Technical Document

Niagara Touch Guide

August 20, 2021

Niagara Touch Guide

Tridium, Inc.
3951 Westerre Parkway, Suite 350
Richmond, Virginia 23233
U.S.A.

Confidentiality

Trademark notice

Copyright and patent notice

Contents

About this guide **5**
Document change log 5
Related documentation 5

Chapter 1 Niagara Touch display **7**
Prerequisites 7
Unpacking 7
Getting started 8
Setting the locale 8
Connecting to a source attached to a router 9
Configuring general settings 12
Configuring sources 14
Managing configured sources 17
Connecting to a Wi-Fi source 23
Connecting to an Ethernet source 26
Connecting to an Ethernet source with Static IP enabled 28

Chapter 2 Security **33**
Files 33
Creating and exporting the client certificate 33
Setting up authentication 35
Setting up a display user 36
Exporting the certificate with its private key (Niagara 4.9) 39
Preparing the .p12 server certificate 40
Installing the .p12 certificate 40

Chapter 3 Workbench Configuration **43**
Setting up a navigation file 43
Creating a role to assign to the display 44
Updating the user assigned to the display 45

Chapter 4 Reference **47**
General Settings 47
Date & time 48

Index **51**

About this guide

This topic contains important information about the purpose, content, context, and intended audience for this document.

Product Documentation

This document is part of the Niagara technical documentation library. Released versions of Niagara software include a complete collection of technical information that is provided in both online help and PDF format. The information in this document is written primarily for Systems Integrators. To make the most of the information in this book, readers should have some training or previous experience with Niagara software, as well as experience working with JACE network controllers.

Document Content

This document describes how to set up and configure the Niagara Touch display.

Document change log

Changes to this document are listed in this topic.

August 20, 2021

Added display information.

June 21, 2021

Initial release

Related documentation

These documents contain related information.

- *Niagara Enterprise Security Installation and Maintenance Guide*

Chapter 1 Niagara Touch display

Topics covered in this chapter

- ♦ Prerequisites
- ♦ Unpacking
- ♦ Getting started
- ♦ Setting the locale
- ♦ Connecting to a source attached to a router
- ♦ Configuring general settings
- ♦ Configuring sources
- ♦ Managing configured sources
- ♦ Connecting to a Wi-Fi source
- ♦ Connecting to an Ethernet source
- ♦ Connecting to an Ethernet source with Static IP enabled

The mobile Niagara Touch display locks down the browser to a specific URL. This general-purpose display has multiple uses, such as serving as an intrusion zone arming and disarming keypad for Niagara Enterprise Security. Client certificate authentication automatically logs in the display to a controller station. This section sets up a Niagara Touch display with a client certificate and connects it to a controller station. The display runs the Android operating system.

Standard tools and certificate authentication support the display. You can create a Px view of an onscreen application and install it on the display.

NOTE: Assigning a user certificate requires the **FoxService** and **WebService** to restart. To avoid disrupting daily operations, configure a new Niagara Touch display after hours.

Prerequisites

To install and configure the Niagara Touch display your configuration needs these prerequisites.

- Up to a 4GB USB thumb drive
- Up to an 8GB MicroSD card

These components must not exceed these sizes.

Unpacking

The unit ships in a protective box.

Prerequisites: You received the unit.

Step 1 Unpack the unit and apply the Tamper Proof Flush Mount to the Display.

Step 2 Plug in a power source.

Step 3 Determine your preferred communication method: Ethernet or WiFi.

Step 4 If Ethernet is your preferred communication method, connect the Ethernet cable to the display and network.

Getting started

Once you assemble the display, connect it to a power source and decide on your preferred communication method, it is time to power up the display.

Step 1 Press the power button once quickly and release.

The battery indicator should appear on the screen.

Step 2 Press the power button again and hold it on.

The battery indicator disappears and a screen with four x penguins appears.

Step 3 Release the power button.

The display powers up.

Step 4 To power down or reboot the display at any time, press and hold the power button until a popup window opens with the options to power down or reboot.

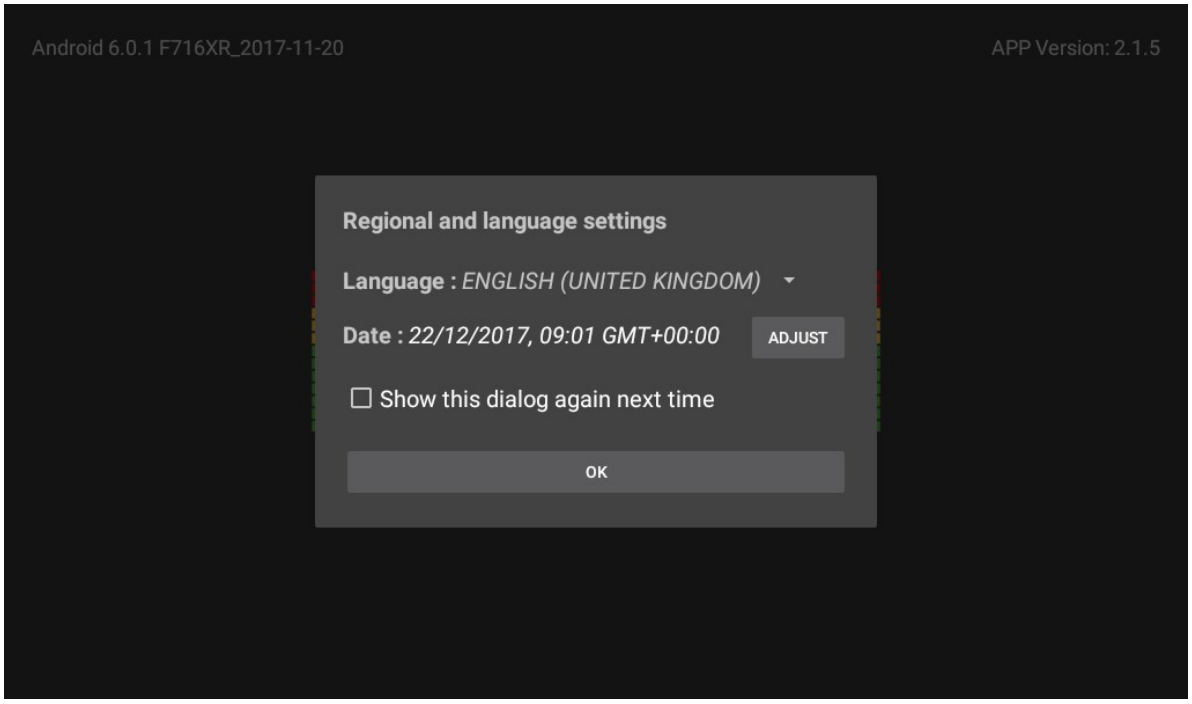
Setting the locale

Regional and language settings configure the locale in which you intend to use the display.

Prerequisites: The display's power is off.

Step 1 Turn the display's power on.

If this is the first time you turned the power on or the display's locale is not configured yet, the **Regional and language settings** window opens.



Step 2 Select a **Language** from the drop-down list.

Step 3 To change the date and time, click **ADJUST**.

Step 4 To disable the automatic display of this window the next time you power up the unit, remove the check mark from **Show this dialog again next time**.

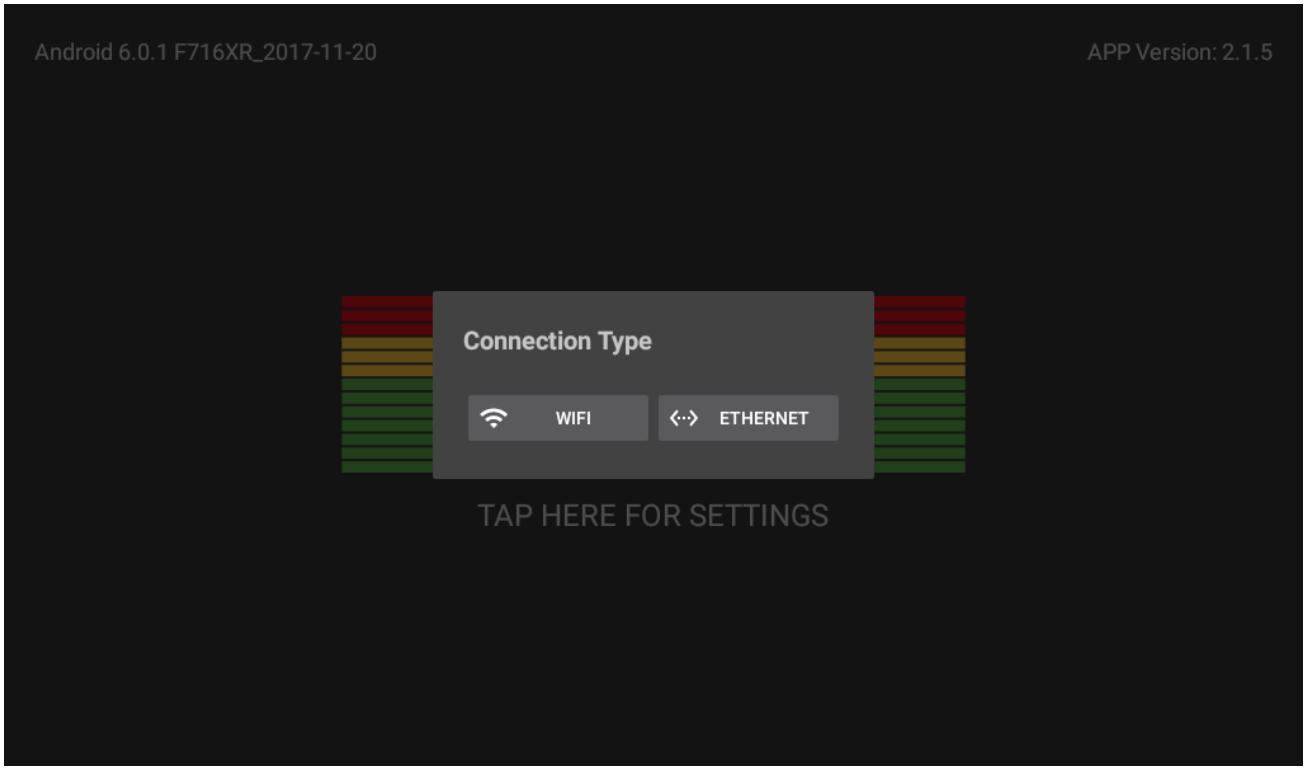
Step 5 When all properties are configured, click **OK**.

To change these properties in the future, use the General Settings window.

Connecting to a source attached to a router

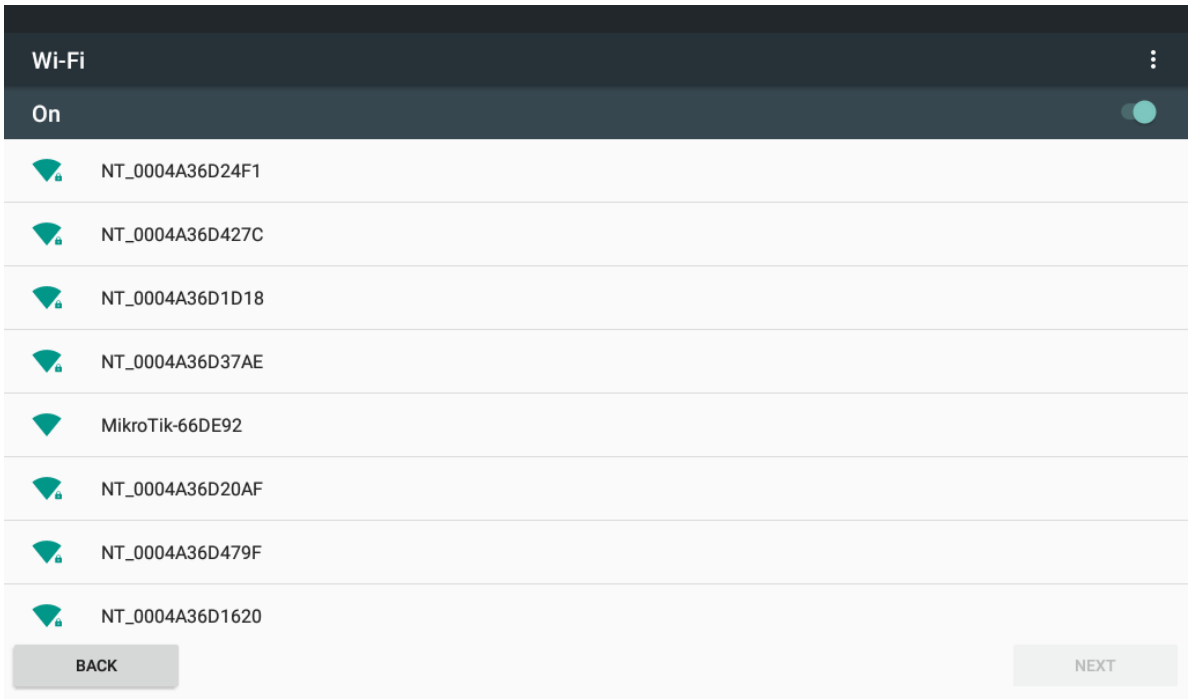
The display supports a WiFi or Ethernet connection to a network.

Prerequisites: You are configuring the unit for the first time, which is indicated by this window:



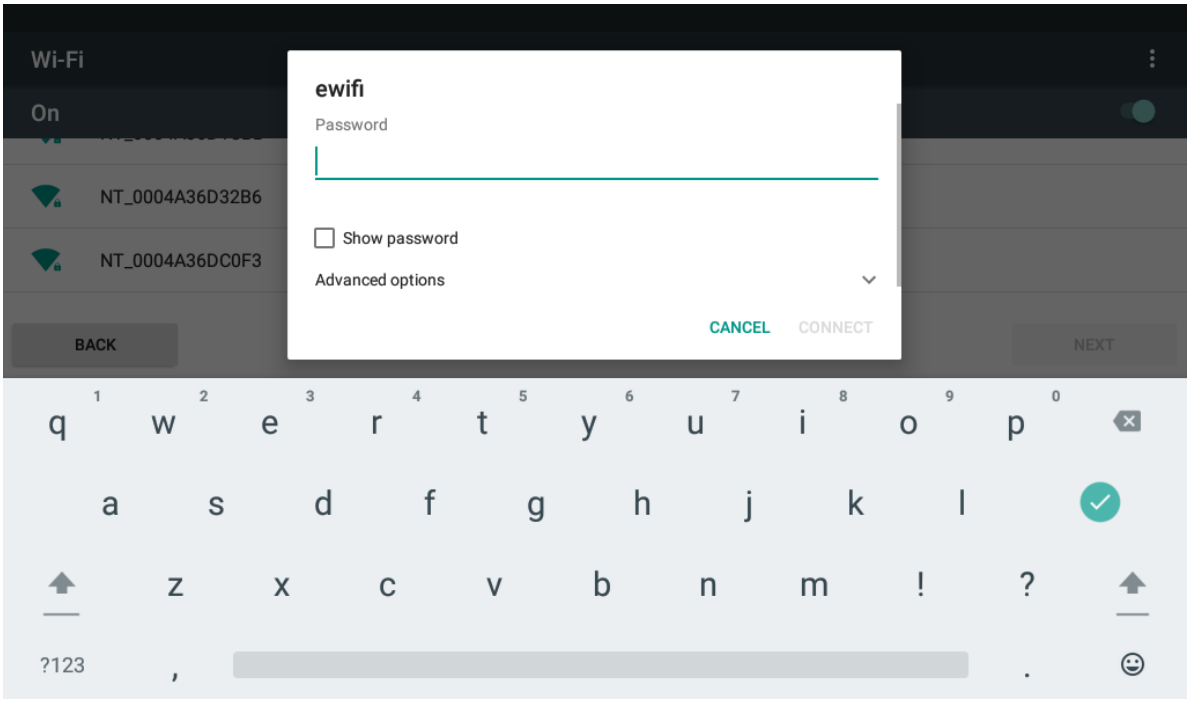
Step 1 Select a **`Connection Type`**.

If you selected WIFI, the list of available **Wi-Fi** connections opens.



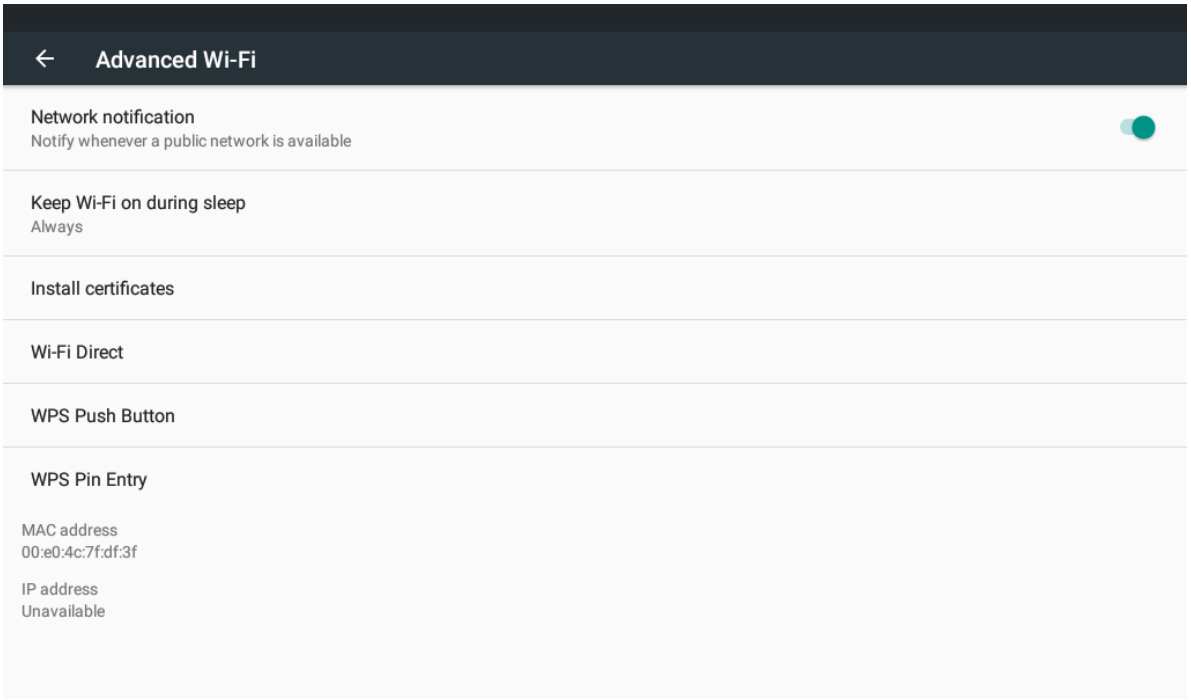
Step 2 Select a network.

The display prompts you for the network password.



Step 3 If WPS (Wi-Fi Protected Setup) is available on your network or source, expand the three vertical dots in the upper right and select **Advanced**.

The **Advanced Wi-Fi** view opens.

