with Touch ID or Face ID.

   - If neither Touch ID nor Face ID is enabled, authenticate with a passcode.

4   Enter and confirm a PIN for the virtual smart card.

5   Tap **Continue** and import the derived credential from the Purebred key chain.

   a   Tap **PIV Authentication Certificate**.

   b   Select the **Purebred Key Chain** location.

   c   Select the certificate to import.

6   (Optional) To import a digital signature certificate or encryption certificate after you import the PIV authentication certificate, tap **Digital Signature Certificate** or **Encryption Certificate** and follow the prompts.

7   To create the virtual smart card, tap **Done**.

   The derived credential appears in the **Settings** window. The **Use Derived Credentials** setting is set to on.

8   To create another virtual smart card for a different Horizon environment, tap **Create new virtual smartcard** and repeat these steps.

What to do next

Pair a Virtual Smart Card with Smart Card Middleware.

Manage a Virtual Smart Card

You can reset the PIN for a virtual smart card in Horizon Client. You can also delete a virtual smart card. After you log in to a remote desktop with a virtual smart card, you can also use the Charismathics Security Token Configurator in the remote desktop to view the certificate and key, manage, and change the user PIN for the virtual smart card.

Prerequisites

Create a Virtual Smart Card.

Procedure

◆ To reset the PIN for a virtual smart card, perform these steps.

    a   Tap **Settings** at the bottom of the Horizon Client window.

    b   Tap **Derived Credentials**.

    c   Tap the virtual smart card.

    d   Tap **Reset PIN**.

    e   Enter the current PIN, enter and confirm the new PIN, and tap **Done**.

◆ To remove a virtual smart card, perform these steps.

    a   Tap **Settings** at the bottom of the Horizon Client window.

    b   Tap **Derived Credentials**.

    c   Touch the virtual smart card, slide your finger to the left, and tap **Delete**.

Configure Device ID Sharing with OPSWAT

If OPSWAT Mobile App is installed on the client device, you are prompted to share the client device ID when you start Horizon Client. You can also enable or disable device ID sharing by configuring a setting in Horizon Client.

Prerequisites

Configure OPSWAT integration. See OPSWAT Integration Requirements.

Procedure

1   Tap **Settings** at the bottom of the Horizon Client window and tap **Share Device ID with OPSWAT**.