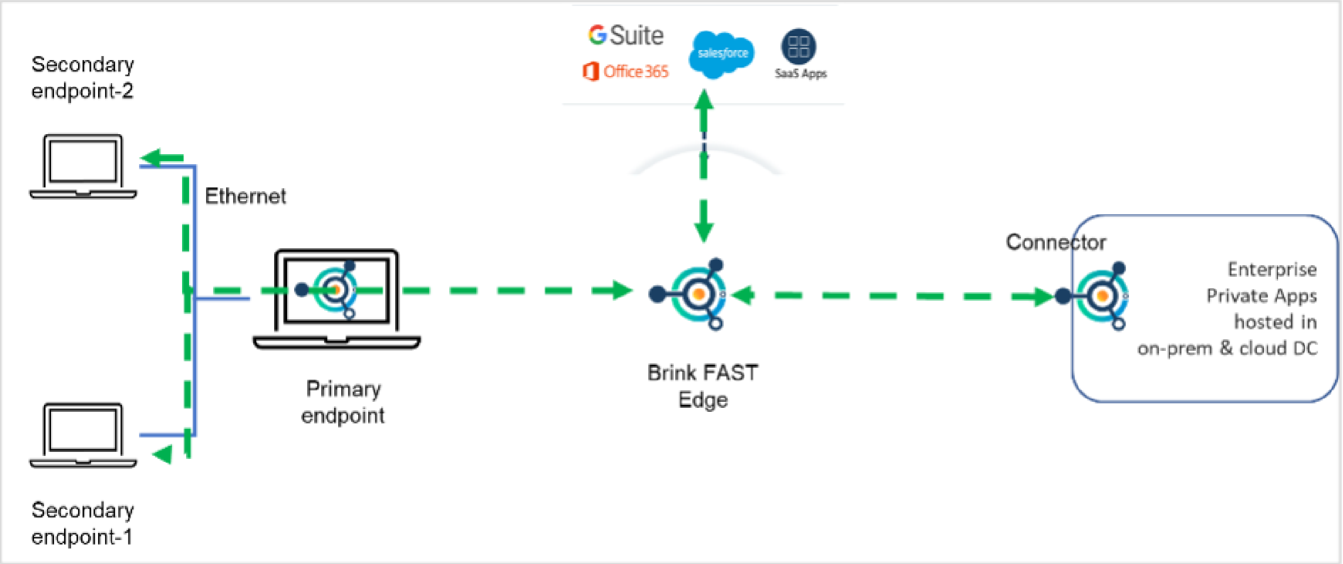
Bridge Mode Admin Guide

Cloudbrink's Bridge Mode enables users to connect more than one endpoint to enterprise private apps as well as SaaS apps through the primary endpoint on which the BrinkAgent is installed. All the other connected endpoints are referred to as secondary endpoints and do not require Brink App to be installed.

This guide outlines the process for configuring the Cloudbrink Admin Portal and BrinkAgent to effectively leverage Bridge Mode.



Introduction

This document will guide in setting up the Cloudbrink Device Session Profiles, and Policy for end users to be able to configure their devices for Bridge Mode. Bridge mode must be enabled by the Cloudbrink Administrator at each device-user-group level before the users can use the option to connect secondary endpoints.

Prerequisites

- A Cloudbrink connector deployed and configured with DHCP or static IP pool.
- Bridge Mode is only supported on Windows platforms. Primary endpoint must be a Windows 10/11 OS.
- Secondary endpoints may be any OS (Windows, Linux, Mac).