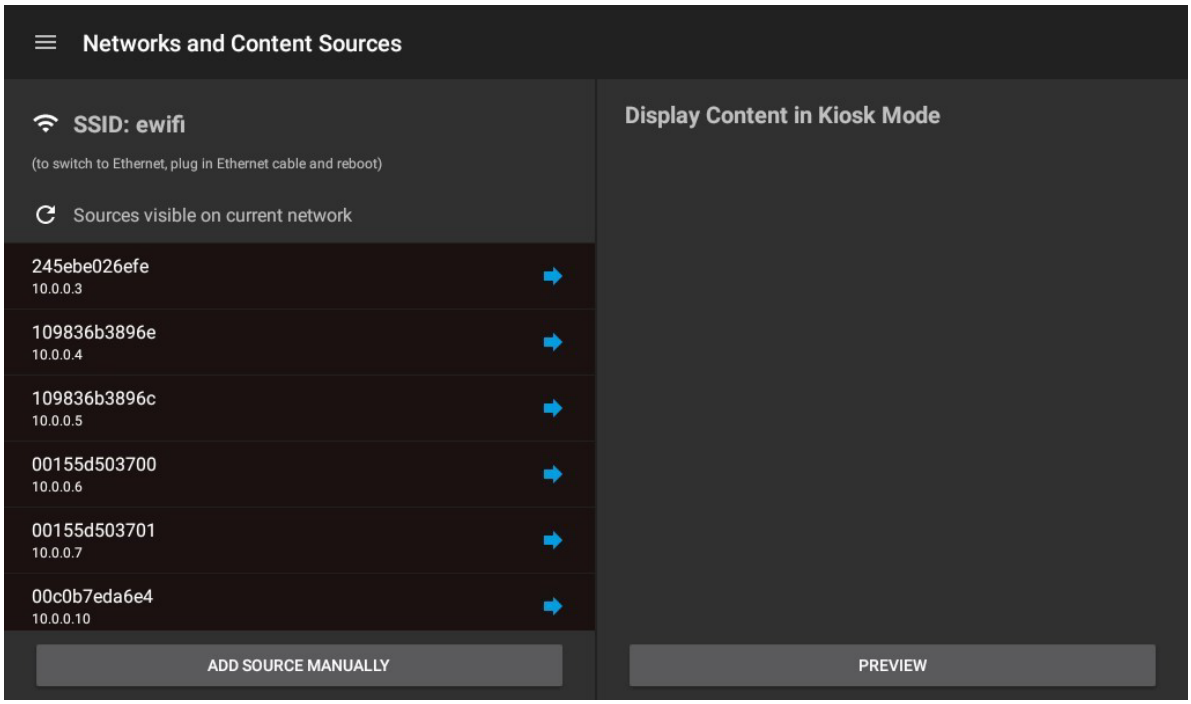


Step 4 To enable these features, tap the push button toggle in the upper right corner of the view.

The WPS system should now connect.

Step 5 Once the WPS system connects, click **NEXT**.

The application displays, "Finding Content Sources." Once search and discovery are complete, the **Networks and Content Sources** view opens.



The display lists sources by IP (Internet Protocol) address in ascending order. Along with the IP address the display includes the MAC (Media Access Control) address for each source. A MAC address is a unique identifier assigned to a Network Interface Controller (NIC) for use as a network address to communicate within a network segment (Wikipedia).

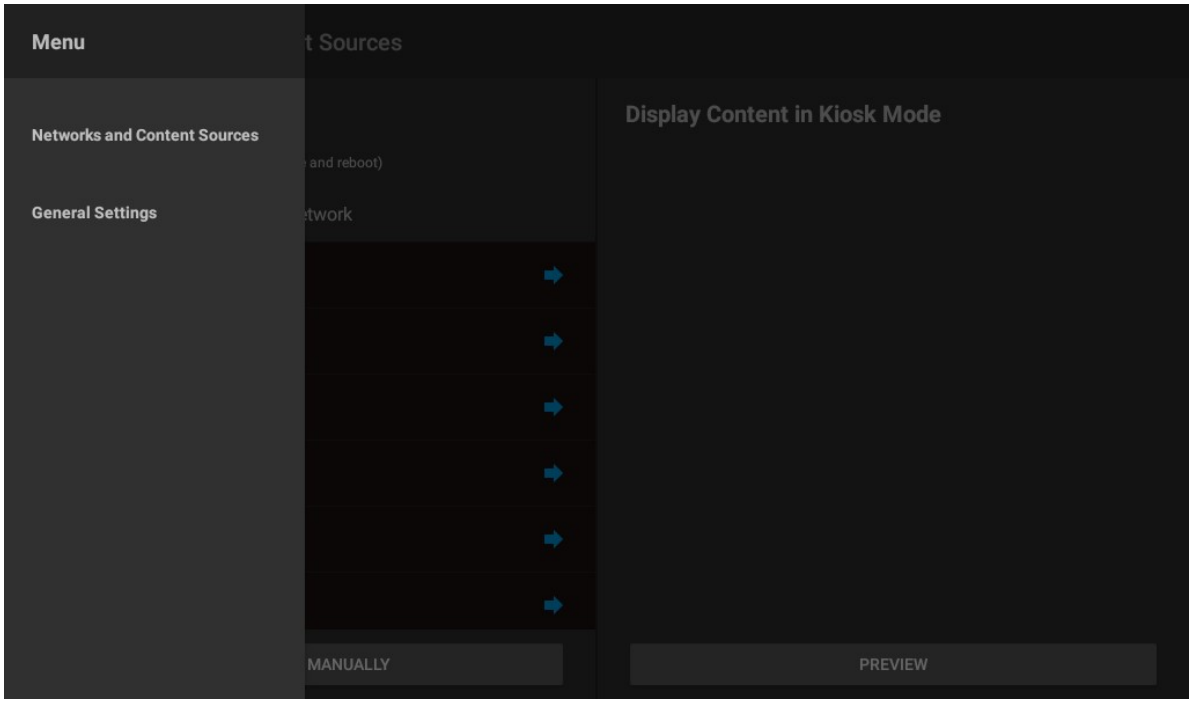
Configuring general settings

General settings customize the display to meet your needs. This procedure provides an example of how to configure the display by changing the date and selecting a browser.

Prerequisites: Your display connects successfully to content sources.

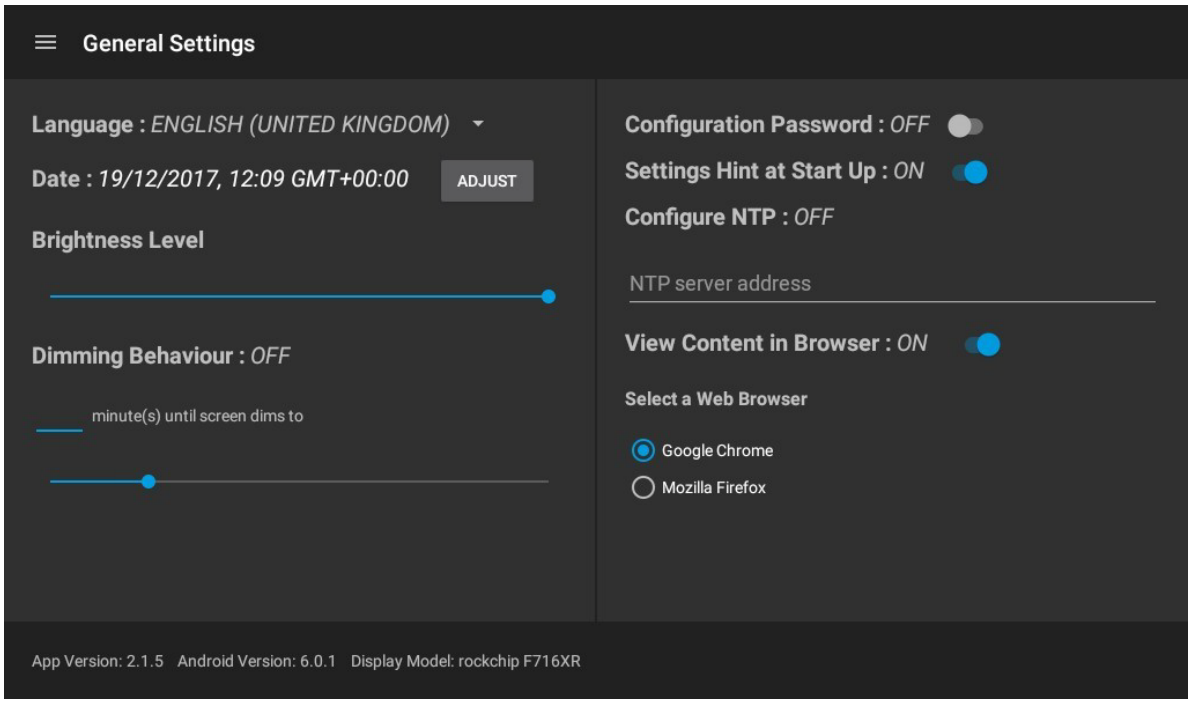
Step 1 To access the menu, tap the menu button ( ) in the upper left or swipe from the left edge of the screen.

The Menu opens.



Step 2 Tap **General Settings**.

The **General Settings** view opens.



Step 3 To change the date, click **ADJUST** and turn off the **`Automatic date & time`** toggle.

The **`Set date`** property becomes available.

Step 4 Change the date, re-enable the **`Automatic date & time`** toggle and click **NEXT**.

The **General Settings** view opens. The View Content in Browser property defaults to OFF, which configures the display to use the built-in Kiosk browser.

Step 5 To select a different browser, tap the **`View Content in Browser`** property.

The browser options expand with two possible browsers: Google Chrome and Mozilla Firefox.

Step 6 Select a browser and return to the **Network Settings** page.

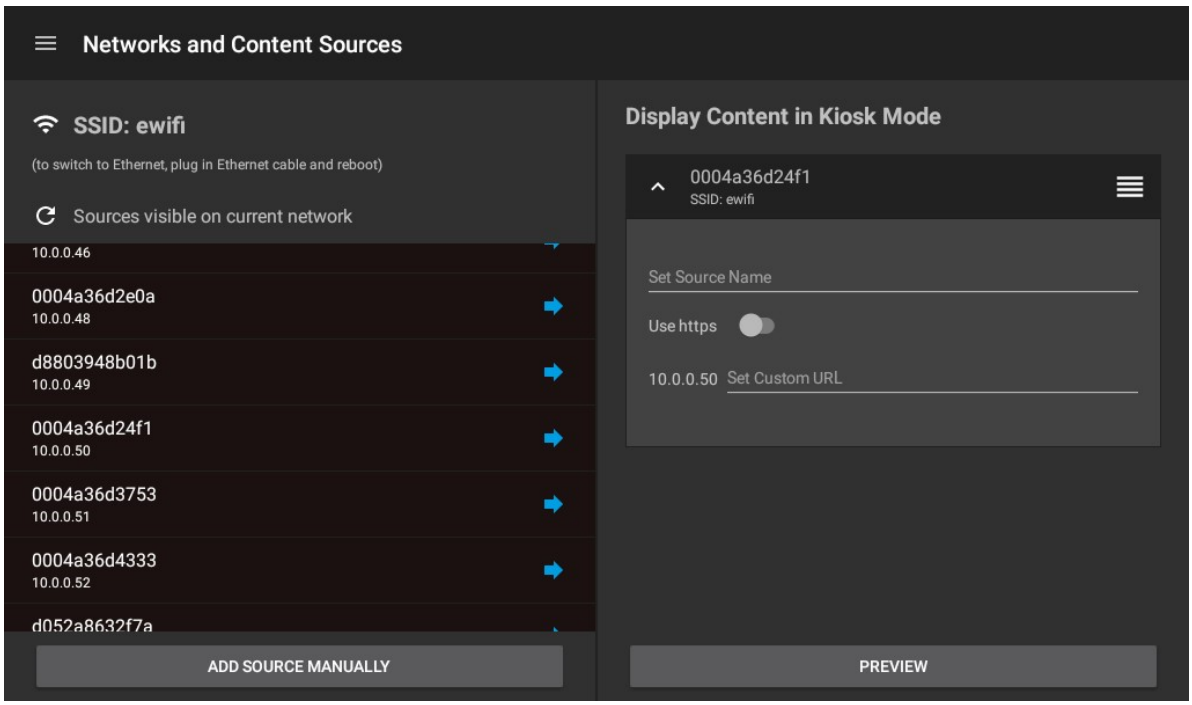
Configuring sources

You can select any number of sources or select the same source numerous times, with a different, manually-added URL for each source instance. For example, you can select different sources or different pages from the same source.

Prerequisites: Your display connects successfully to all available content sources.

Step 1 To configure a source, click on its box.

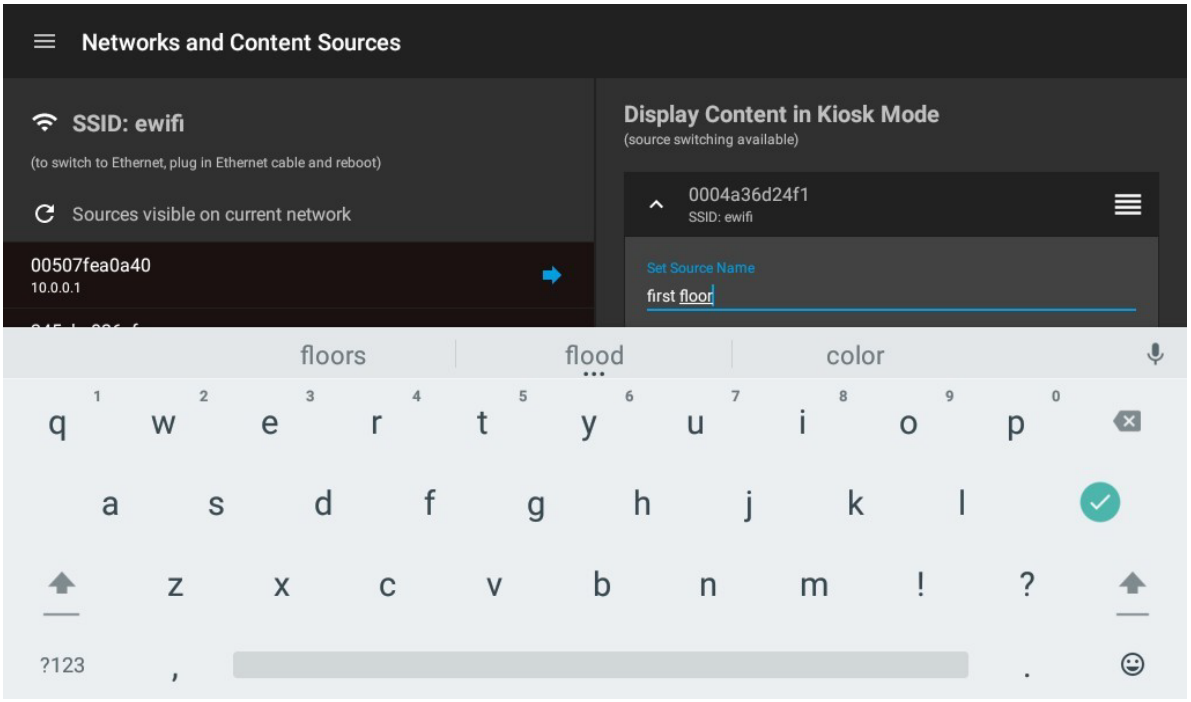
The source's configuration options expand.



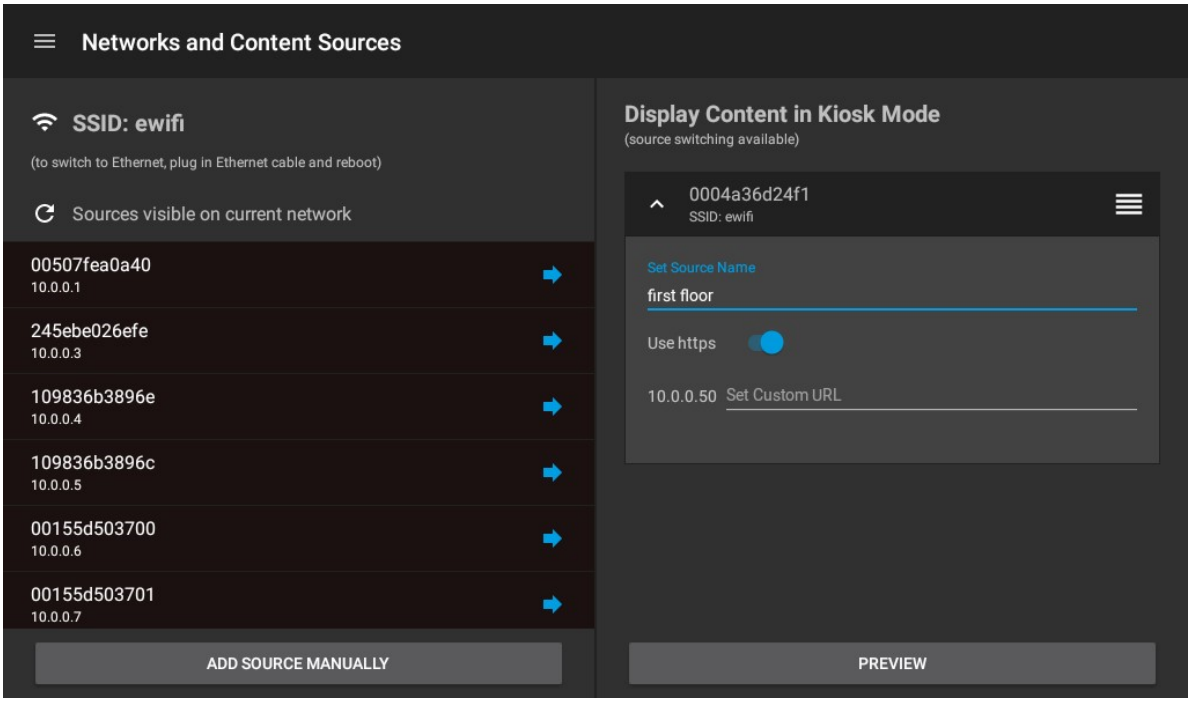
Using these options you can rename the source, enable HTTPS, add a custom URL, and include any custom port numbers in the URL.

Step 2 To rename the source, click into **`Set Source Name`** and enter the name.

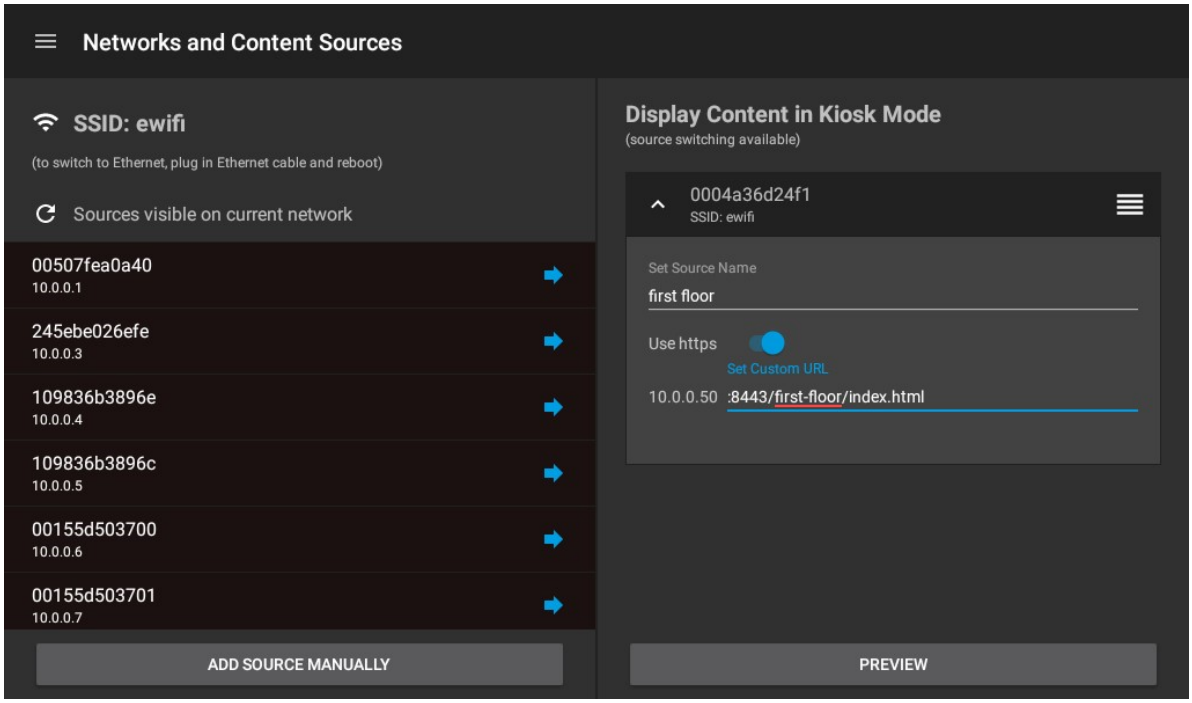
The keyboard opens.



