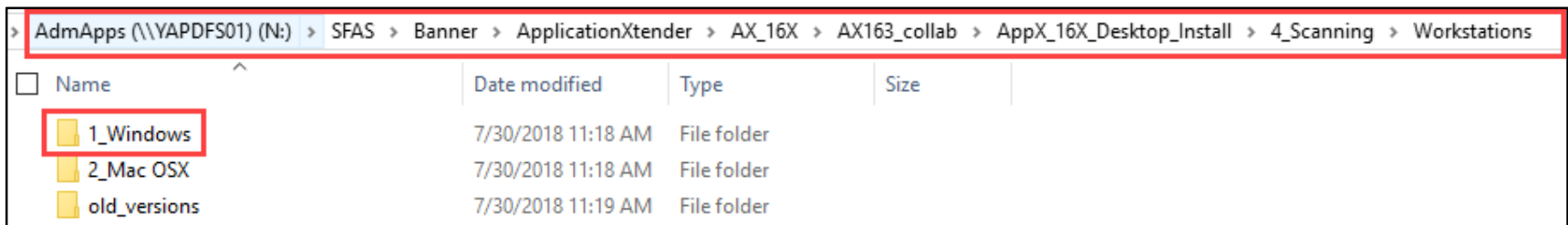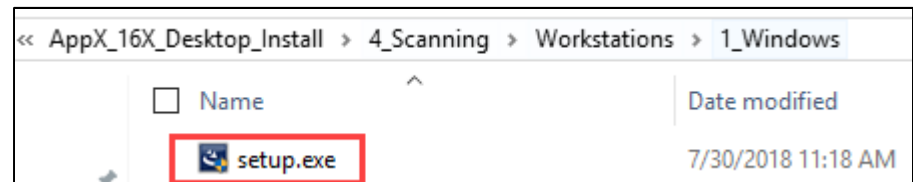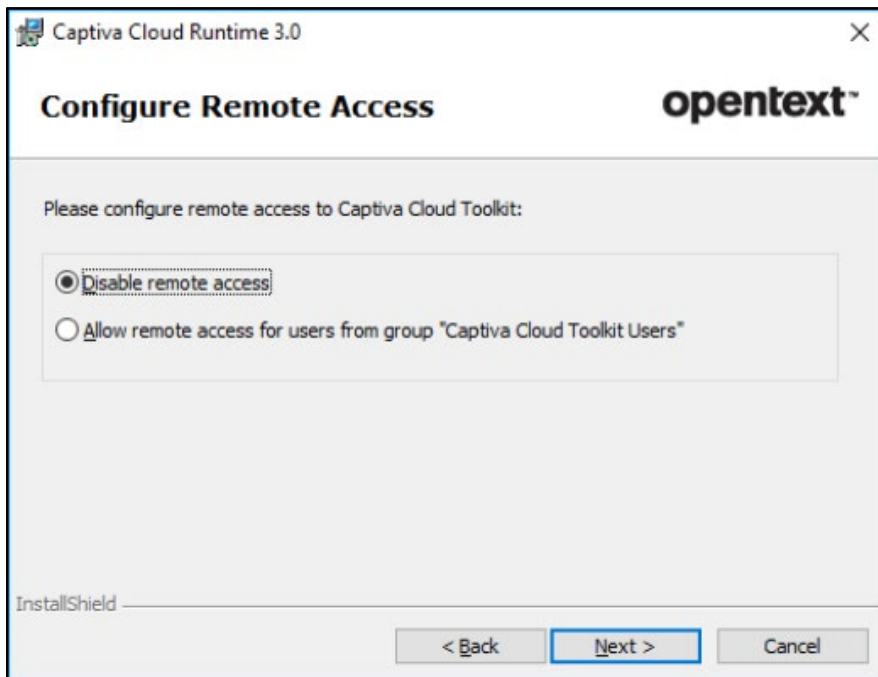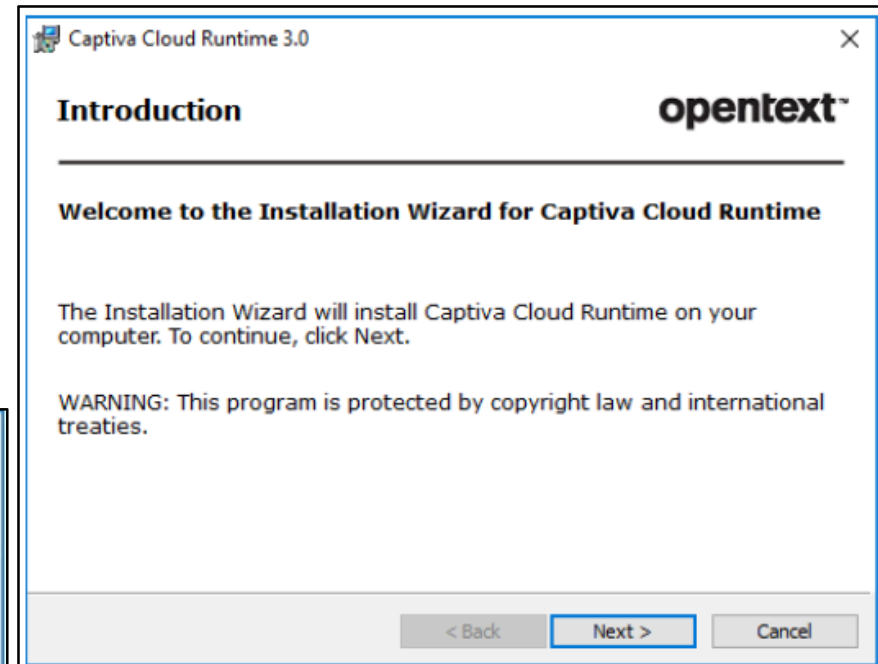# Scanning networks
Toolkit Installation