Bridge Mode Important Notes

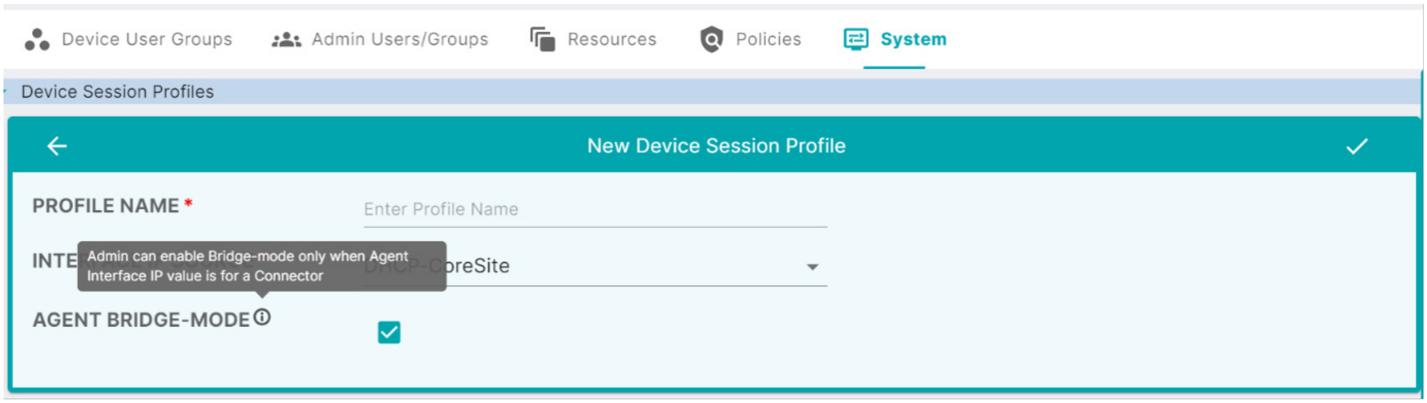
- When the secondary endpoint is connected to the primary endpoint via an L2/L3 switch, certain features such as physical interface flap on secondary endpoint may not detected on the primary endpoint (Brink Agent).
- To establish a "bridge" users must carefully choose the physical interface of primary endpoint to which secondary endpoints will be connected.
- The WAN Interface (internet providing interface) must not be used for bridge.
- After configuring bridge mode on the primary BrinkAgent endpoint, and connecting the secondary endpoint, ensure the secondary endpoint interface is flapped (DOWN/UP) so that secondary endpoint generates DHCP request
- It is recommended to setup the "Bridge" on the primary device first, then connect the secondary endpoint to that device.
- Certain secondary endpoint operating systems may need to have an MTU manually configured.

Admin Portal High Level Instructions

- Create a device session profile with "Agent Bridge Mode" checked.
- Create a device policy with a mapping to the appropriate profile.
- Map the device user group policy to the "Device Session Policy"

Admin Portal Detailed Instructions

1. From the admin portal, navigate to "Configure > System > Device Session Profiles".
2. Click on Device Session Profiles to drop down a list of profiles, and click the blue circle plus icon to create a new one.
3. In the new windows provide a profile name, select the connector that will be used to assign the enterprise private IP to the primary and secondary endpoint, and check the box to en-



PROFILE NAME * Enter Profile Name

INTE DHCP-CoreSite

Admin can enable Bridge-mode only when Agent Interface IP value is for a Connector