Step 3 To enable HTTPS, toggle **`Use https`**.



Step 4 To set a custom URL including a custom port number, click into the IP property (Set Custom URL).



For example:

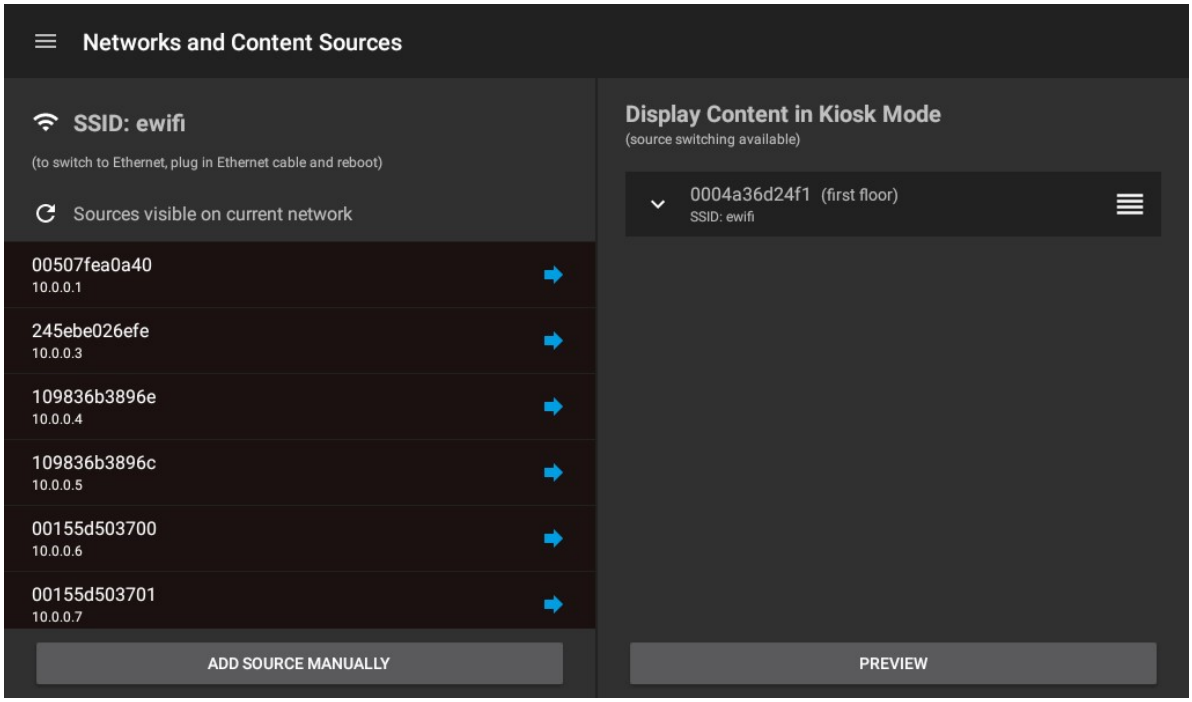
Source name — first floor

HTTPS — yes

Custom URL — :8443/first-floor/index.html

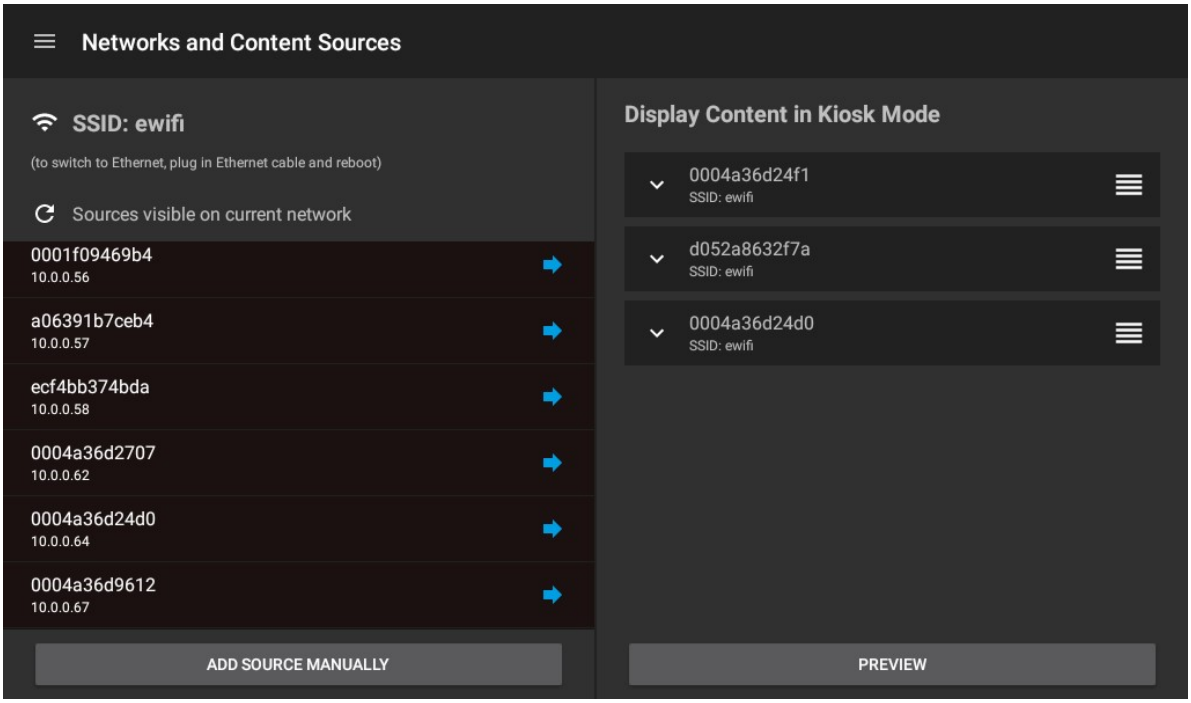
To include multiple port numbers place a colon before each port number. For example, :8080, :8443.

Step 5 When you finish editing a source, click to collapse the box and save your changes.



Step 6 Repeat these steps for each source to configure.

Multiple sources display in the right-hand side.

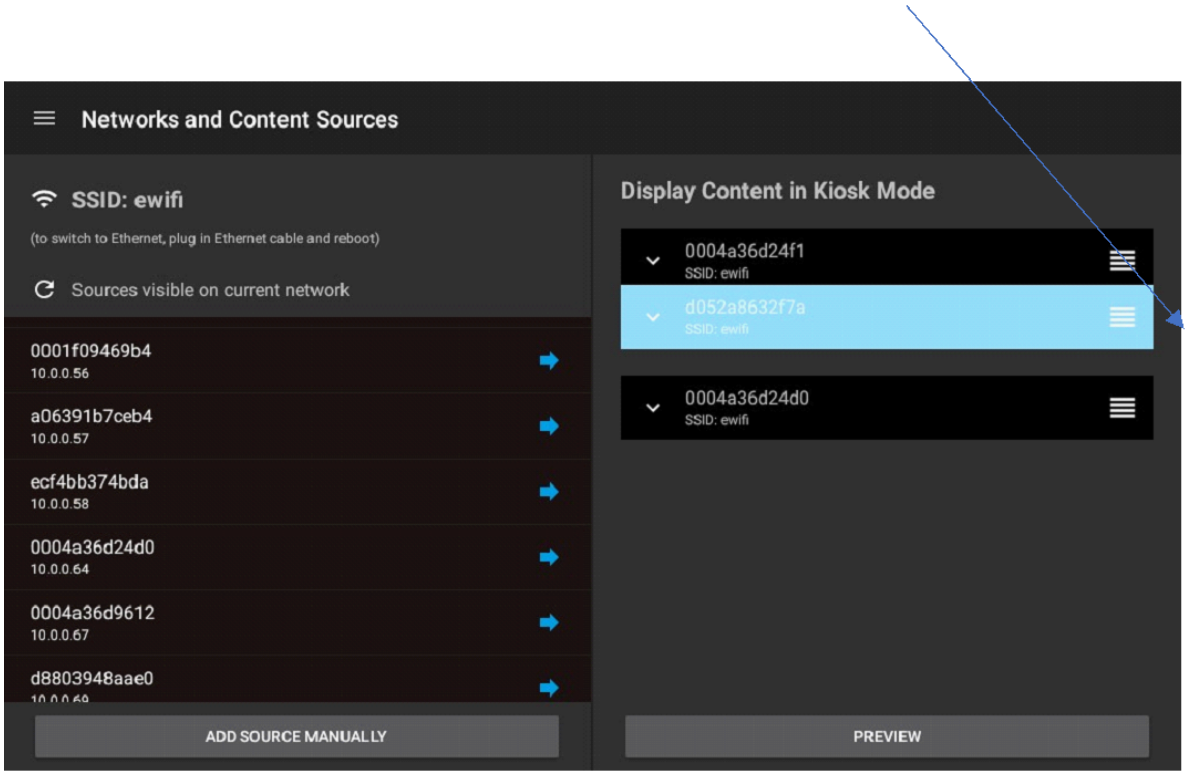


Managing configured sources

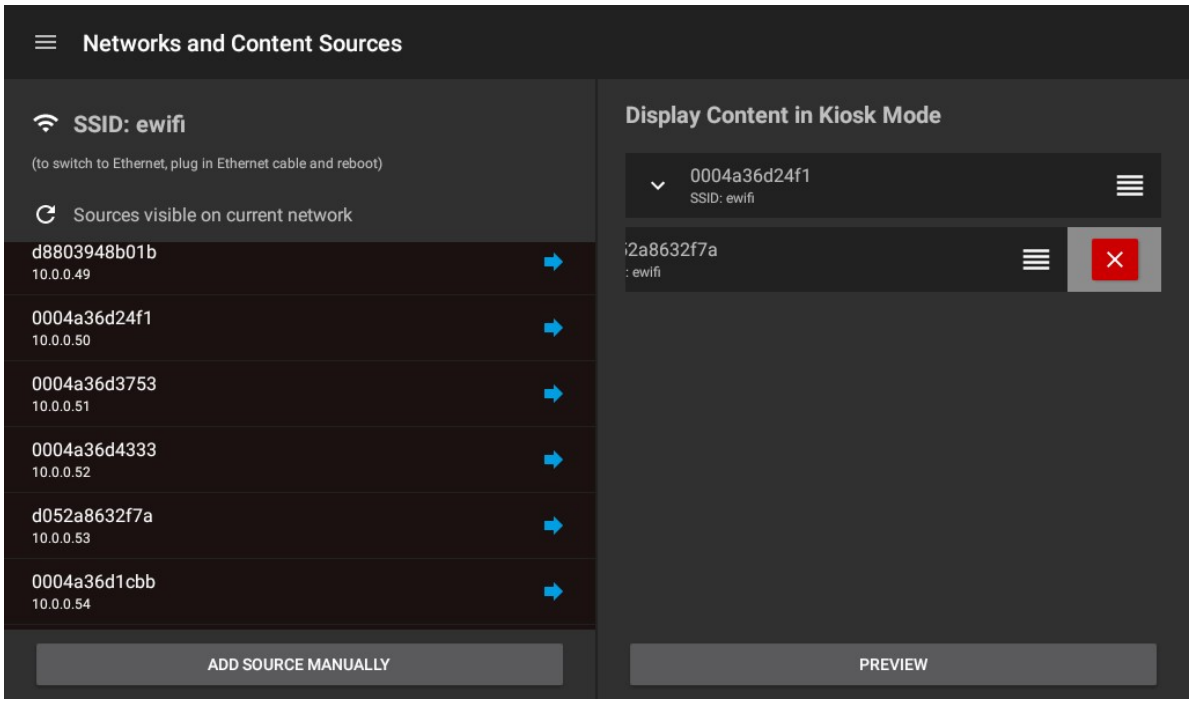
Once you finish configuring sources you can reorder them, delete them, add new ones manually, preview and finally launch them.

Prerequisites: Your display connects successfully to all available content sources.

Step 1 To reorder the configured sources, tap and hold, then drag the handle to the right of each saved source, up or down.

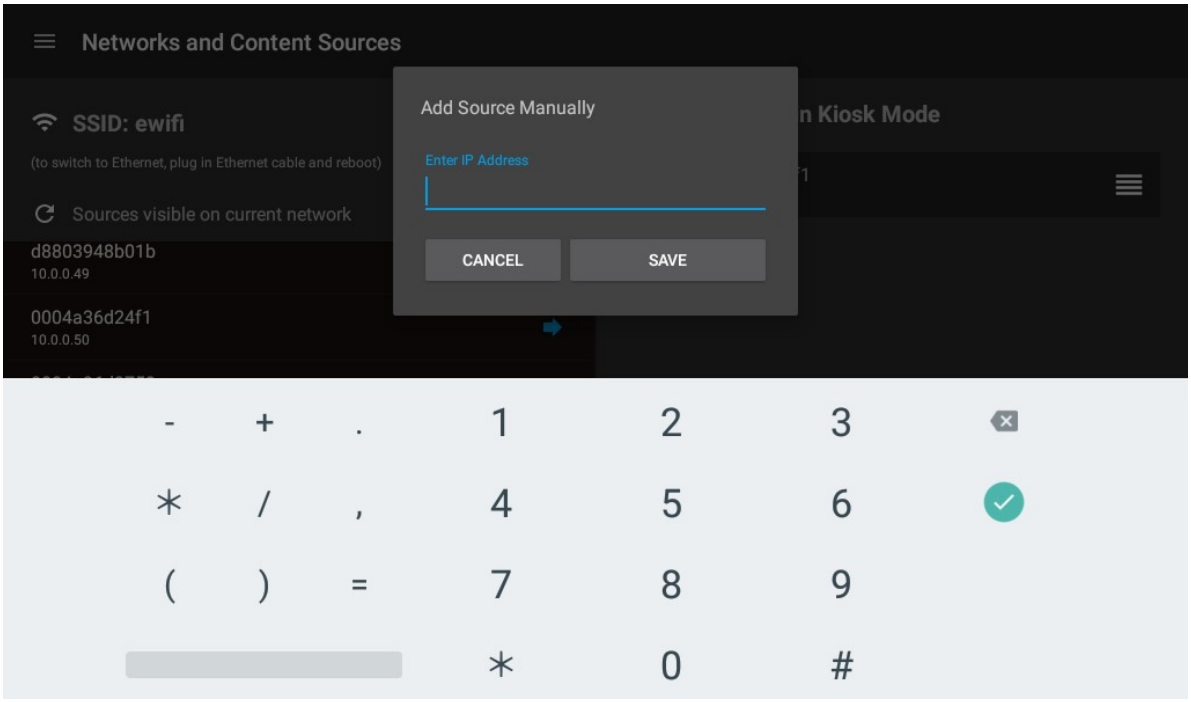


Step 2 To remove a source, swipe left from the center and click the remove button.



Step 3 To add a source manually, click the **ADD SOURCE MANUALLY** button.

The Add Source Manually window and a keyboard open.

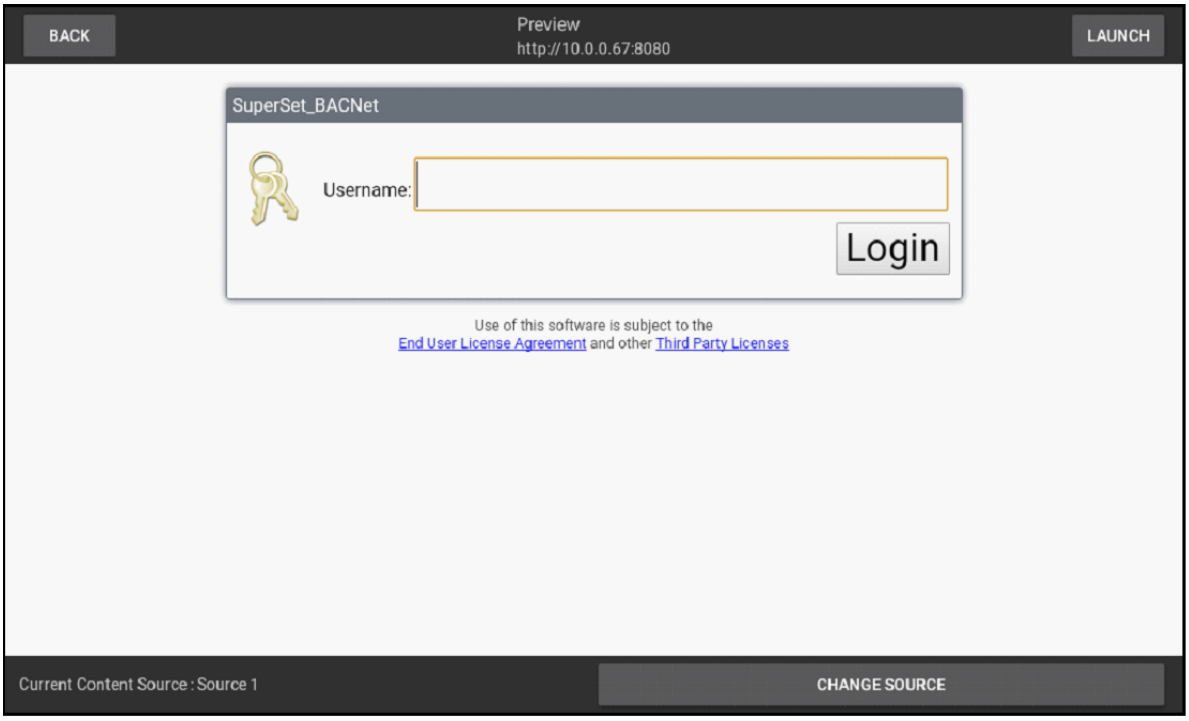


Step 4 After manually adding the source, tap it and configure it.

Step 5 Click **PREVIEW**.

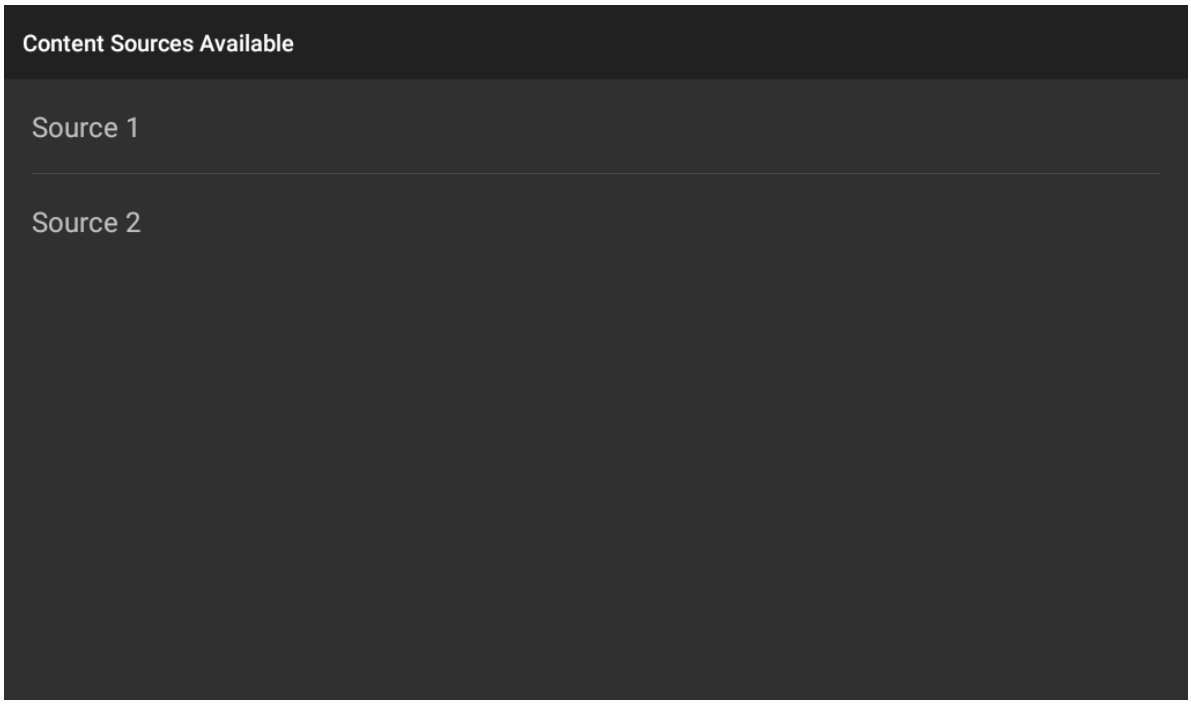
If any sources are expanded, the application automatically saves any changes made to the source.