1. Click and go to **N: ApplicationXtender Desktop Install Scanning Workstations.**

2. Select the **1_Windows** folder and double-click to open it.

3. With *Administrator privileges* you can double-click and run **setup.exe**.

Revised: 3/23/2020 Note: Made corrections for typos.

4   The installation begins to run, click **Next**.

.   Accept the terms of the EULA, click **Next**.

5   In Configure Remote Access select
    Disable Remote Accessand click **Next**.
.

7. Click **Next**again.
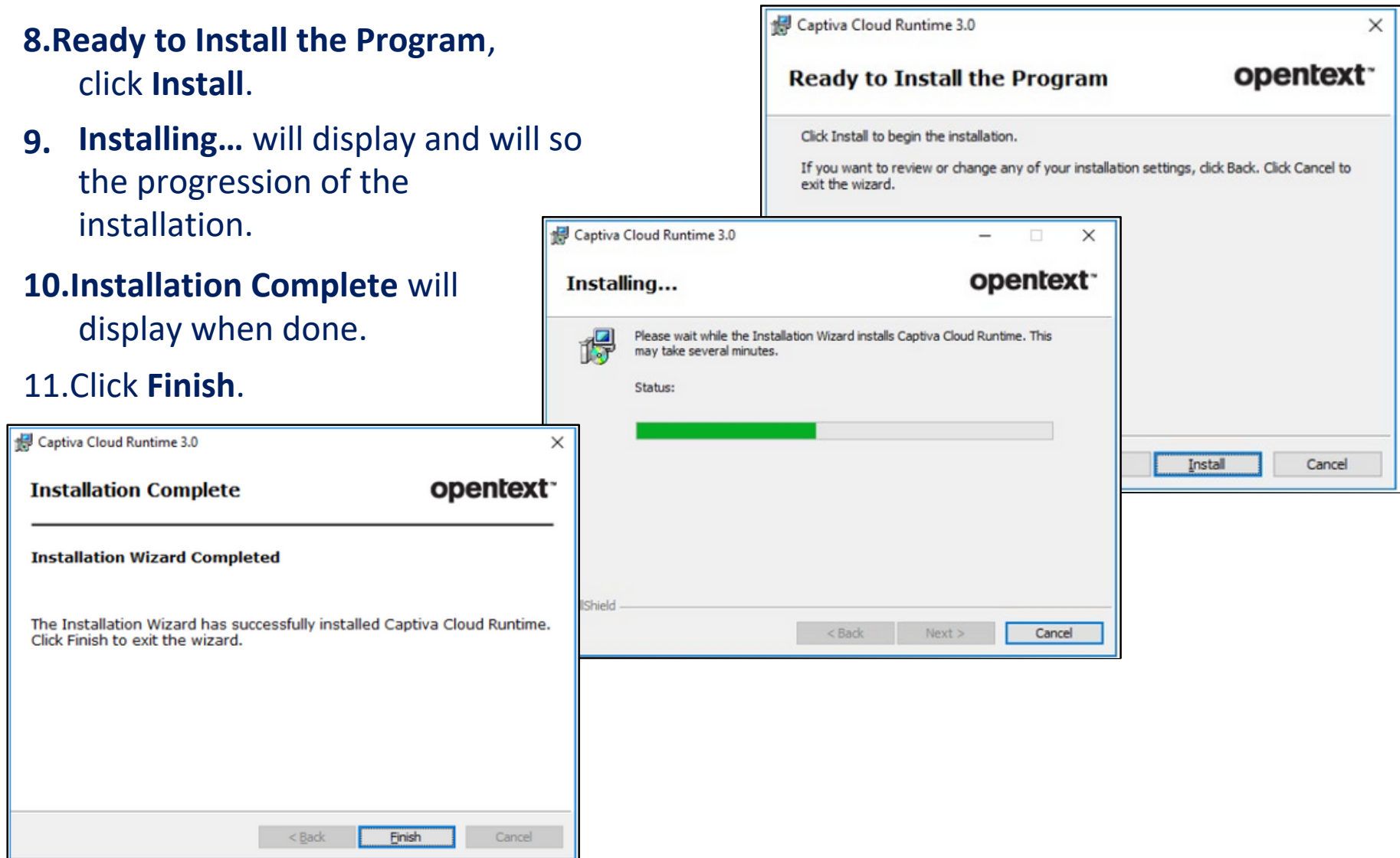
.

8. Ready to Install the Program, click **Install**.

9. Installing… will display and will so the progression of the installation.

10. Installation Complete will display when done.
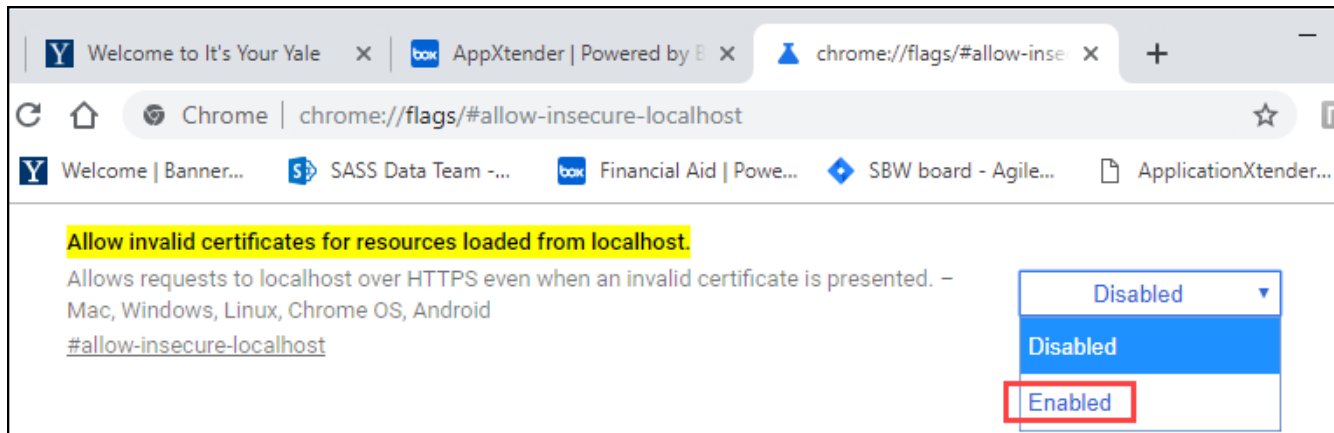
11. Click **Finish**.

Firefox and Chrome (the preferred browsers for AppXtender) are finicky about communicating with the Captiva Cloud toolkit. This is a known issue that Ellucian is working with OpenText.

The browser does not want to allow communication with the Captiva Cloud

Toolkit/runtime, which runs as a service on the user's machine. Some other institutions have reported that this problem is only seen when the AppXtender site is running as https instead of http.
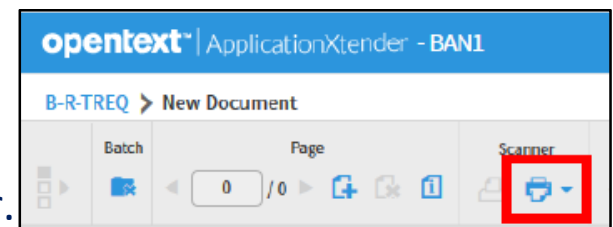
Technical Info: By default, the Captiva Cloud Service is configured to start automatically

when the computer starts. When the service starts, it scans for available TCP network ports that your application can use to communicate with the local web capture server. The server listens on port 49732, 49733, or 49734 for HTTP and on port 49735, 49736, or 49737 for HTTPS. If none of the ports are available, then an error is logged in the Windows System event log.