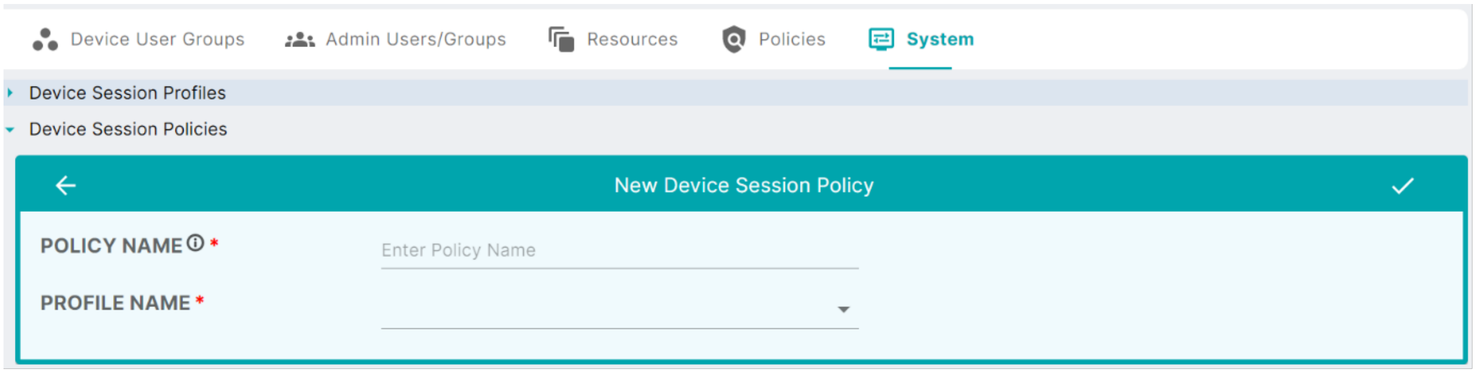
AGENT BRIDGE-MODE ☑

Note-1: Bridge-mode can be enabled only when a Connector is selected that will assign the enterprise private-IP to the endpoints. This restriction will be removed in future software.

Admin Portal Detailed Instructions - Cont

able "Agent Bridge Mode".

4. Still Under "System" expand out "Device Session Policies"
5. Click the blue circle plus icon to create a new policy.
6. In the new policy window, provide a name for the session policy, and select the profile created in the previous step from the drop down.



Device Session Profiles

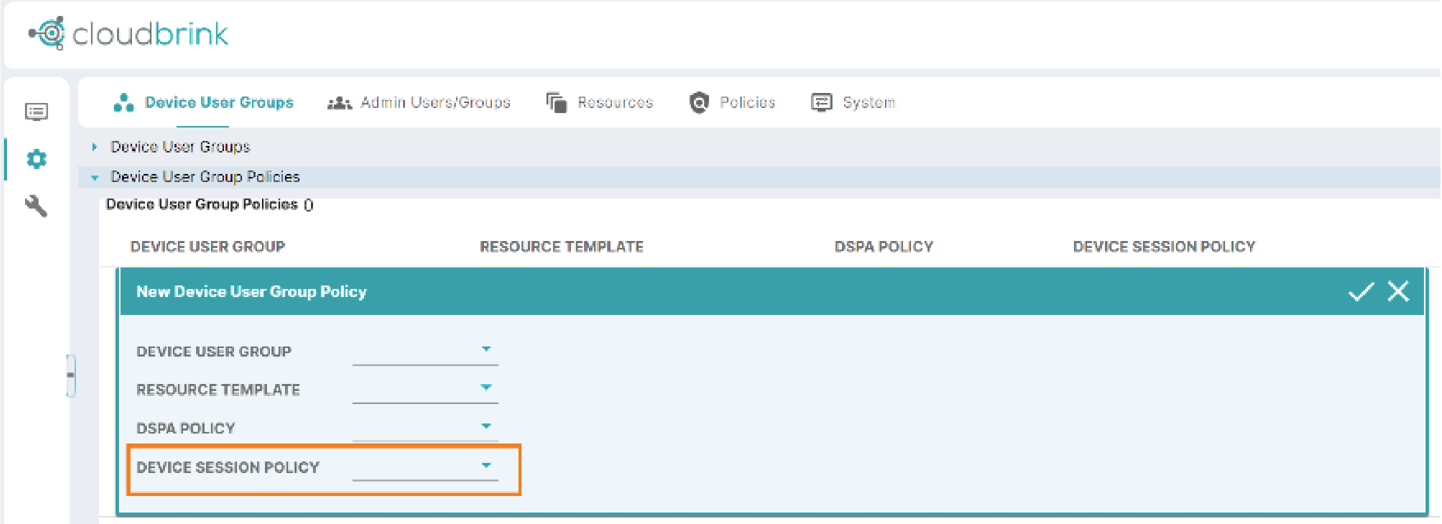
Device Session Policies

New Device Session Policy

POLICY NAME * Enter Policy Name

PROFILE NAME *

7. Next, Navigate to > Configure > Device User Groups > Device User Group Policies
8. Select the device user group to which the device session policy is to be assigned
9. In the assignment window, select the device session policy created in the previous step for "Device Session Policy" field.