The app displays the web content from the top saved content source. A preview bar gives you easy access back to the **Network and Content Sources** view.



If you have chosen more than one Source at launch point, the app superimposes an additional ribbon at the bottom of the loaded view, as above. This displays the current Source name, with a

button offering you the ability to swap among sources quickly. If clicked, the view shows a list of pre-loaded sources.

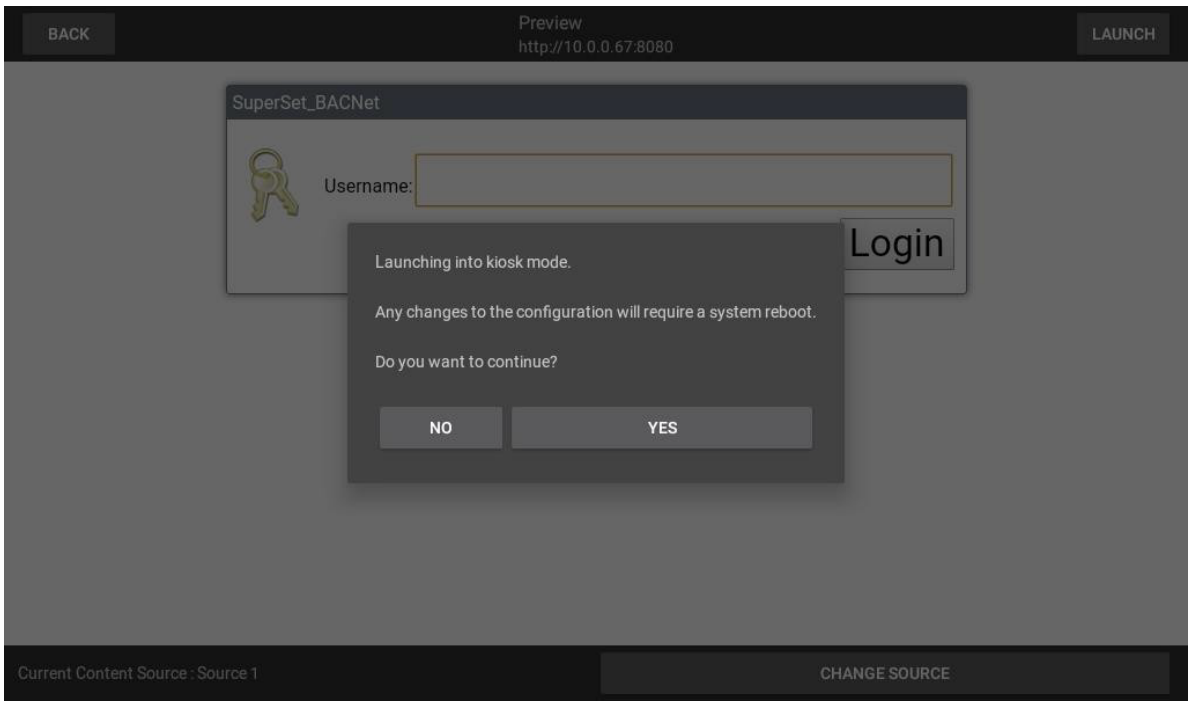


Step 6 Select a source.

The app loads it accordingly.

Step 7 When you are happy with the loaded content, click **LAUNCH**.

The **Launching into kiosk mode** window opens.

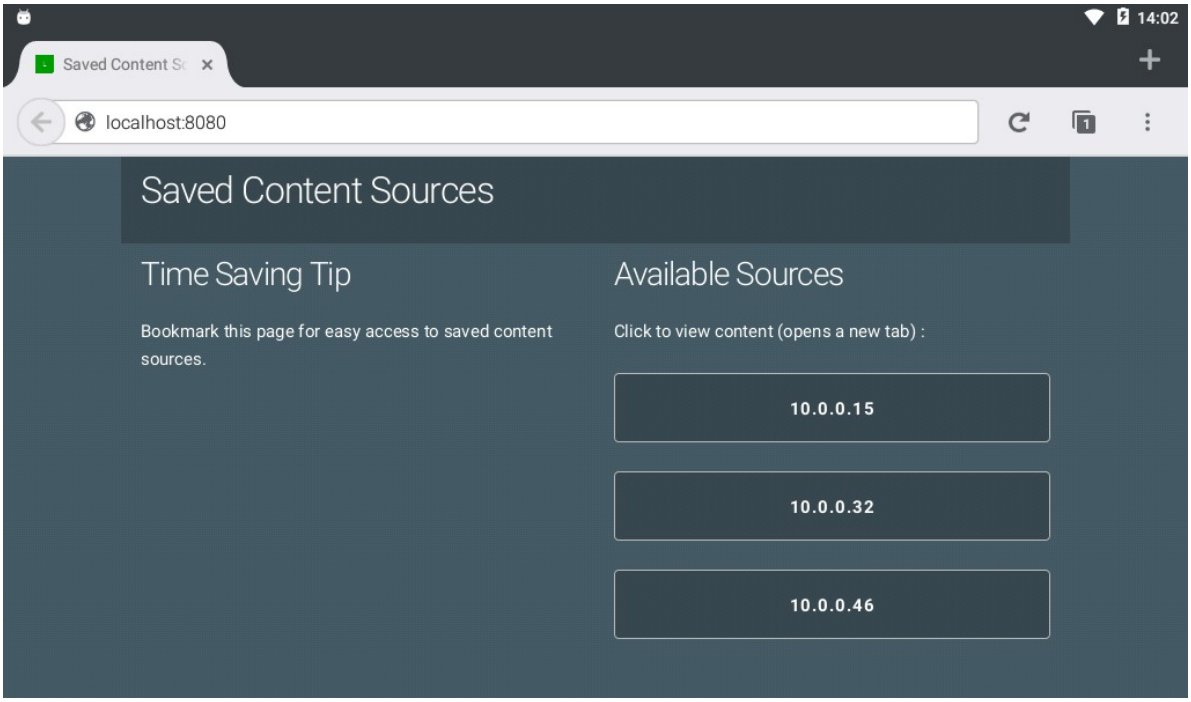


Clicking **NO** closes the window.

Clicking **YES** puts the display into kiosk mode. To make any further changes requires a reboot.

Step 8 To continue, click **YES**.

If you selected to view content in a browser, such as Chrome, the app starts the content within the selected browser. For convenience, the app creates a web page at launch, displaying all the sources you enabled on the launch screen.

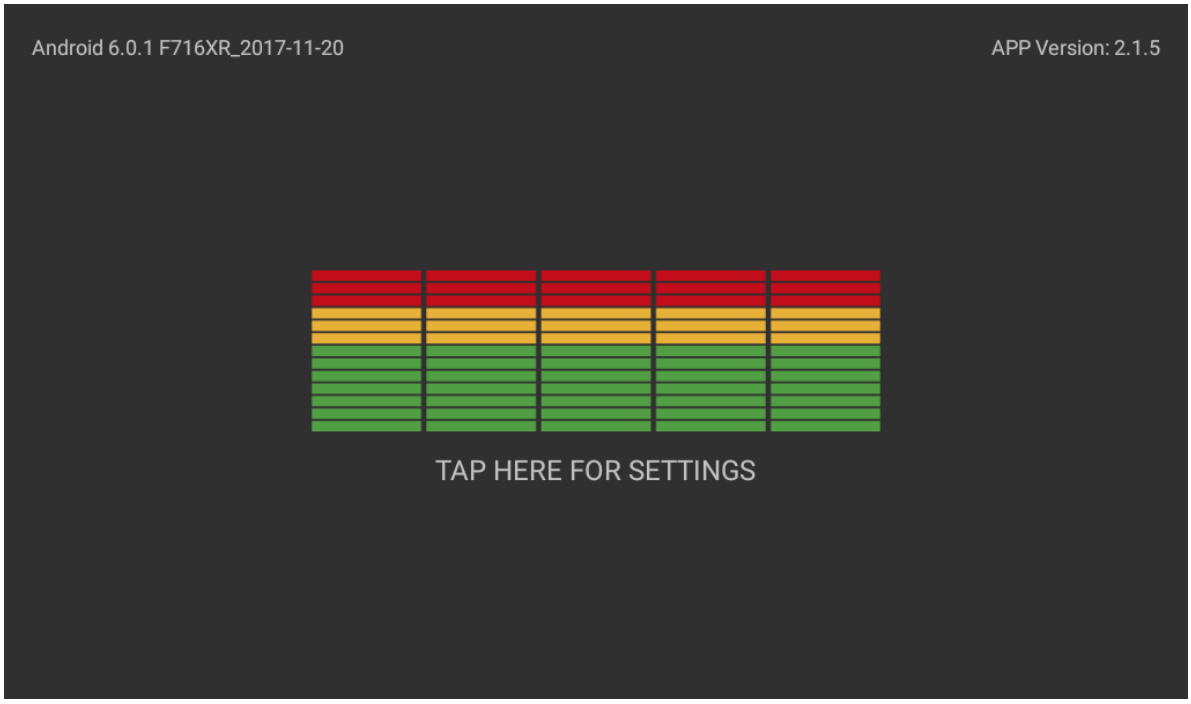


Step 9 For speed and ease-of-use going forward, bookmark this page on first loading.

Clicking on the tab for any added source launches that source's content in a separate tab.

Step 10 To change the network connection of the launch sequence at any time, re-boot the display by pressing the power button only once.

The app displays the splash screen.

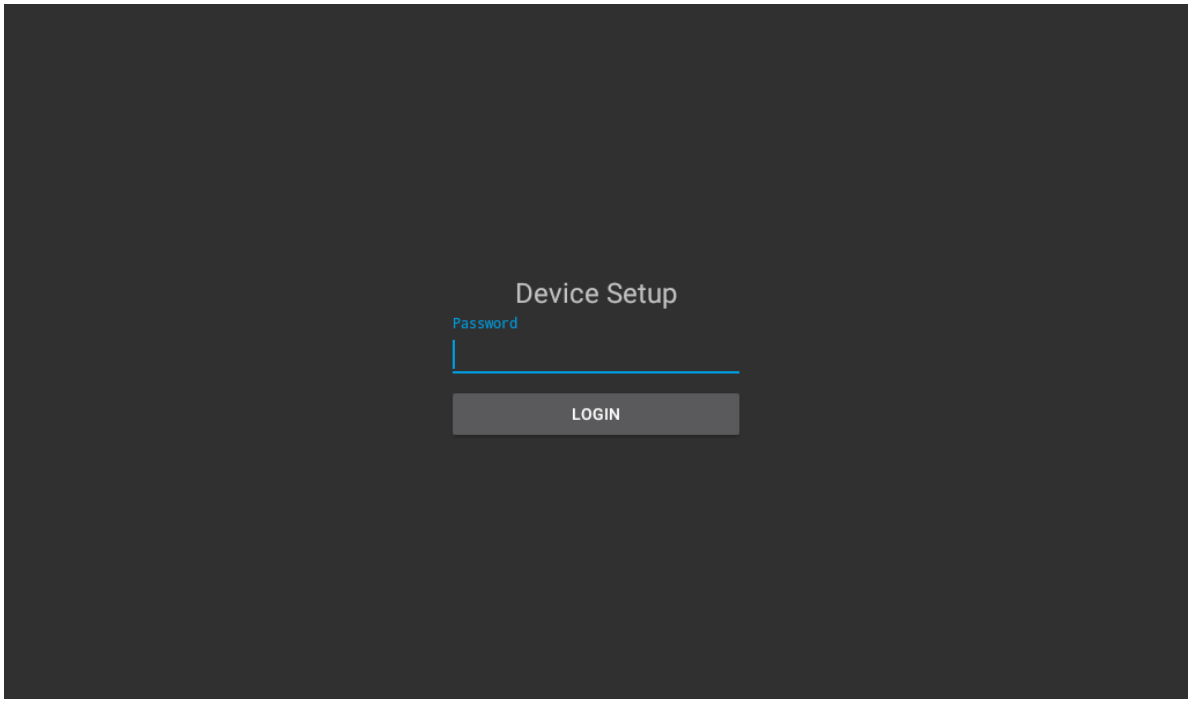


You may turn off the “TAP HERE FOR SETTINGS” hint in **General Settings**.

The top, right corner of the splash screen reports the version number of the app.

Step 11 Tap the screen.

If you enabled the configuration password, the login page opens.



Step 12 Enter the password and tap **LOGIN**.

The default password is: `ipd_admin`

The app returns to the **Networks and Content Sources** view.

Step 13 Adjust your requirements.

The app displays, “Config Mode Active.”

Connecting to a Wi-Fi source

This procedure connects the display to a Wi-Fi source with a static IP enabled.

Prerequisites: Your display has been configured.

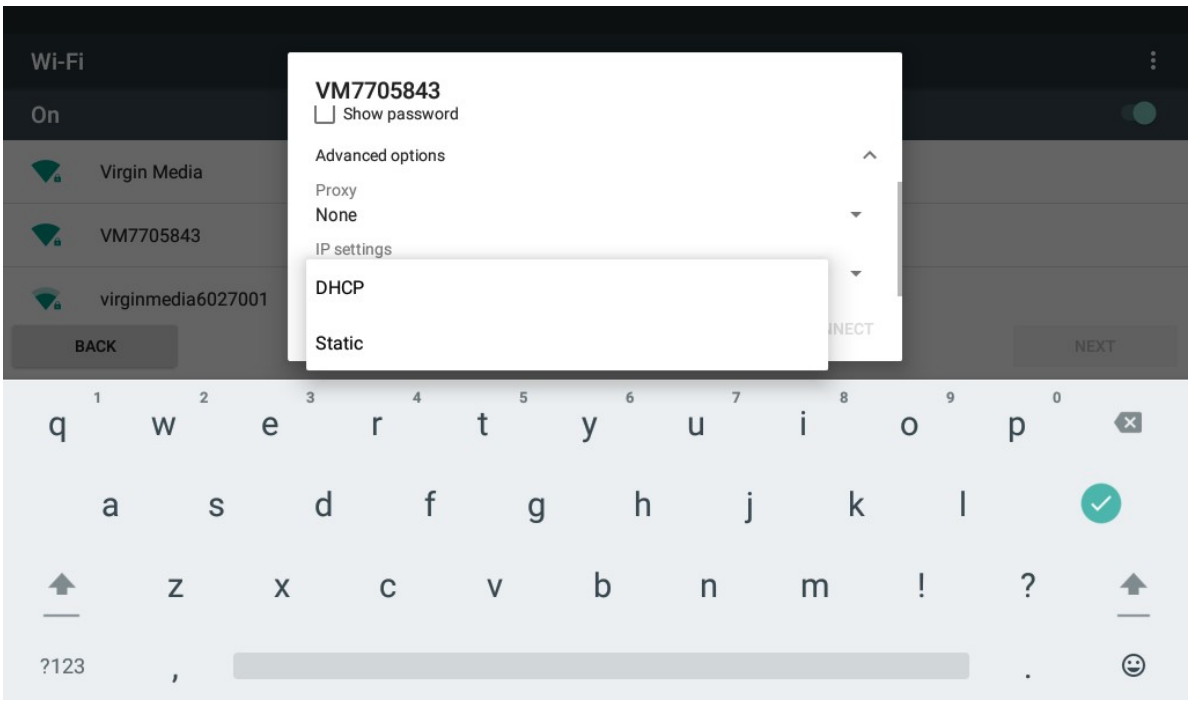
Step 1 Turn the display’s power on.

The app prompts you for the **`Connection Type`**.

Step 2 Tap **WIFI**.

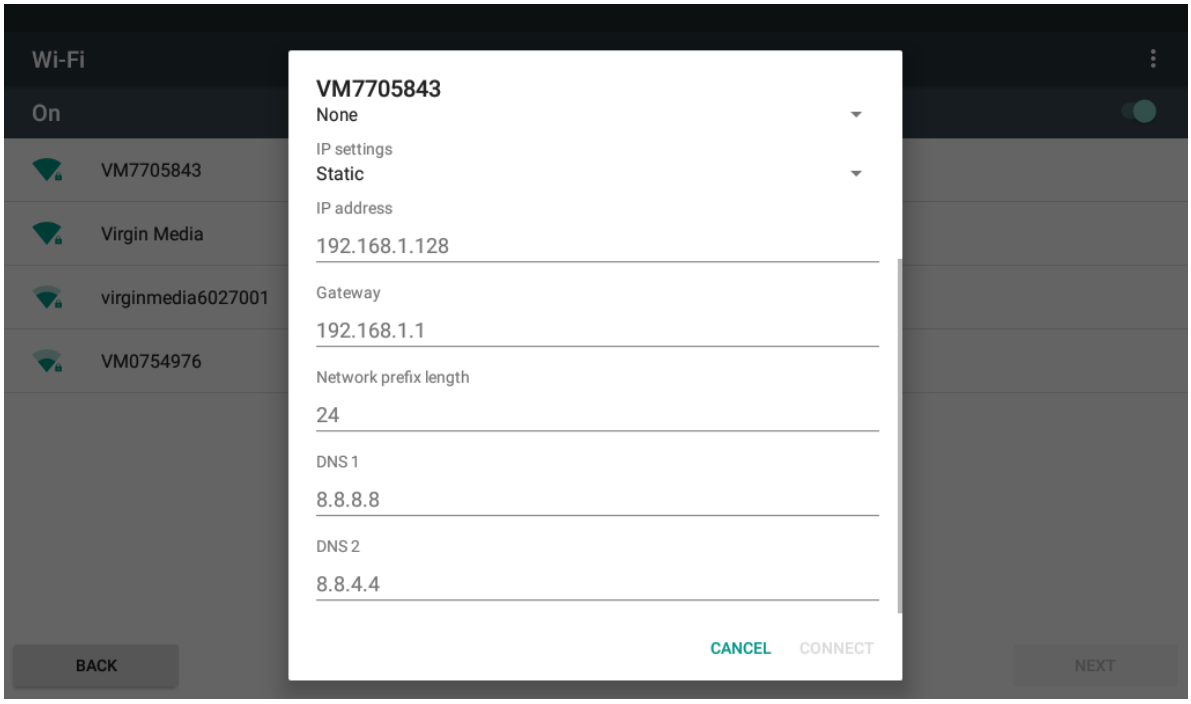
The list of Wi-Fi network connections opens.

Step 3 Select a Wi-Fi network, tap the three vertical dots in the upper right corner of the view, tap **Advanced** and scroll down.