Ellucian Support Workaround: The browser exceptions provided must be applied on a per

user-basis on your local computer. If you change computers or your computer is re-imaged you will have to run the workaround again.

1. Log into the computer as the user who will be doing the scanning.
. Open a session of the Chrome browser.
2. Enter this URL in the Chrome address bar: **chrome://flags/#allow-insecure-localhost**.
3/4. Chrome will highlight and bring you to the **Allow invalid certificates for resources loaded from local host** flag.
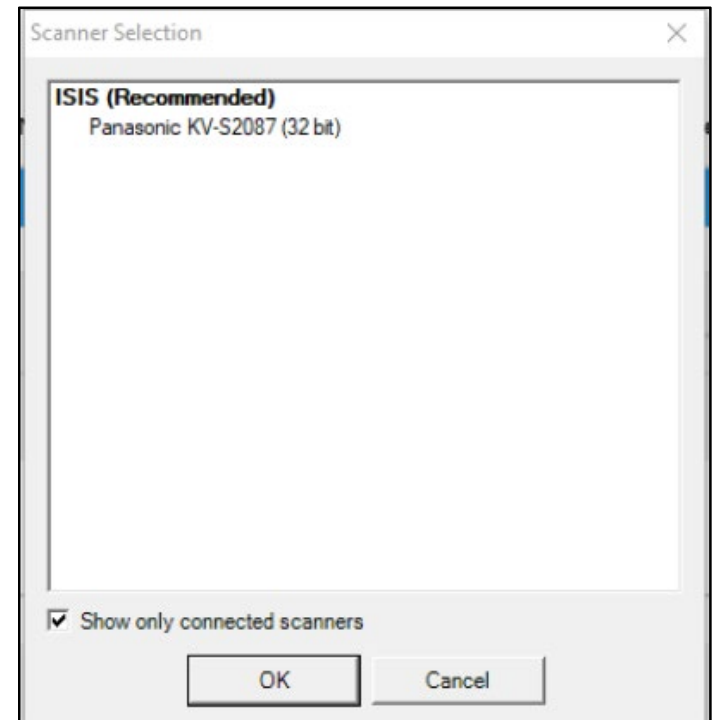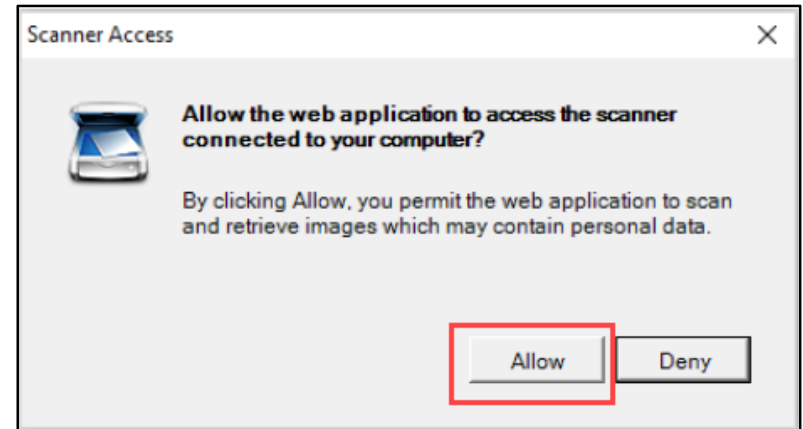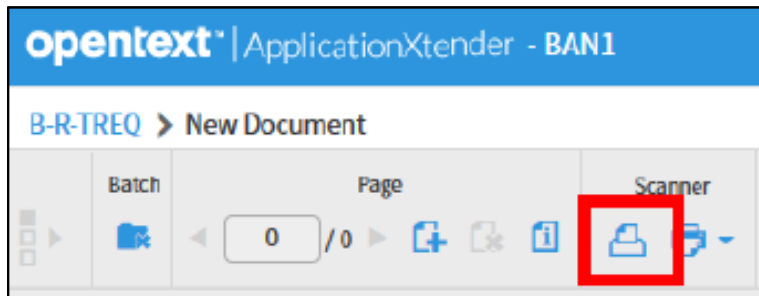5. Using the drop-down menu change the status to **Enabled**.