Device User Groups

Device User Group Policies

Device User Group Policies ()

DEVICE USER GROUP	RESOURCE TEMPLATE	DSPA POLICY	DEVICE SESSION POLICY

New Device User Group Policy

DEVICE USER GROUP

RESOURCE TEMPLATE

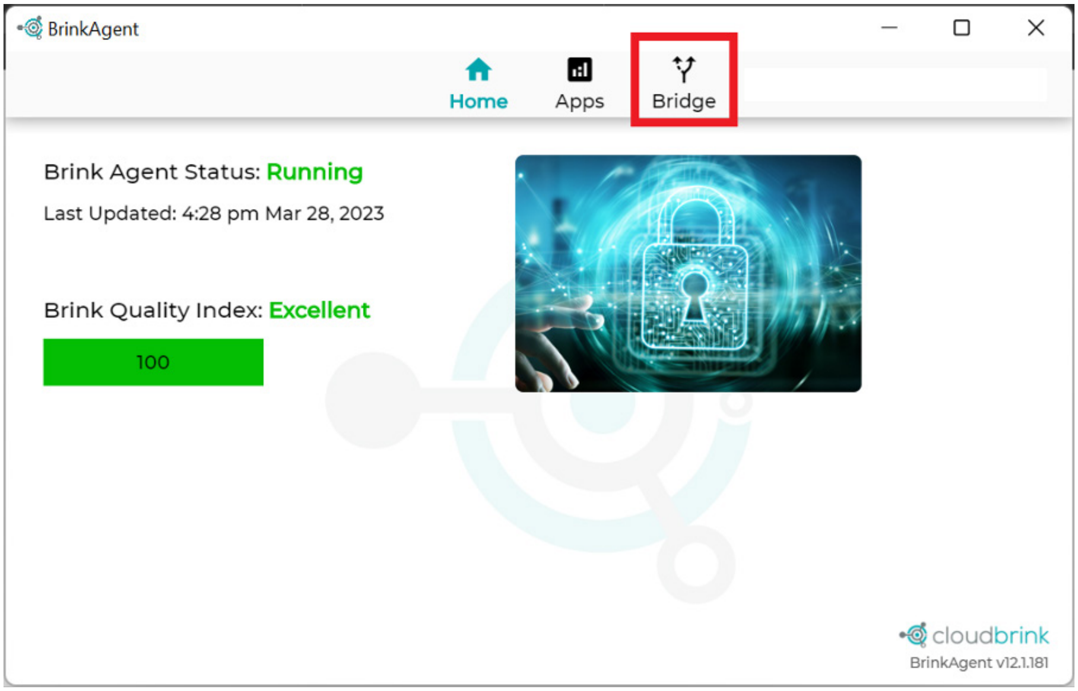
DSPA POLICY

DEVICE SESSION POLICY

10. This completes the configuration from the adminstrator side.
11. Once bridge mode is enabled for a device user group, users belonging to that security group will see a new option "Bridge" on the Brink App.