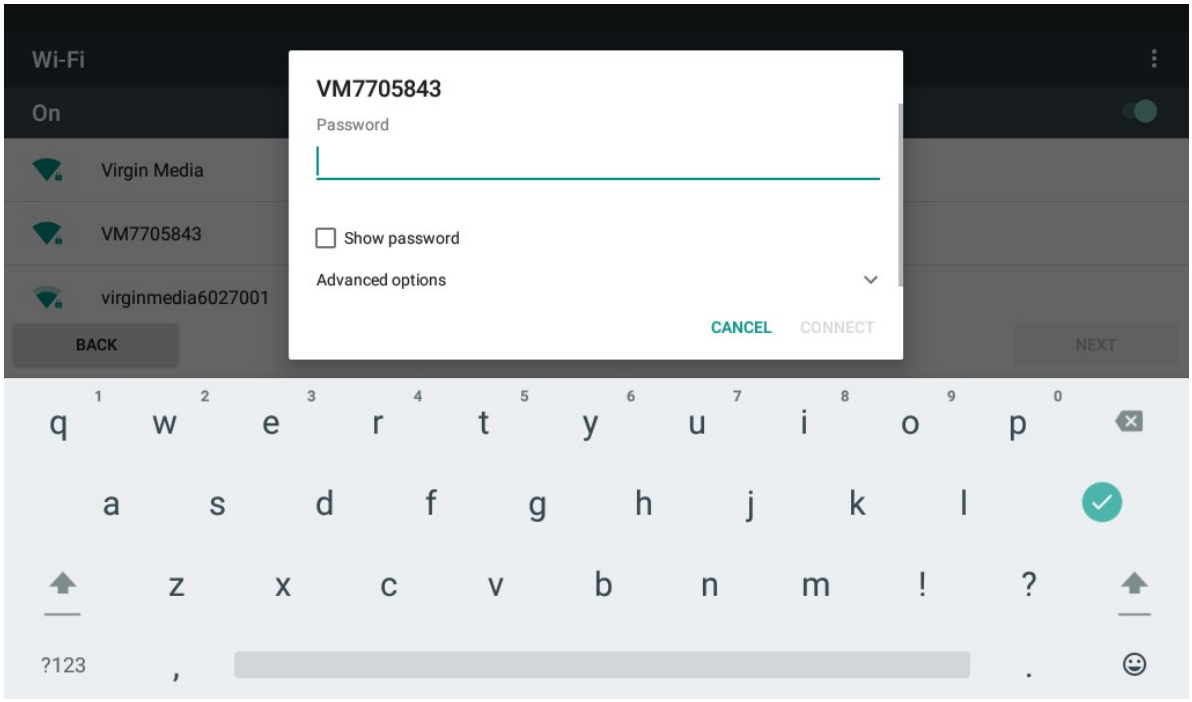
Step 4 Select `Static` for **`IP settings`**.

The IP settings properties expand.



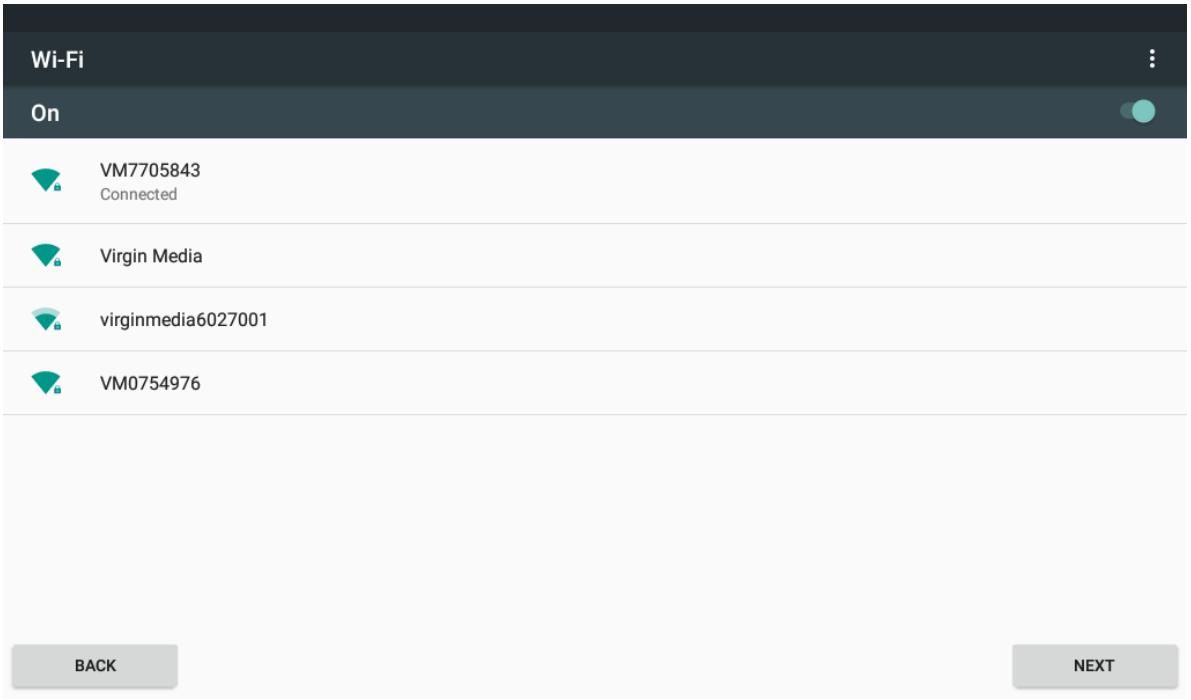
Step 5 Give the display a static IP address to use on the network, change other custom values, such as **DNS 1** as required.

The app prompts for the Wi-Fi password.



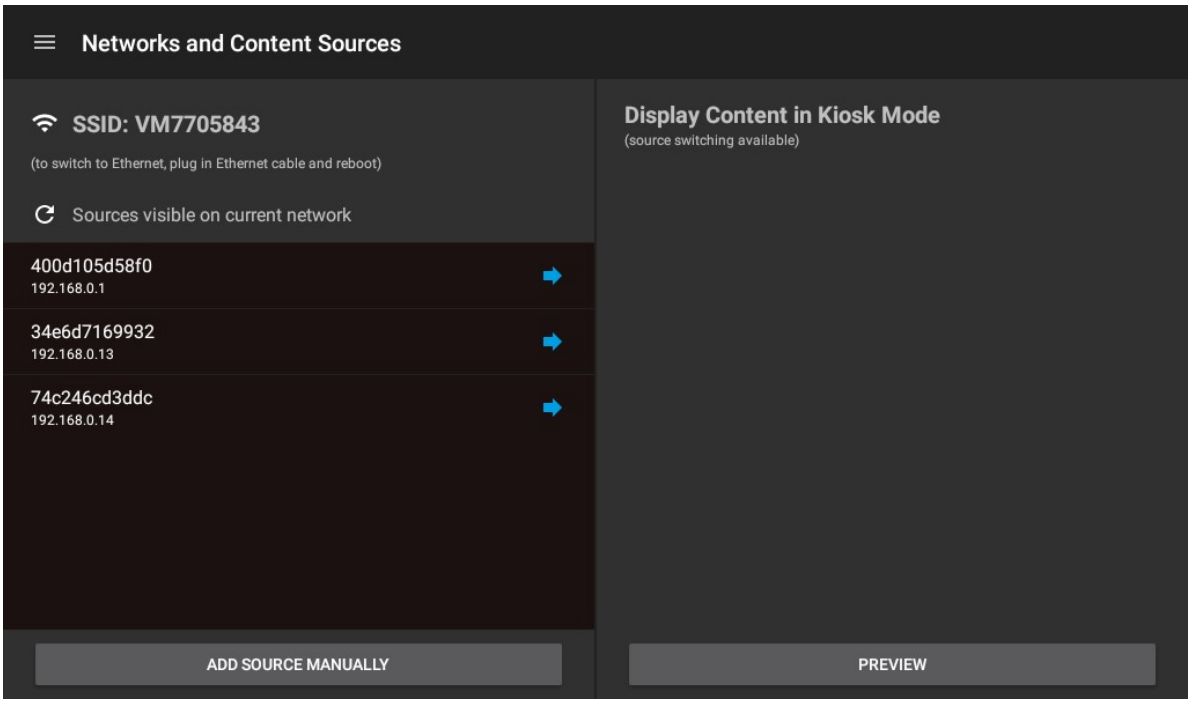
Step 6 Enter the password and click **CONNECT**.

The app makes the connection.



Step 7 Click **NEXT**.

The app finds all the sources on the network.



Step 8 Tap **PREVIEW**.

The app displays the web content from the top saved content source. A preview bar gives you easy access back to the N**etworks and Content Sources** view.

Step 9 When you are happy with the content, click **LAUNCH** and click **YES**.

The app displays the web content from the source.

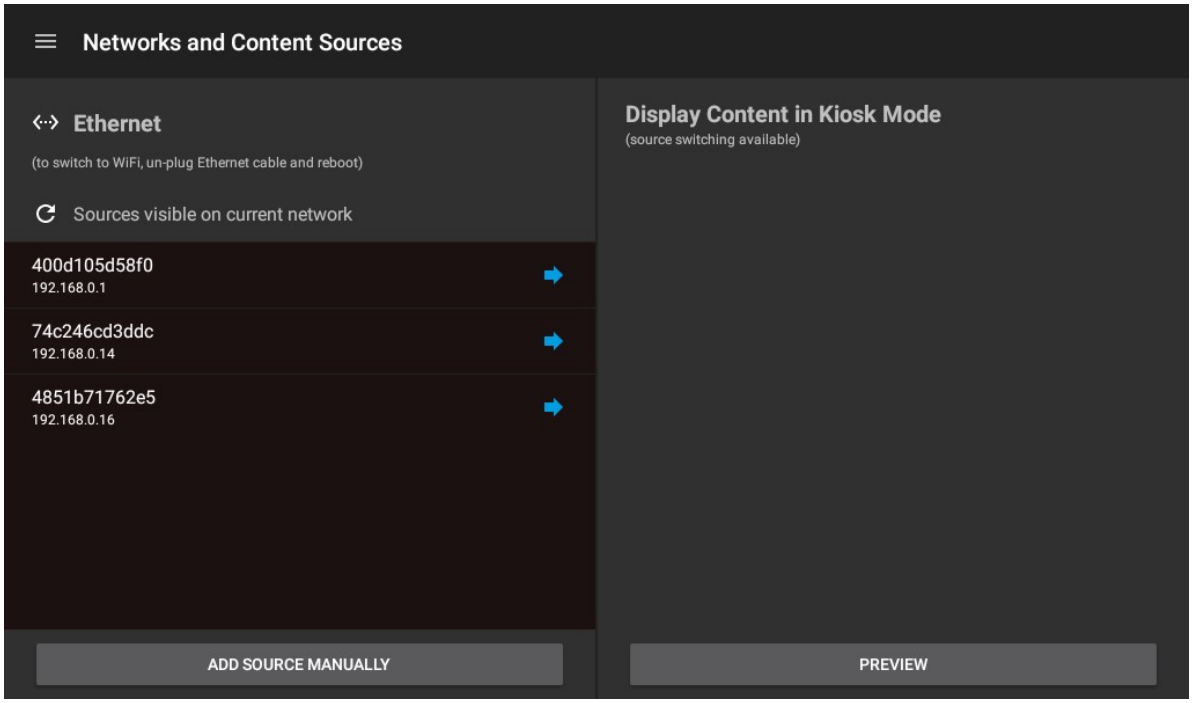
Connecting to an Ethernet source

Connecting to an Ethernet source is an alternative to using a Wi-Fi source.

Prerequisites: The display is connected to the network using an Ethernet cable.

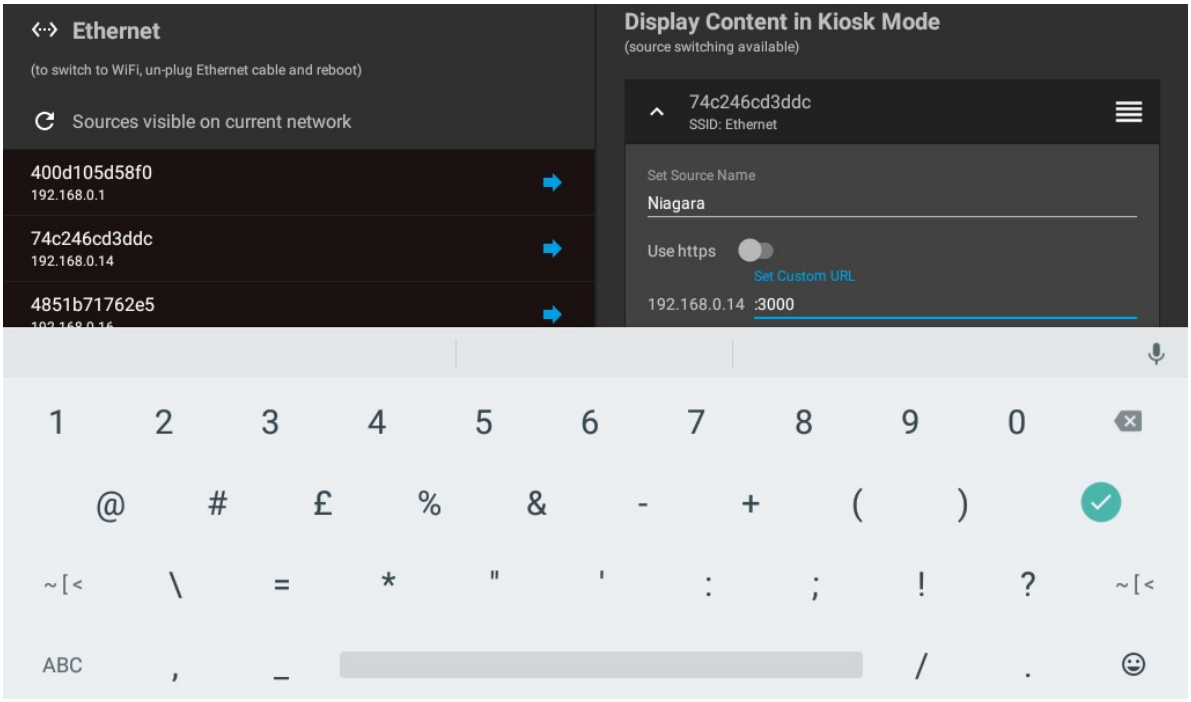
Step 1 Turn the power on to the display and boot the Ethernet source.

The app bypasses the **Connection Type** window, finds and displays all the sources on the LAN.



Step 2 Scroll to find the source to connect to and click the blue arrow.

The source configuration options expand.

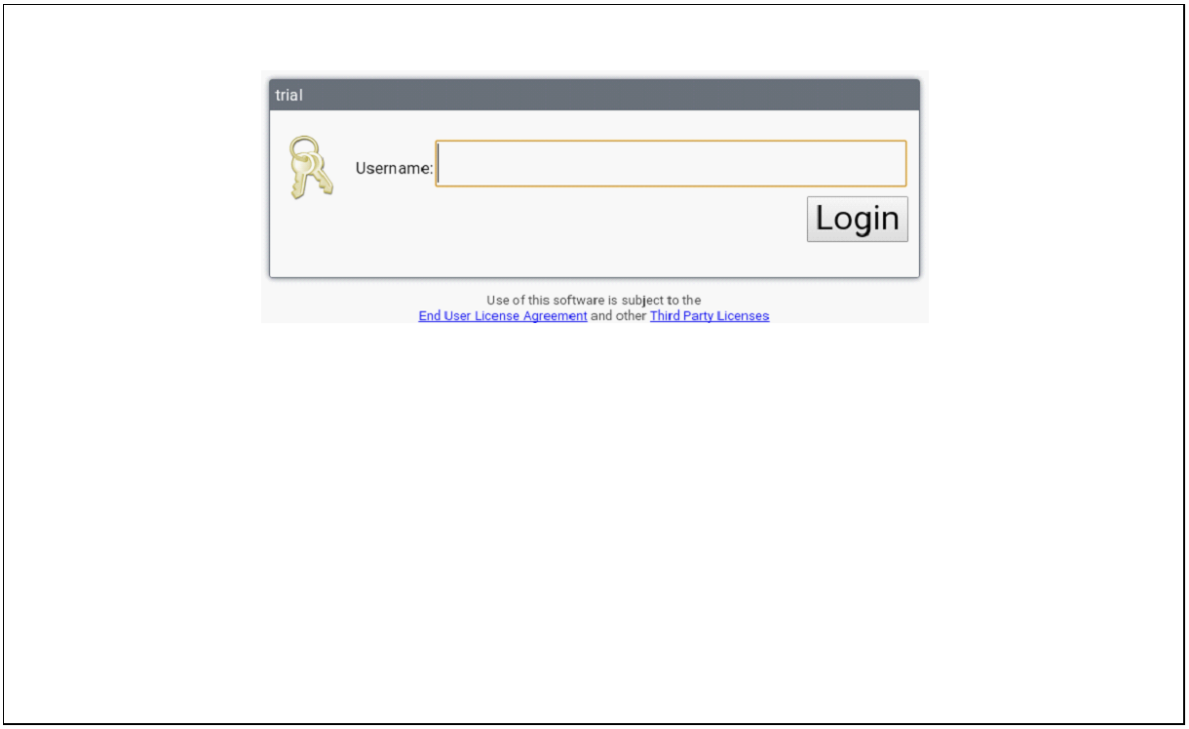


Step 3 Configure the name and/or the custom URL.

This is where you enter any ports. The example uses port :3000 to connect to the Niagara box.

Step 4 Click **PREVIEW**, then click **LAUNCH**.

The app displays the content from the source. In this case it displays a Login.



In this example, a Niagara station is the source. The screen capture shows the station login.

Connecting to an Ethernet source with Static IP enabled

This is a special case when connecting to an Ethernet source.

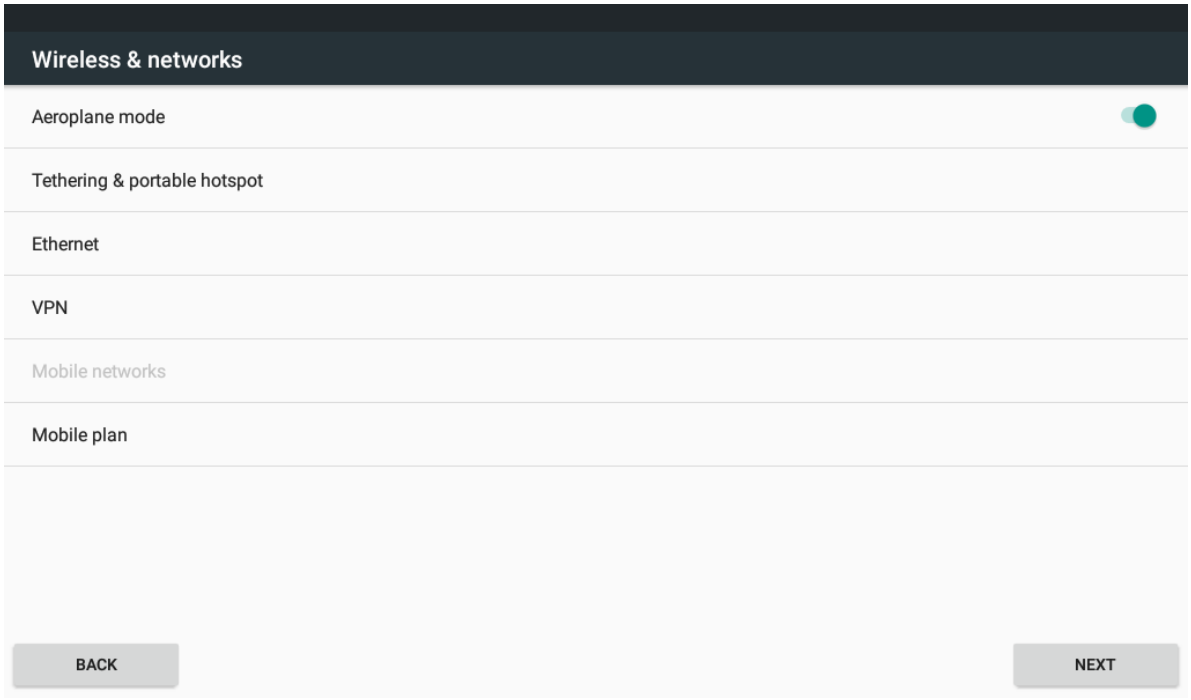
Prerequisites: The display is connected to the network using an Ethernet cable.