6. Now login to AppXtender via Chrome.
7. The **Select Scanner** button should now be enabled in AppXtender.
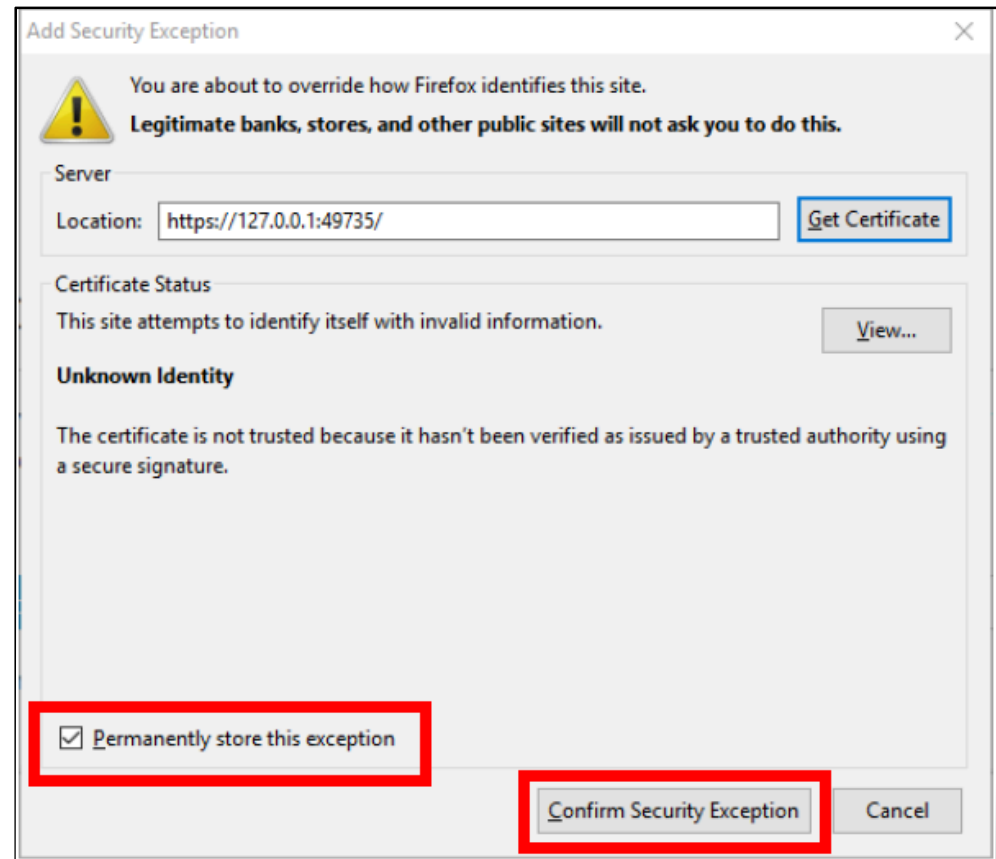8. Click the **Select Scanner** button to connect to the scanner.

Chrome Workaround continued

9. The Scanner Access dialog box will display **Allow the web application to access the scanner connected to your computer?**

10. Click **Allow**.

11. The Scanner Selection dialog will display. Select your scanner and click **OK**.

12. AppXtender will access the scanner and return to the application window with the **Scan**button enabled.

13. Now load your documents into the scanner and click the **Scan**button.

1. Log into the computer as the user who will be doing the scanning.

2. Open a session of the Firefox browser.

3. Enter this IP in the Firefox address bar: https://127.0.0.1:49735/

4. Firefox will display a message box warning **Your connection is not secure**. This is normal.

5. Click the **Advanced** button.

6. Click **Add Exception** and the **Add Security Exception** dialog opens.

7. Check the **Permanently store this exception** option.

8. Click **Confirm Security Exception**.

9. Now login to AppXtender via Firefox.

Firefox Workaround continued

10. The **Select Scanner** button should now be enabled in AppXtender.

11. Click the **Select Scanner** button to connect to the scanner.

12. The Scanner Access dialog box will display **Allow the web application to access the scanner connected to your computer?**

13. Click **Allow**.

14. The Scanner Selection dialog will display. Select your scanner and click **OK**.

15. AppXtender will access the scanner and return to the application window with the **Scan**button enabled.

16. Now load your documents into the scanner and click the **Scan**button.