Bridge Mode - End User Config

1. When logging into the Brink App, users should now see a new tab "Bridge" once properly enabled.



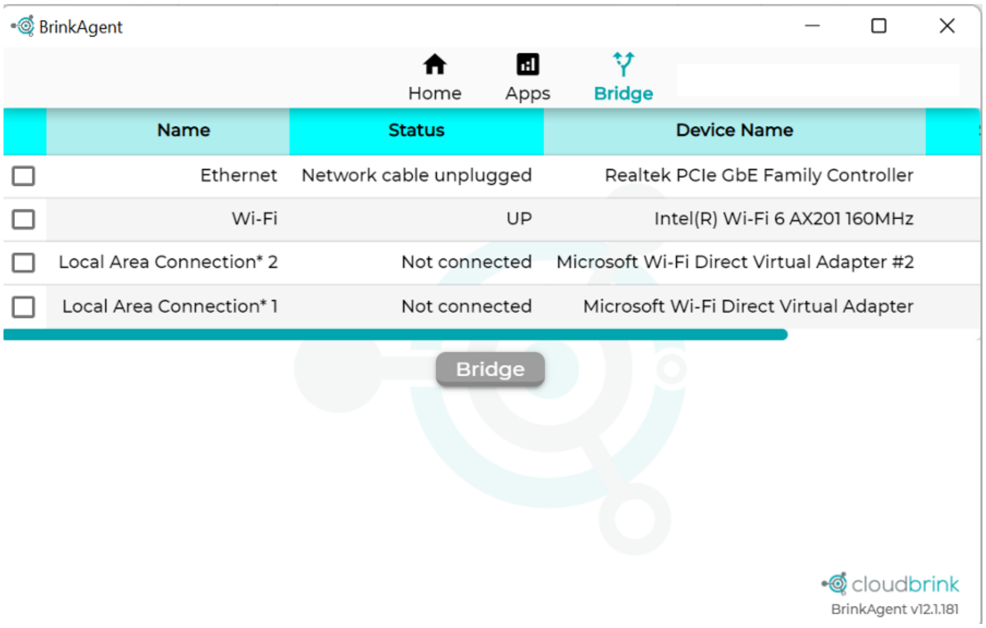
Brink Agent Status: Running

Last Updated: 4:28 pm Mar 28, 2023

Brink Quality Index: Excellent

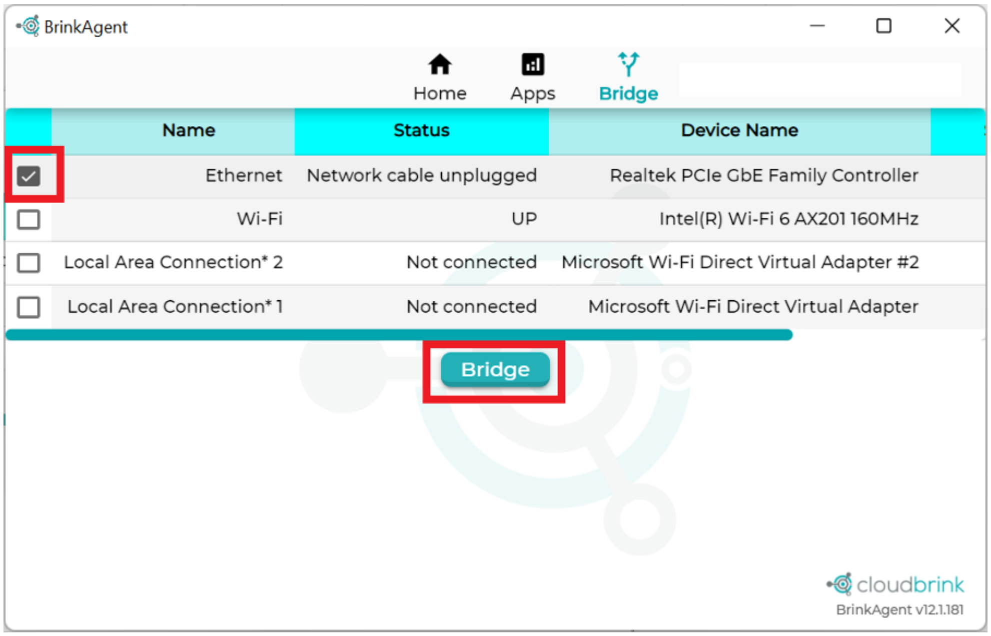
100

2. Click on the "Bridge" tab, and users will see all available interfaces on the primary endpoint.



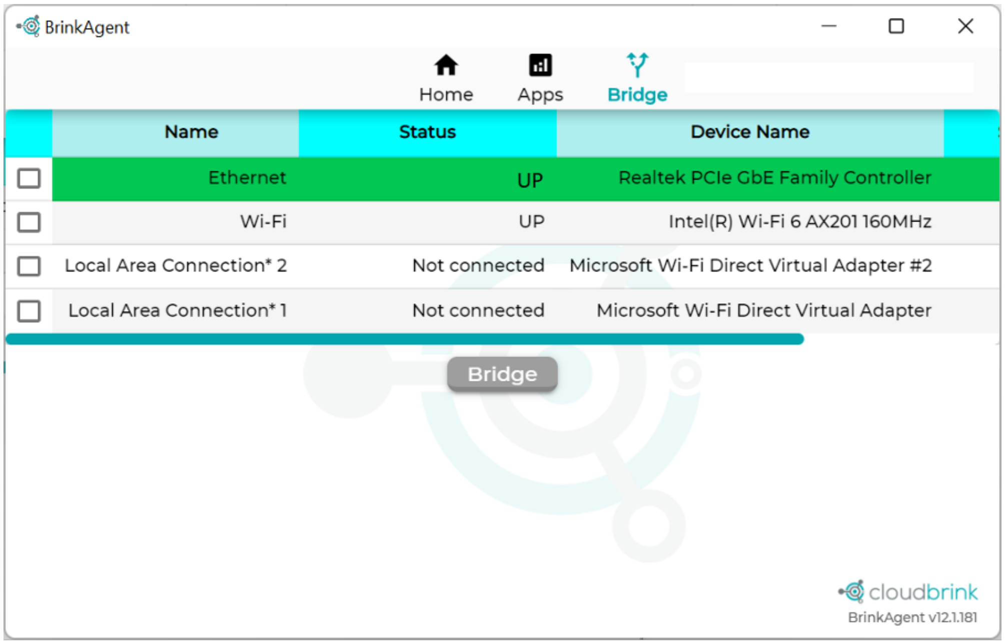
	Name	Status	Device Name
☐	Ethernet	Network cable unplugged	Realtek PCIe GbE Family Controller
☐	Wi-Fi	UP	Intel(R) Wi-Fi 6 AX201 160MHz
☐	Local Area Connection* 2	Not connected	Microsoft Wi-Fi Direct Virtual Adapter #2
☐	Local Area Connection* 1	Not connected	Microsoft Wi-Fi Direct Virtual Adapter

3. Check the box(es) to select the interface(es) you want to bridge out to a secondary device(s), and click on the "Bridge" button at the bottom.



	Name	Status	Device Name
☑	Ethernet	Network cable unplugged	Realtek PCIe GbE Family Controller
☐	Wi-Fi	UP	Intel(R) Wi-Fi 6 AX201 160MHz
☐	Local Area Connection* 2	Not connected	Microsoft Wi-Fi Direct Virtual Adapter #2
☐	Local Area Connection* 1	Not connected	Microsoft Wi-Fi Direct Virtual Adapter

4. Once the interface is successfully added to the "Bridge", connect the secondary endpoint to this interface to start accessing enterprise app from the secondary endpoint.



	Name	Status	Device Name
☐	Ethernet	UP	Realtek PCIe GbE Family Controller
☐	Wi-Fi	UP	Intel(R) Wi-Fi 6 AX201 160MHz
☐	Local Area Connection* 2	Not connected	Microsoft Wi-Fi Direct Virtual Adapter #2
☐	Local Area Connection* 1	Not connected	Microsoft Wi-Fi Direct Virtual Adapter