Step 1 Turn the display on and boot the source.

There is no DHCP (Dynamic Host Configuration Protocol) so the **Connection Type** window opens.

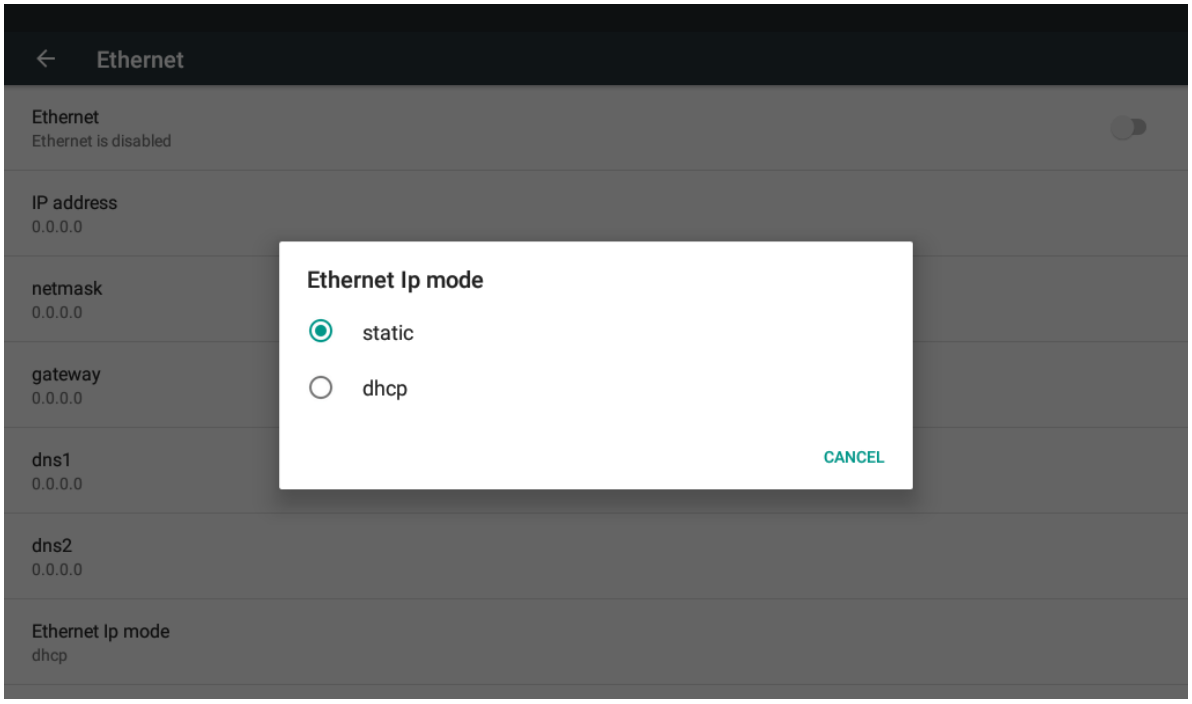
Step 2 Tap **ETHERNET**.

The **Wireless & networks** view opens.



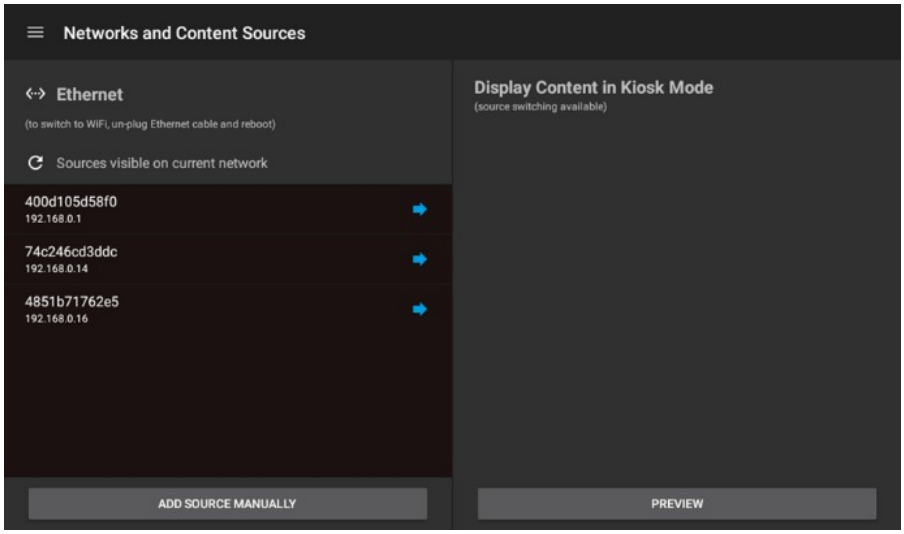
Step 3 Scroll to the bottom of the view and select **`Ethernet Ip mode`**.

The **Ethernet Ip mode** window opens.



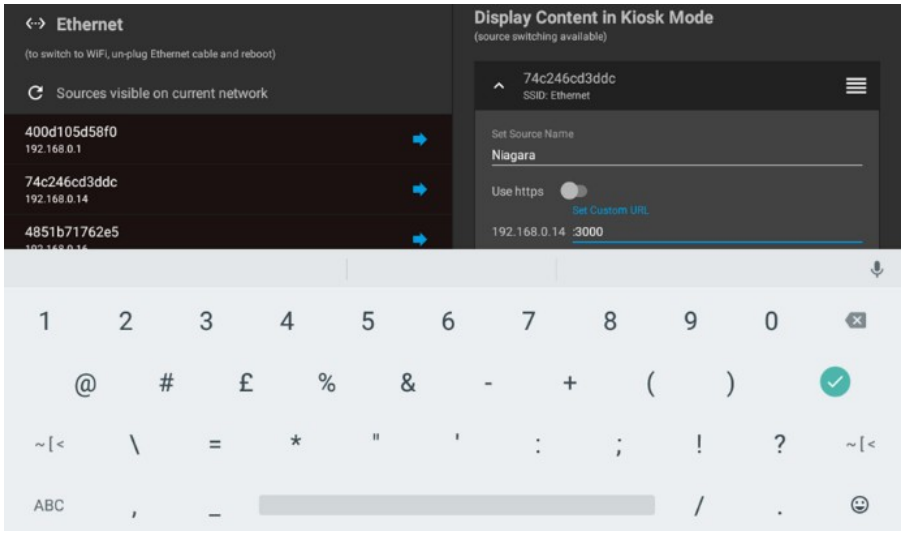
Step 4 Select static and enter the network settings for a static Ethernet connection. Add a value to each property, then save the settings.

The app finds any sources already connected to the same network and displays the **Networks and Content Sources** view.



Step 5 Scroll to find the source to connect to and click the blue arrow.

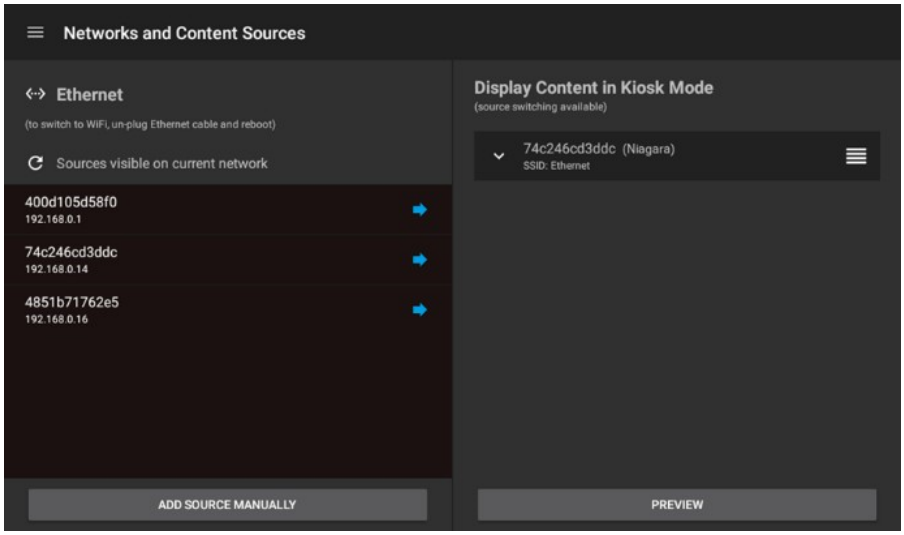
The source options expand.



Step 6 Configure the name and custom URL.

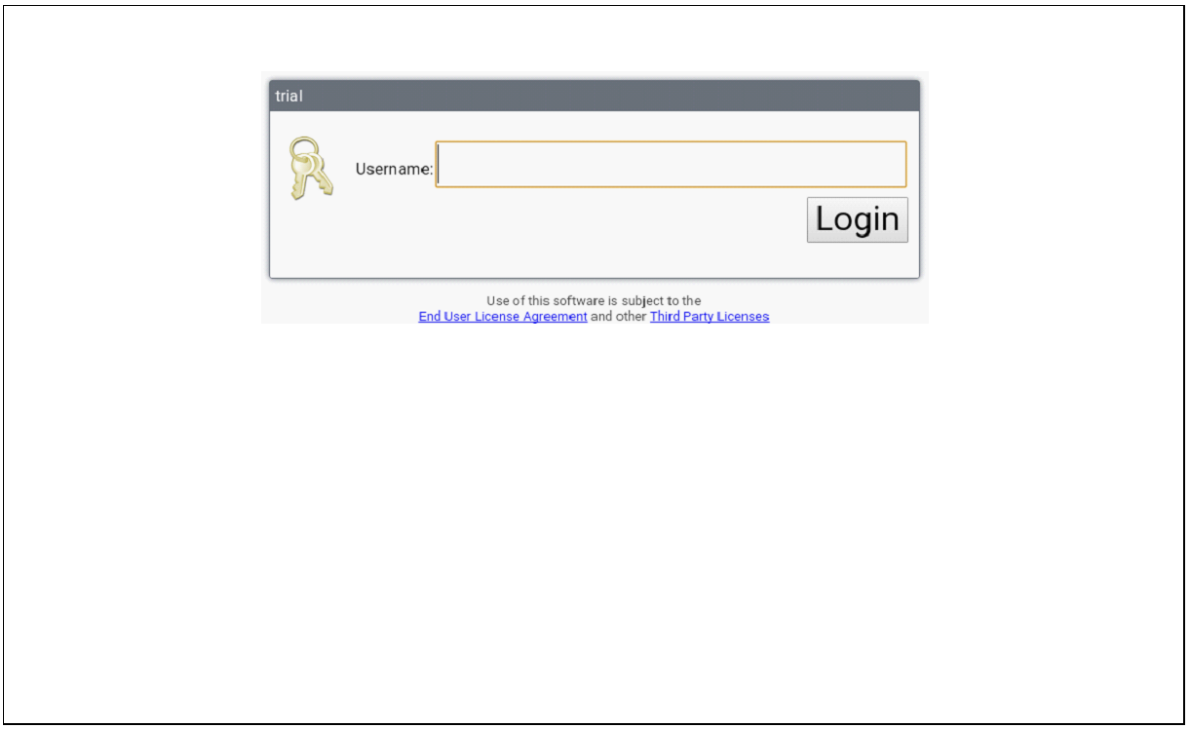
This is where you enter any port(s). In this case :3000 for the Niagara box we are connecting to.

The edited source appears to the right.



Step 7 Click **PREVIEW**, then click **LAUNCH**.

The app displays the content from the source. In this case it displays a Login.



In this example, a Niagara station is the source. The screen capture shows the station login.

Chapter 2 Security

Topics covered in this chapter

- Files
- Creating and exporting the client certificate
- Setting up authentication
- Setting up a display user
- Exporting the certificate with its private key (Niagara 4.9)
- Preparing the .p12 server certificate
- Installing the .p12 certificate

The communication between the tablet and its sources must be secure.

Only authorized users should use the tablet for its intended purpose. Data communication should be encrypted and the server authenticated before communication begins.

Files

Configuring the Niagara Touch display involves several files. As a best practice, take time to identify where you will save these files so that you can easily find them when you need them.

You can name your files differently from the names used in this table. These names are used as examples in these configuration procedures.

File	Where stored	Comments
Certificate .pem file	User home: `C:/Users/<User Name>/<Software version>/tridium/certManagement`	This file will reside in the User Key Store of the remote controller station. The remote controller is the client in this client-server relationship.
Certificate .pem file with key and .p12 file	`C:\certs`	This path should be short because you enter it when using OpenSSL to convert a .pem certificate file to a .p12 file. This certificate is destined for the display, which is the server in this client-server relationship.

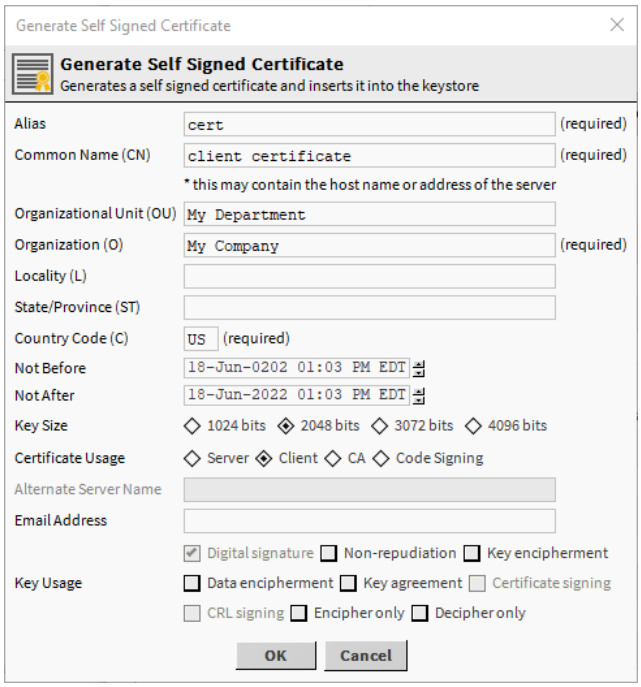
Creating and exporting the client certificate

A certificate authenticates the display to the station that manages the device. You need a separate certificate for each display.

Prerequisites: You are working in Workbench connected to the station that manages the display device.

Step 1 To create a client certificate, expand**Config→Services→PlatformServices**, double-click **CertManagerService** and click **New**.

The **Generate Self Signed Certificate** window opens.



Step 2 Enter values for at least these required properties:

- **`Alias`** provides the certificate name. Enter it as "cert." This is a required name.
- **`Common Name`** should match the display user you will set up with certificate authentication.
- **`Organization`** is your company.
- **`Country Code`** is the two-character ISO CODE you can find at `countrycode.org`.

Step 3 Select `Client` for **`Certificate Usage`** and click **OK**.

The certificate appears in the **`User Key Store`**.

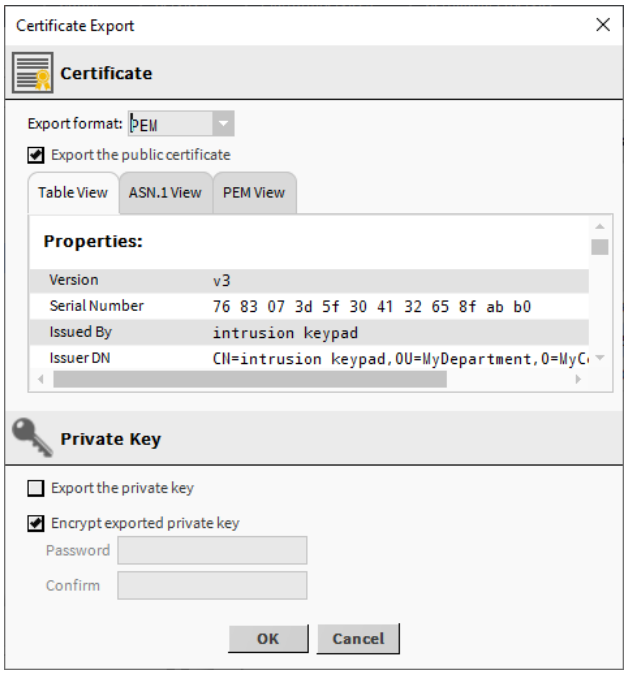
The next step exports the certificate so that you can associate it with the display user you just created.

Step 4 To export the certificate, select it in the **`User Key Store`** and click **Export**.

The certificate file is located here: `C:\Users\<your user>\<Niagara Version>\tridium\certManagement` where:

- `<your user>` is your user name
- `<Niagara Version>` is the folder that contains the Niagara software

The **Certificate Export** window opens.



Do not export this certificate with its private key.

Step 5 To continue, click **OK**, store the certificate's `.pem` file where you can find it later and click **OK** again to close the **Certificate Export** window.

The next step sets up single sign-on in the **AuthenticationService**.

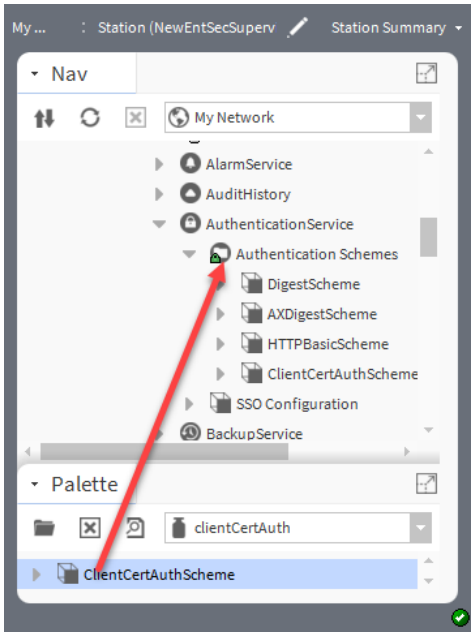
Setting up authentication

Client authentication verifies that a keypad user is authorized to connect to the security system. This user is not a person, rather it represents the Niagara Touch display.

Prerequisites: You are working in Workbench connected to the station that manages the display device. The station has an AuthenticationService in the Services folder.

Step 1 Expand **Config→Services→AuthenticationService→AuthenticationSchemes**.

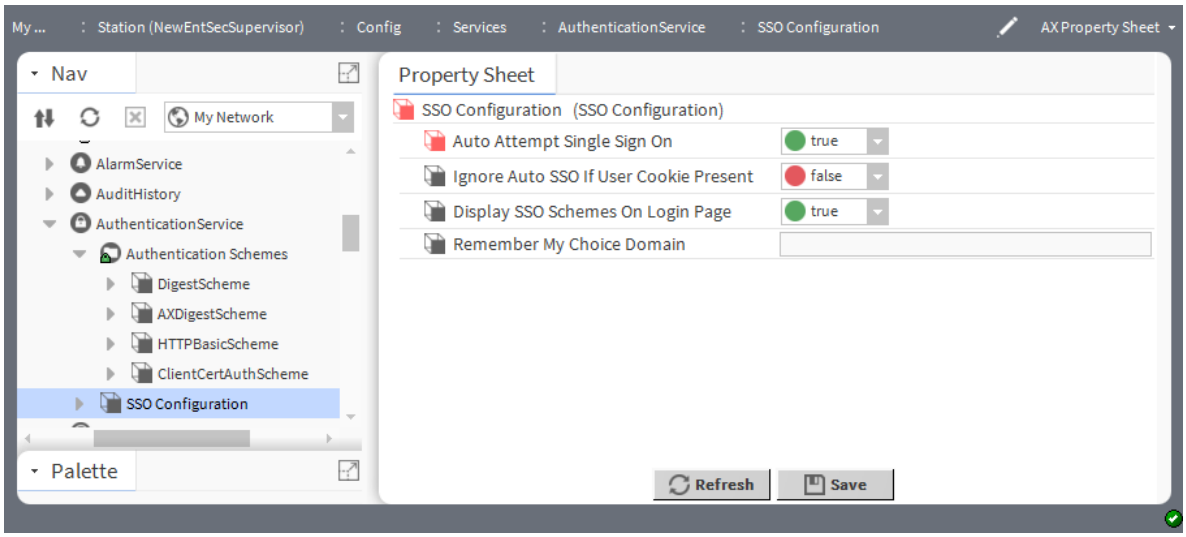
By default, this station comes with one **ClientCertAuthScheme**.



Step 2 If you need a second scheme, open the **`clientCertAuth`** palette and drag the **ClientCertAuth-Scheme** component from the palette to the **Authentication Schemes** node under the **AuthenticationService**.

Step 3 Double-click **SSO Configuration** (this component is at the same level as **Authentication Schemes** under the **AuthenticationService**).

The SSO Configuration **AX Property Sheet** opens.



Step 4 Set **`Auto Attempt Single Sign-On`** to `true`, confirm that **`Ignore Auto SSO if User Cookie Present`** is set to `false` and click **Save**.

The next step associates the exported certificate with the display user.

Setting up a display user

This system user represents the Niagara Touch display, which is authorized to connect to the station and should be configured with the most restrictive role and permissions possible. This procedure creates this

user and assigns the authentication certificate you created to this user. You will need a separate user for each display.

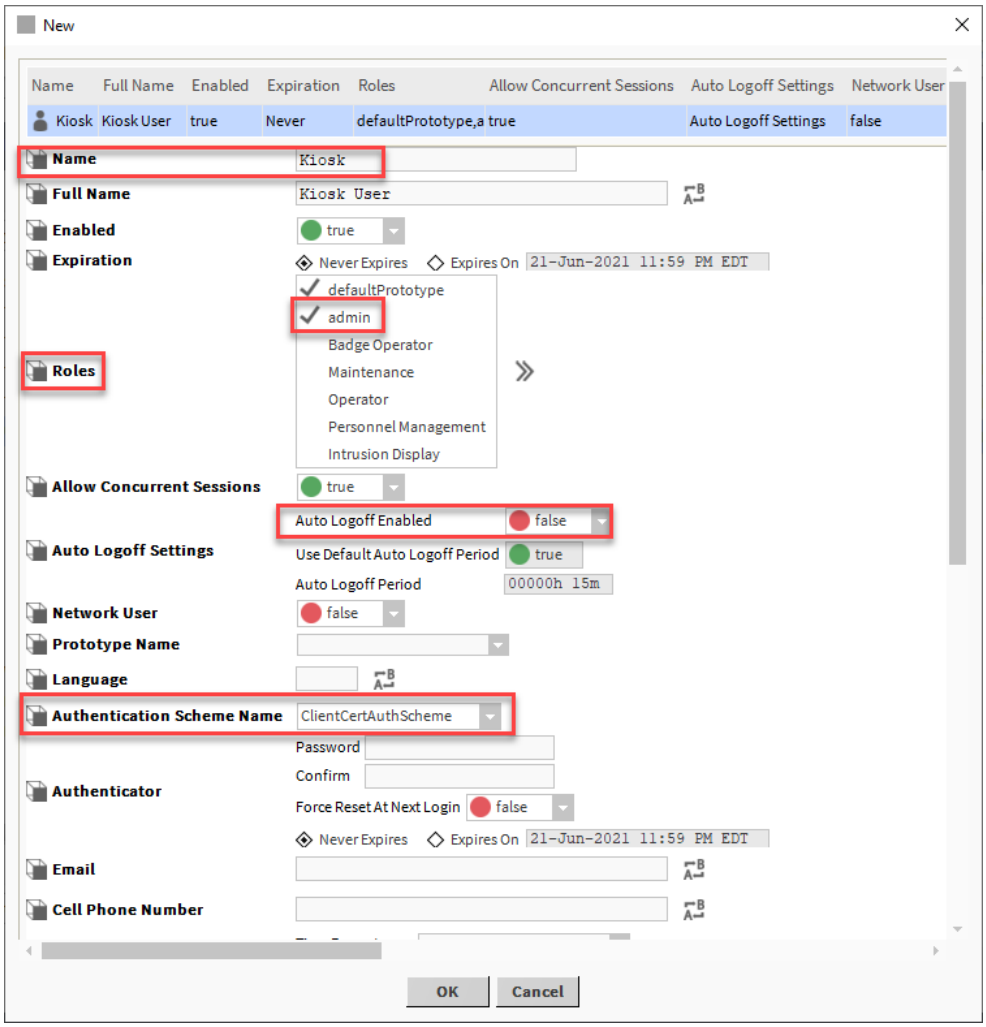
Prerequisites: You are working in Workbench connected to the station that manages the intrusion zones.

Step 1 Expand **Config→Services** and double-click the **UserService**.

The **User Manager** opens.

Step 2 To create the user for the client certificate you created, click **New**, select the number of users to create and click **OK**.

The **New** view opens.

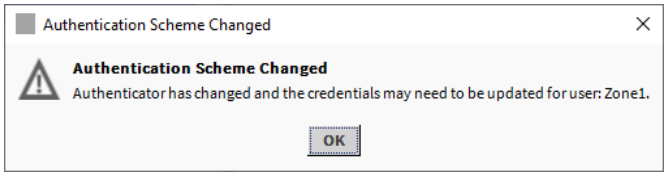


Step 3 Enter values for at least these properties:

- **`Name`** can be the **`Common Name`** you used for the certificate.
- **`Roles`**, for now assign the `admin` role. You will change this later to the most restrictive role.
- Under **`Auto Logoff Settings`**, remove the check mark to select `false` for **`Auto Logoff Enabled`**.
- **`Authentication Scheme`**, set to `ClientCertAuthScheme`.

Step 4 To accept the changes and save the user, click **OK**.

The software alerts you that the credentials for the user need to be updated.

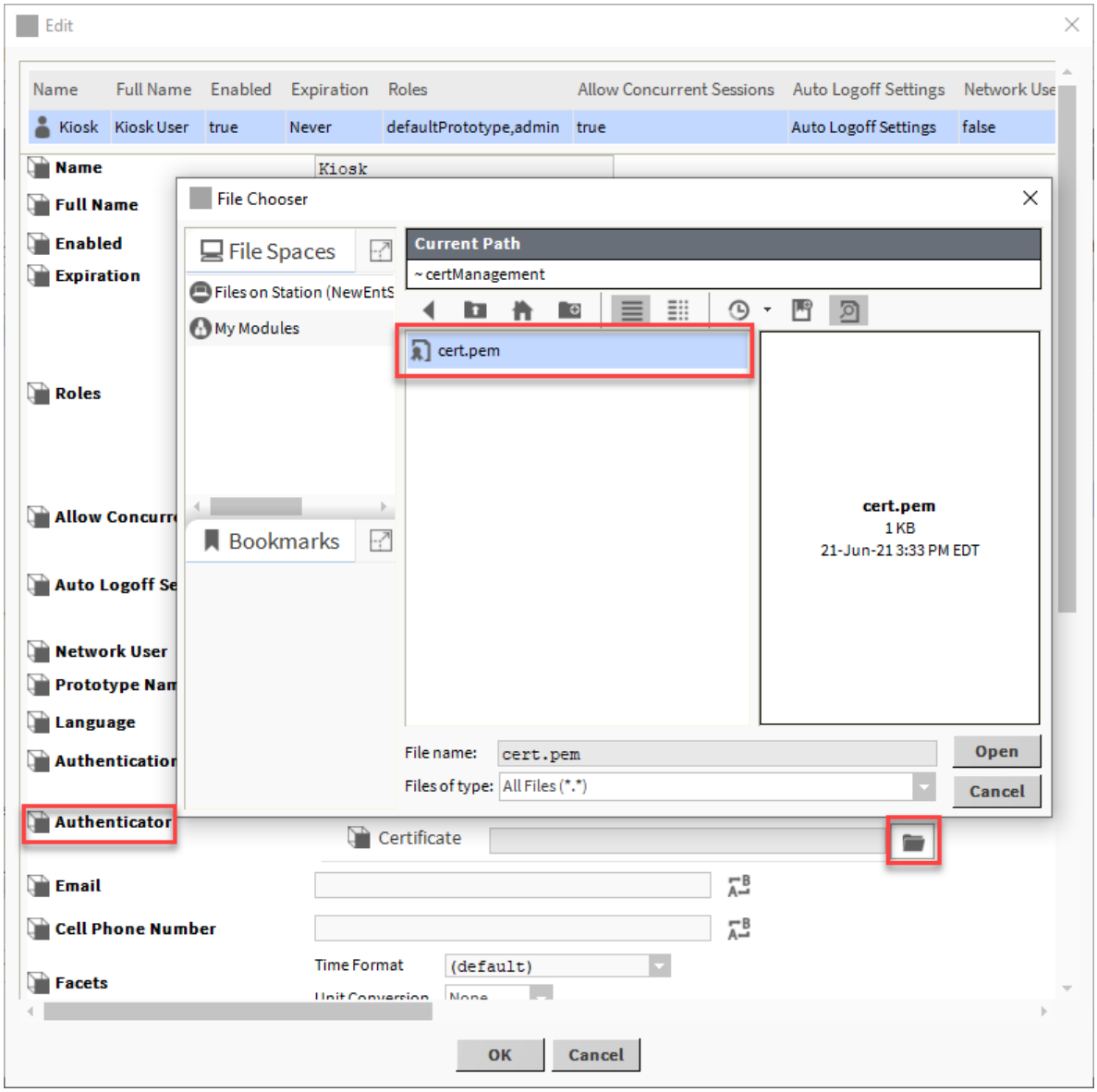


Step 5 To assign the certificate to this user, open the user again by double-clicking **UserService**, select the user you just created and click **Edit**.

The **Edit** window opens.

Step 6 Scroll down to **Authenticator** and under **Certificate**, click **Choose File**.

A **File Chooser** window opens.



Step 7 Navigate to the client certificate you created and, to assign the certificate to this user, select the certificate and click **Open**.

If you used the default location, double-click **User HomeCertManagement**.

The system advises you that the **FoxService** and **WebService** need to restart.

Step 8 To save the change you just made, click **OK**.

Next, for Niagara 4.9 and earlier, you export the same certificate, but this time with its private key. Then, for all versions you add the certificate to the server socket's TrustAnchor list. You will return to this user to configure more properties later.

Exporting the certificate with its private key (Niagara 4.9)

If you are using Niagara 4.9 you may export the display certificate with its private key. This provides the most robust security for data communication.

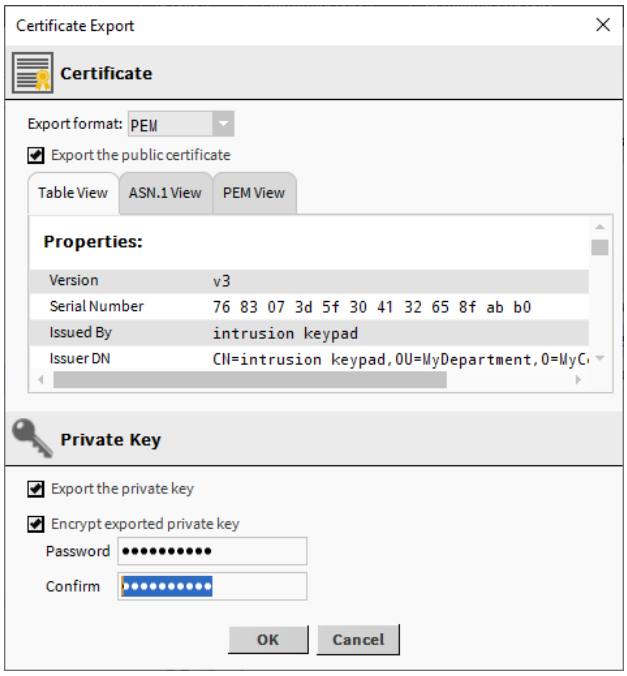
Prerequisites: You are using Niagara 4.9 or earlier. You are working in Workbench running on a PC. You are connected to the station that manages the display device.

If you are using Niagara 4.10 or later you do not need to export the certificate with its private key. You can use the .pem file you exported to configure the **UserService**. OpenSSL does not support .pem files and private keys exported from Niagara 4.10.

NOTE: The private key of the server certificate validates the public key presented to the display by the client station. A server certificate without a private key is less secure than one with its private key. Without the encryption of the private key, a malicious user could install the certificate into devices that should not be allowed to make a connection. However, when a PIN is involved, as it is with arming and disarming an intrusion zone, the risk is low.

Step 1 To export the certificate with its private key, expand **Config→Services→PlatformServices**; double-click **CertManagerService**; in the **User Key Store**, select the certificate you created and click **Export**.

The **Certificate Export** window opens.



Step 2 Enable **`Export the private key`**, create and confirm a strong password to protect the key, record the password in a safe location and click **OK**.

A **File Chooser** window opens.

Step 3 Save the file in a location other than the location you used for the first save, for example, `C:\certs`.

Since you will use an OpenSSL command prompt to convert the .pem file to a .p12 file, a short path will make it easier to enter the commands.

The next procedure downloads OpenSSL to create a .p12 certificate.

Preparing the .p12 server certificate

OpenSSL converts a .pem certificate file to a .p12 certificate file. The display recognizes this format.

Prerequisites: You are working in Workbench running on a PC. You are connected to the station that manages the display device.

Step 1 Download the appropriate version of OpenSSL for Windows and install it.

Multiple sites provide pre-compiled executables. For example, you can download it from here: `https://slproweb.com/products/Win32OpenSSL.html`.

More information about OpenSSL is available here: `https://www.openssl.org/source/`

This YouTube video provides a tutorial for setting up OpenSSL: `https://www.youtube.com/watch?v=jSkQ27sTto0`

Step 2 Follow the instructions to install OpenSSL.

Step 3 Open an OpenSSL command prompt and change your directory to the folder that contains the certificate you exported, for example: `cd\certs`.

Step 4 To run the OpenSSL conversion from the command prompt, type this command and press **Enter**.

`openssl pkcs12 -export -out cert.p12 -in <your cert> -inkey <your cert>.pem`

The output certificate name must be `cert.p12`.

OpenSSL prompts you to enter the pass phrase for the Niagara 4.9 (or earlier) certificate you exported with the private key.

Step 5 Do one of the following:

- For Niagara 4.9, enter the password you created when you exported the certificate with its private key.
- For Niagara 4.10, press **Enter**.

OpenSSL prompts you to create and confirm its password. Both certificates with and without an export private key require this .p12 password.

Step 6 Enter, verify and record this password in a safe place.

OpenSSL creates a new certificate with the .p12 extension and associated password.

Step 7 Confirm that the new certificate exists and move it to a secure location.

You do not want an unauthorized person to have access to this certificate.

The next step is to install the .p12 certificate in the display.

Installing the .p12 certificate

The display requires the server certificate to make a secure connection to the station.

Prerequisites: Your display is charged and ready to use. Your network router is within range so that the display can connect to it using WiFi.

Step 1 Save the .p12 certificate to a USB thumb drive or MicroSD card.

The USB adapter comes with the display unit.

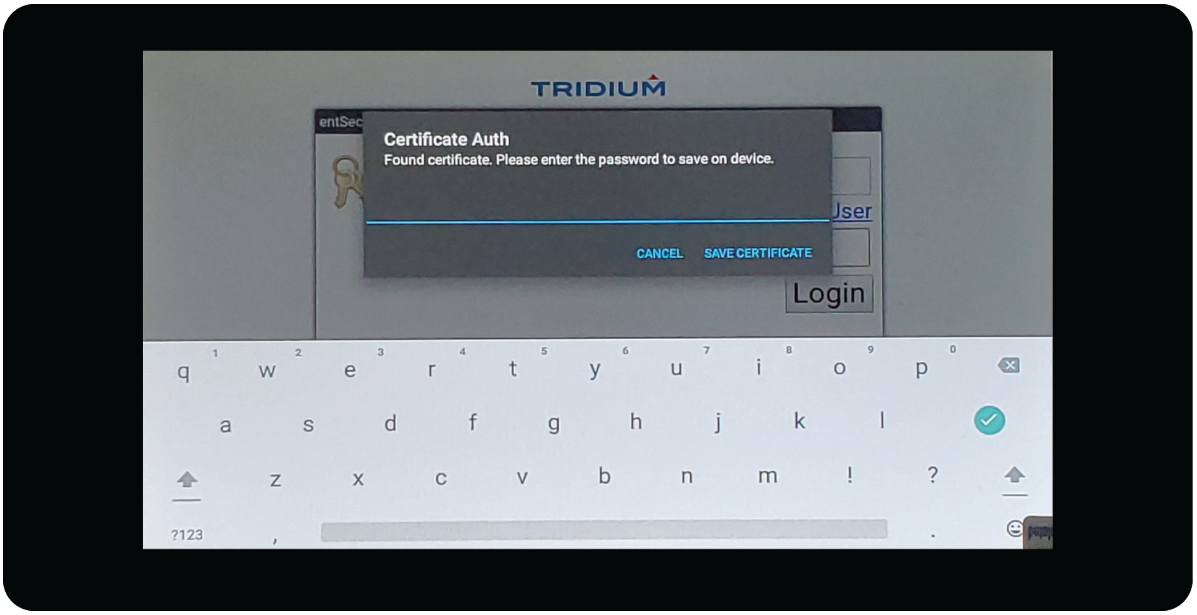
Step 2 Use the adapter to connect the USB thumb drive to the display's mini-USB connector or insert the MicroSD card.

Step 3 Turn on the display (the on/off button is the small button to the right of the mini–USB receptacle on one end of the display).

A start-up splash screen opens followed by a screen with this instruction: **TAP HERE FOR SETTINGS** as the device connects to your local area network.

Step 4 Tap **TAP HERE FOR SETTINGS**.

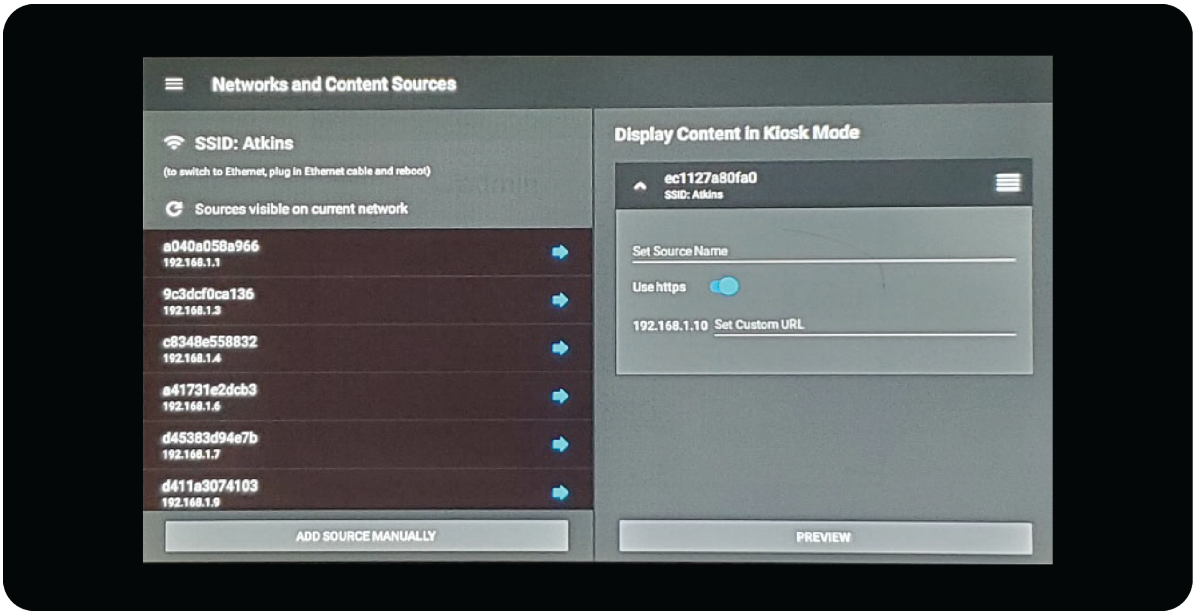
The display finds the certificate on the thumb drive or MicroSD card, imports it and opens the **Certificate Auth** window.



If, for any reason, you need to return to the first screen that reads, **TAP HERE FOR SETTINGS**, press the on/off button, and select `Restart`.

Step 5 Using the onscreen keypad, enter the password you created when you exported the certificate using OpenSSL and tap **SAVE CERTIFICATE**.

The **Networks and Content Sources** view opens.



On the left, under “Sources visible on current network” is the list of devices that are connected to your network.

Step 6 Using the IP address of the remote controller station, scroll down the list on the left, find the controller and tap the blue, right-pointing arrow.

The controller appears under the “Display Content in Kiosk Mode” list.

The display supports only one source at a time. If more than one source appears in the list on the right, swipe to the left over the source you do not need. This exposes a delete option (white X on a red square). Tap this X to delete the extra option.

Step 7 Expand the source by tapping the down arrow and tap to turn on **`Use https`**.

This enables secure communication between the display and controller station.

Step 8 To preview the connection, tap **PREVIEW**.

Step 9 Assuming the connection works as expected, tap **LAUNCH**.

The display connects to the controller station using certificate authentication.

Step 10 In the browser, select `Log in with SSO` using the user you created in the station.

You do not need to input a password as the display recognizes the certificate you installed. The display automatically logs in using this user each time it reboots.

Chapter 3 Workbench Configuration

Topics covered in this chapter

♦ Setting up a navigation file
♦ Creating a role to assign to the display
♦ Updating the user assigned to the display

How to configure and associate the display device with the station depends on its application.

For example, to configure a Niagara Enterprise Security intrusion keypad you associate the display device with a zone and configure the Px view for the onscreen keypad. Similar tasks are required for use with another application. You may use Workbench to configure the device in the station or you may have a custom-designed Web UI.

Setting up a navigation file

The onscreen Px view serves as the home page for the display user. When a person turns the display on, it defaults to this page. You need a separate .nav file for each display.

Prerequisites: You are working in Workbench connected to the controller station.

Step 1 Create a folder under the station's **Files** node named **Nav**.

Nav files must reside under the **Files** node. They are not stored in the station database.

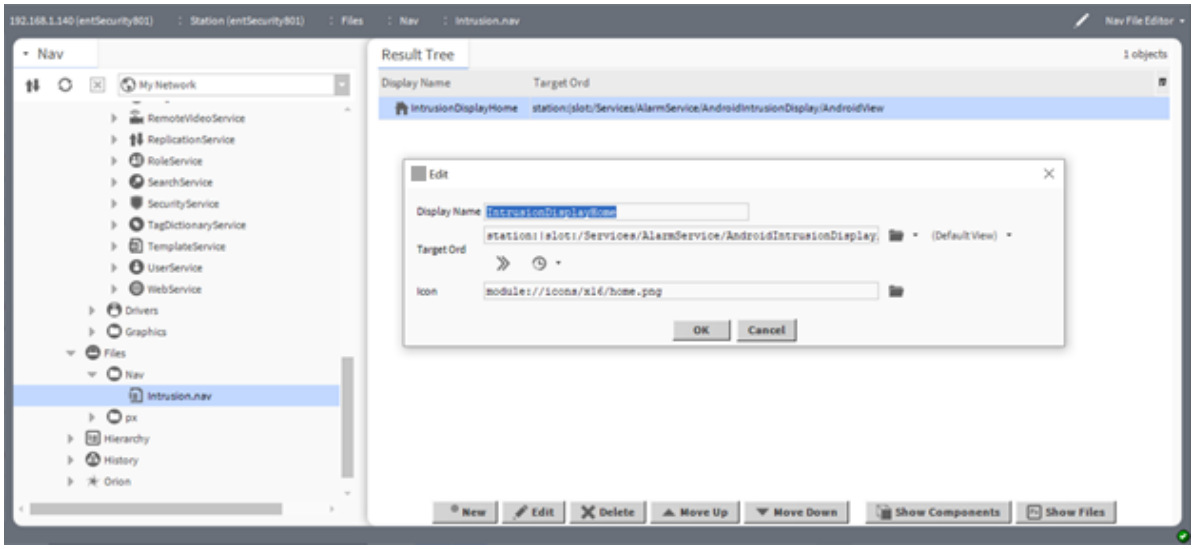
Step 2 To create a new .nav file, right-click the **Files** node and click **New→NewFile.nav**.

The **Name for New File** window opens.

Step 3 Give the .nav file a name, click **OK** and expand the **Files** node.

Step 4 To associate the .nav file with the onscreen display, double-click the file name, select the slot and click **Edit**.

The **Edit** window opens.



Step 5 Click the folder icon and use the **File Ord Chooser** to select the location of the display folder.

In the example, this location is: `station:|slot:/Services/AlarmService/AndroidIntrusionDisplay/AndroidView`.

The next procedure creates an display role.

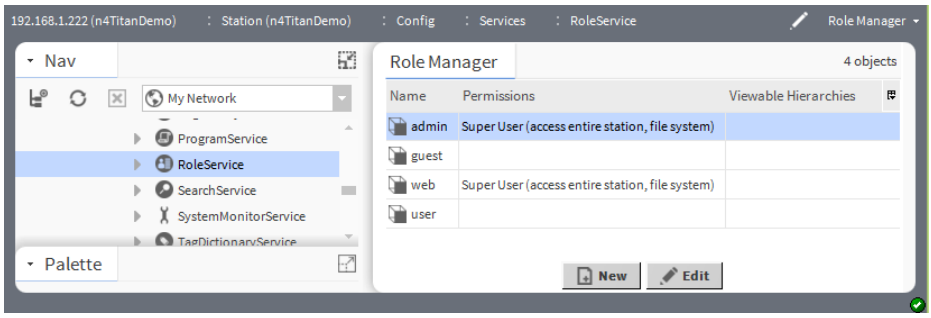
Creating a role to assign to the display

This special role limits the actions that a person can perform with the display to only those related to the application. For example, you would limit the actions a user can perform using an onscreen intrusion keypad to arming and disarming intrusion zones.

Prerequisites: You are working in Workbench connected to the controller station that manages your building's intrusion zones.

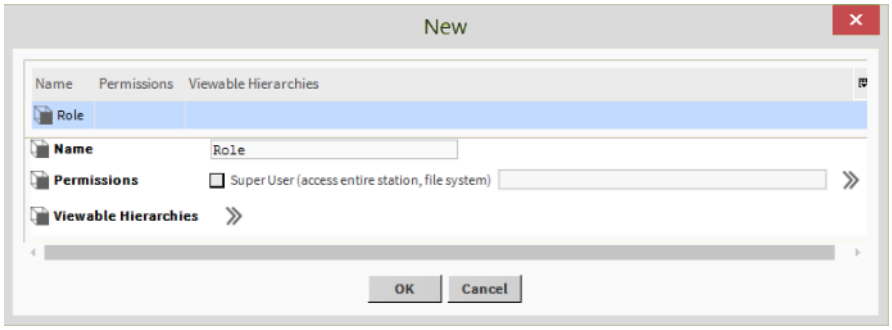
Step 1 Right-click **RoleService** in the Nav tree, click **Views→Role Manager**.

The **Role Manager** view opens.



Step 2 Click the **New** button, enter the number of roles to create in the pop-up window and click **OK**.

The system displays the **New** window with a row for each role you are creating.



Step 3 To set up individual permissions, click the chevron at the end of the **`Permissions`** property.

The **Permissions** map opens.

Step 4 Click the cell to assign read (R) and invoke (I) permissions for the application categories and click **OK**.

The permissions appear in the **`Permissions`** property of the **New** window.

Step 5 To finalize permissions, click **OK**.

Step 6 In a multi-station system, perform these same steps in each station so that each station has the same set of roles.

NOTE: During the network user synchronization process the framework sends the user's role assignment to the receiving station, however, it does not create the actual role(s) on the receiving station. You must set up matching roles on each receiving station before synchronizing network users.

Updating the user assigned to the display

You already set up this user when you created and assigned the certificate to it. This procedure updates this user with additional information: role, .nav file and other information.

Prerequisites: You are working in Workbench connected to your station that manages the display device.

Step 1 Expand **Config→Services** and double-click the **UserService**.

The **User Manager** opens.

Step 2 To edit the existing user, select it in the table and click **Edit**.

The **Edit** window opens.

Step 3 Configure these properties:

- For **Roles**, assign the name of the role you created, for example, `Intrusion Display`
- For **Nav File**, assign the name of the file you created, for example, `file:^Nav/Intrusion.nav`
- For **Allow Concurrent Sessions**, select `false`

Step 4 Configure the **Default Web Profile**, `HTML5 Hx Profile` as follows:

- Enable Hx Workbench View = Yes
- Enable Nav Tree Side Bar = No
- Enable Search Side Bar = No
- Enable Nav File Tree = No
- Enable Config Tree = No
- Enable Files Tree = No
- Enable Histories Tree = No
- Enable Hierarchies Tree = No
- Enable View Selection = No

Step 5 For the **Mobile Web Profile**, configure properties as follows:

- For **Mobile Nav File** enter the name of the file you created, for example, `file:^Nav/Intrusion.nav`.
- Set **Type** to `Handheld Hx Profile`.

Step 6 When you finish setting up these properties, click **OK**.

The display should now be able to connect to your station. The role and permissions you configured for the display user are the minimum needed to operate the device. You can certainly add more permissions later. To ensure that your display always attempts to navigate to the correct station page, add a path to the url for your controller in the display setup of your station connection. Using the example of an intrusion keypad, the url for the display could be: `/ord/station:|slot:/Services/AlarmService/AndroidIntrusionDisplay/AndroidView`.

Chapter 4 Reference

Topics covered in this chapter

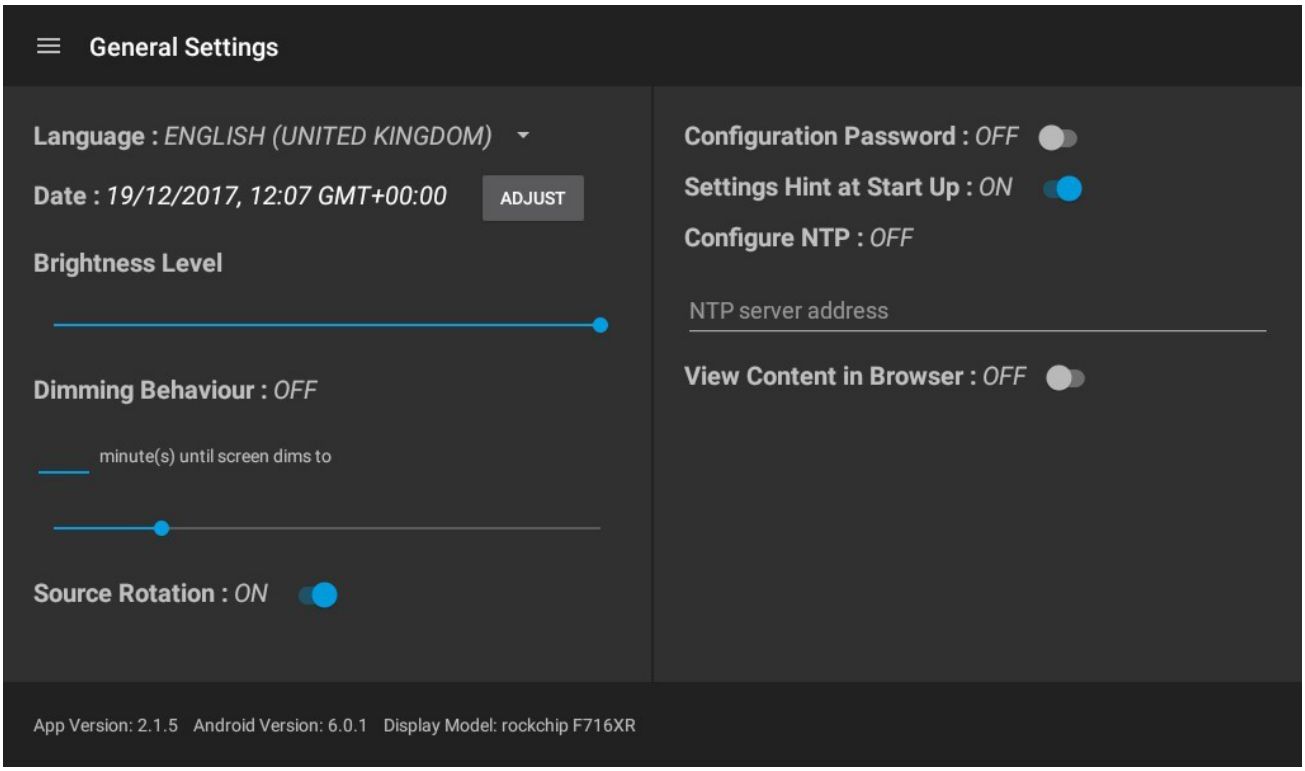
♦ General Settings
♦ Date & time

This chapter documents all configuration options.

General Settings

These settings control how the display behaves.

Figure 1 General Settings



To view these settings, expand the menu icon in the upper left corner of the view and click **General Settings**.

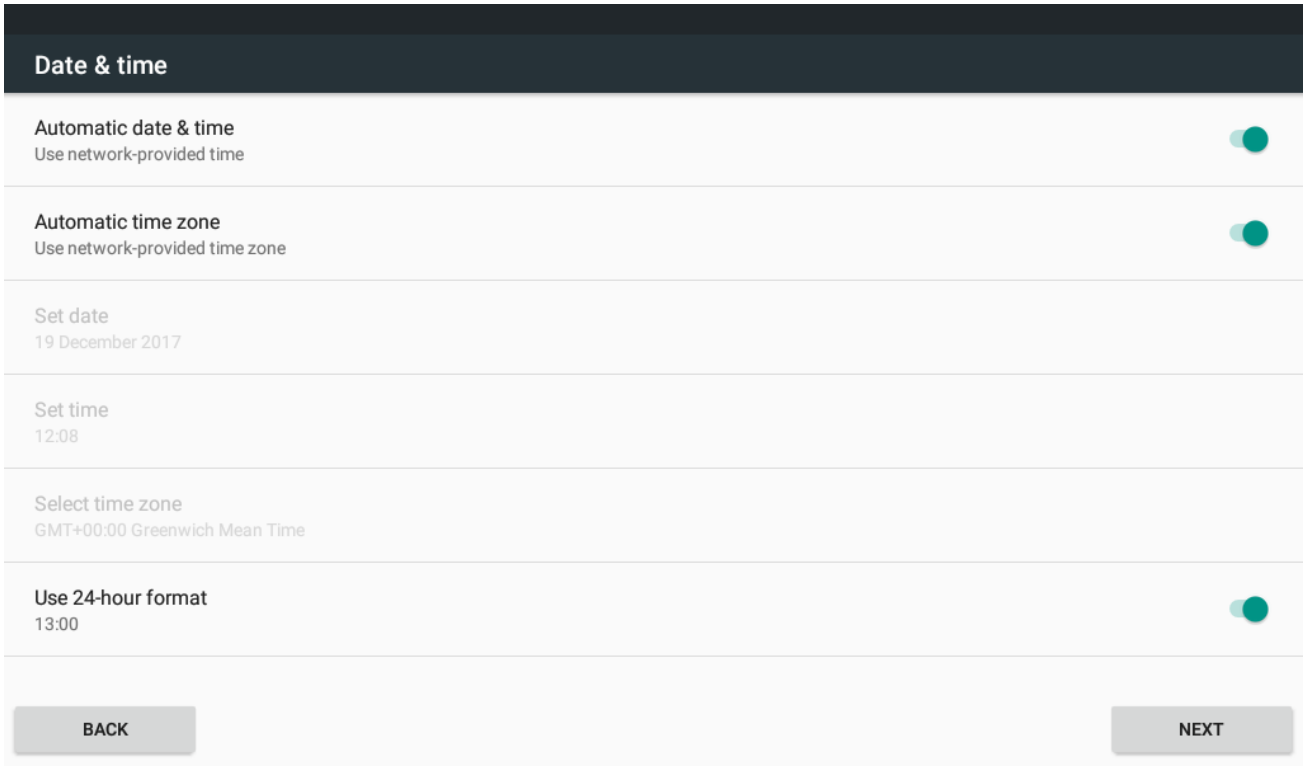
Setting	Value	Description
Language	drop-down list	Selects the supported language: two flavors of English and Español and Français.
Date	additional properties and **ADJUST** button	Configures the date, time and time zone.
Brightness Level	slider	Adjusts the dimming behaviour. To turn dimming off set the dimming value to zero (0) or blank. Move the slider to make the brightness level and dimming level the same.

Setting	Value	Description
		NOTE: If you turn off dimming, the display may display temporary image ghosting if a static image is displayed for a prolonged period.
Source Rotation	ON (default) and OFF toggle	Controls how the sources display in the view. You would turn this property off if you configure more than one source.
Configuration Password	ON and OFF (default) toggle	Enables (ON) and disables (OFF) the requirement to provide a password to access the configuration view.
Configure NTP	ON and OFF (default) toggle	Enables (ON) and disables (OFF) a required NTP (Network Time Protocol) server.
View Content in Browser	ON and OFF (default) toggle	Configures how to view content served by saved sources. `OFF` displays Internet content using the Kiosk browser within the display's app. This gives a full browser experience in a full-frame environment. `ON` expands the settings properties to offer two typical Internet browsers: • Google Chrome • Mozilla Firefox

Date & time

This view configures date, time and time zone properties.

Figure 2 Date and time properties



To view these settings, expand the menu icon in the upper left corner of the view, click **General Settings** and click **ADJUST** to the right of the date and time.

Setting	Value	Description
Automatic date & time	ON (default) and OFF toggle	Enables (ON) and disables (OFF) use of time provided by the network. Turn this property off to configure the time. Then turn it back on.
Automatic time zone	ON (default) and OFF toggle	Enables (ON) and disables (OFF) use of the time zone as provided by the network. Turn this property off to configure the time zone. Then turn it back on.
Set date	text	Enabled when Automatic date & time is OFF.
Set time	time	Enabled when Automatic date & time is OFF.
Select time zone	drop-down list	Enabled when Automatic time zone is OFF.
Use 24–hour format	ON (default) and OFF toggle	Enables (ON) and disables (OFF) the display of the time using a 24–hour clock.

Index

C

certificate
  conversion 40
  creating 33
  export for a display 39
  exporting without the private key 33
  for the display 40
  to connect to a display 35
configuration 43

D

date 48
display 7, 39–40
document change log 5

E

Ethernet source
  connecting 28
  connecting to 26

F

file management 33

G

general settings
  configuring 12
General Settings 47

I

installation 8

L

language
  selecting 8
locale
  setting 8

N

navigation file
  for the onscreen display 43
network
  connecting to 9

P

.p12 certificate 40
prerequisites 7

R

reference 47
region
  selecting 8
related documentation 5
role
  for display user 44

S

security 33
settings
  configuring 12
source
  connecting to 9
sources
  configuring 14
  managing 17

T

time 48
time zone 48

U

unpacking 7
user
  setting up to use a display 37, 45

W

Wi-Fi source
  connecting to 23