

Cloudbrink How-To Guide: Install a Brink Connector

Introduction	1
Prerequisites	2
Instructions	2
Login	2
Connector Configuration	3
Generate Connector Key	5
Cloud Init Customization Script	6
Connector Validation	7

Introduction

A Brink Connector enables enterprises to securely deliver applications hosted in a data center, private cloud, or public cloud to remote users working from anywhere. They enable end-to-end security and quality of experience (QoX) optimizations, from the end user device all the way to any applications specifically allowed by a Cloudbrink administrator.

For more information, please see [this video](#), which covers a typical Cloudbrink architecture as shown below.

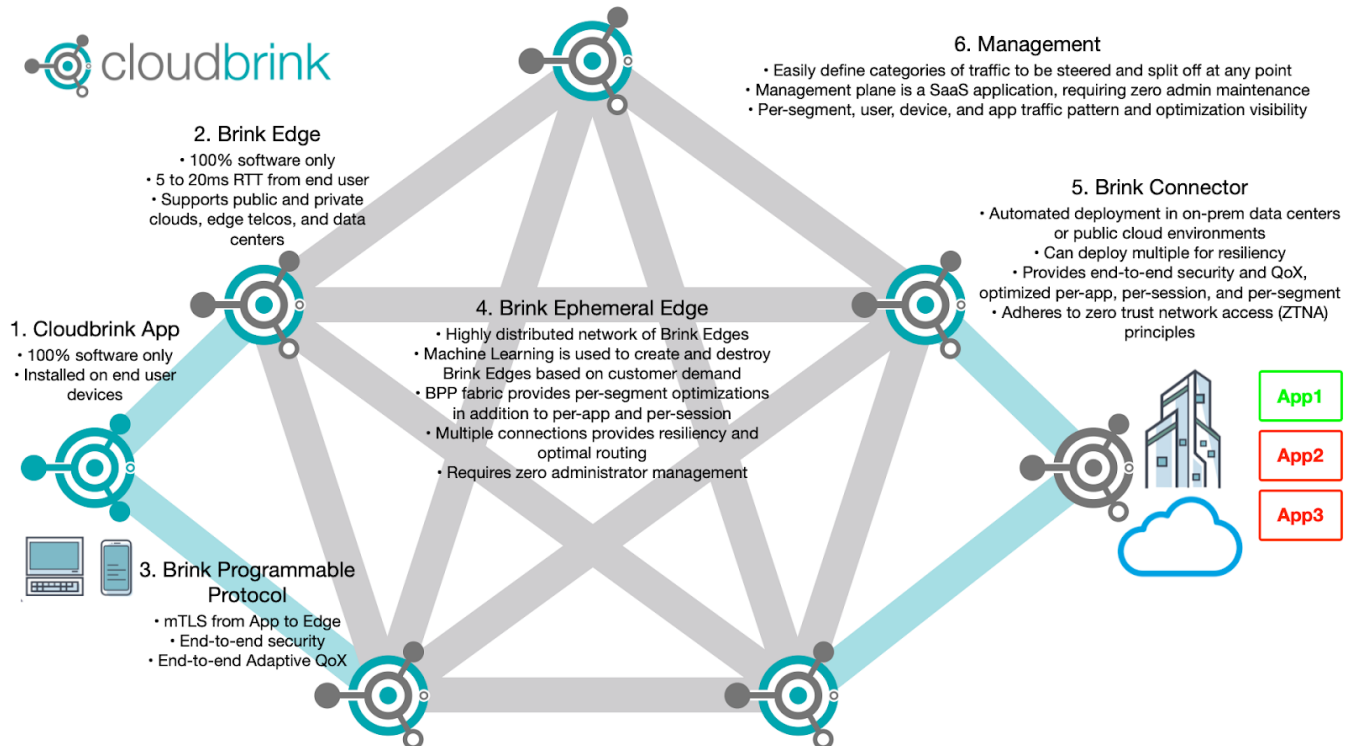


Figure 1: Typical Cloudbrink Architecture

Prerequisites

In order to successfully follow this documentation, please ensure the following prerequisites are met:

- 1.1. A Cloudbrink account with Super-Admin or Delegated-Admin privileges
- 1.2. Cloud or hypervisor credentials with privileges to deploy a virtual machine (and consume necessary compute and storage), depending on installation target
- 1.3. One or more Enterprise Services representing data center or cloud resources have been created (see **Create an Enterprise Service** section of the **Publish an Application** guide)

Instructions

Login

- 2.1. Navigate to <https://admin.cloudbrink.com>, and enter your **email** to be redirected to your organization's identity provider **login**.

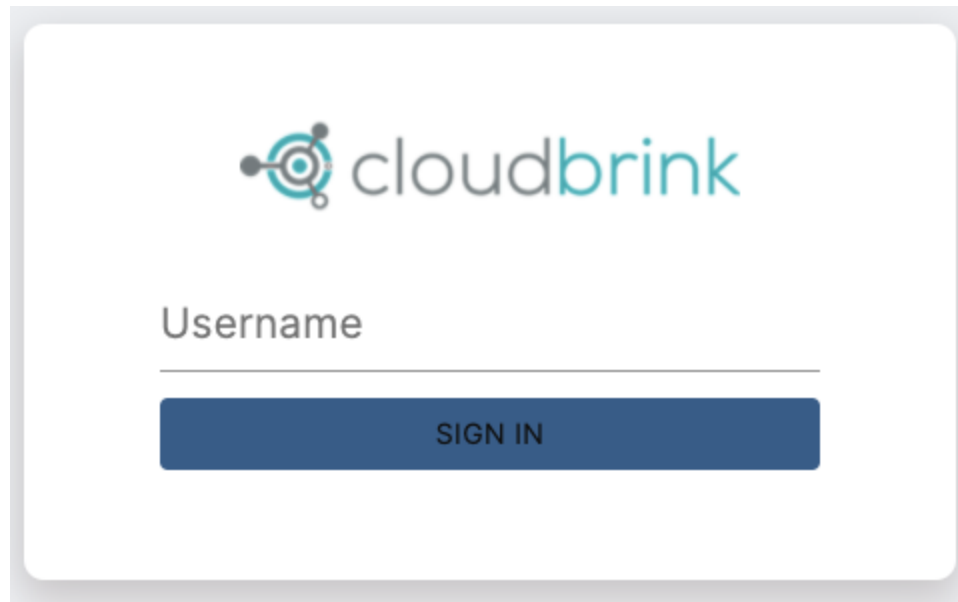


Figure 2: Cloudbrink Portal Login

2.2. After a successful login you'll be redirected to the Cloudbrink Dashboard.

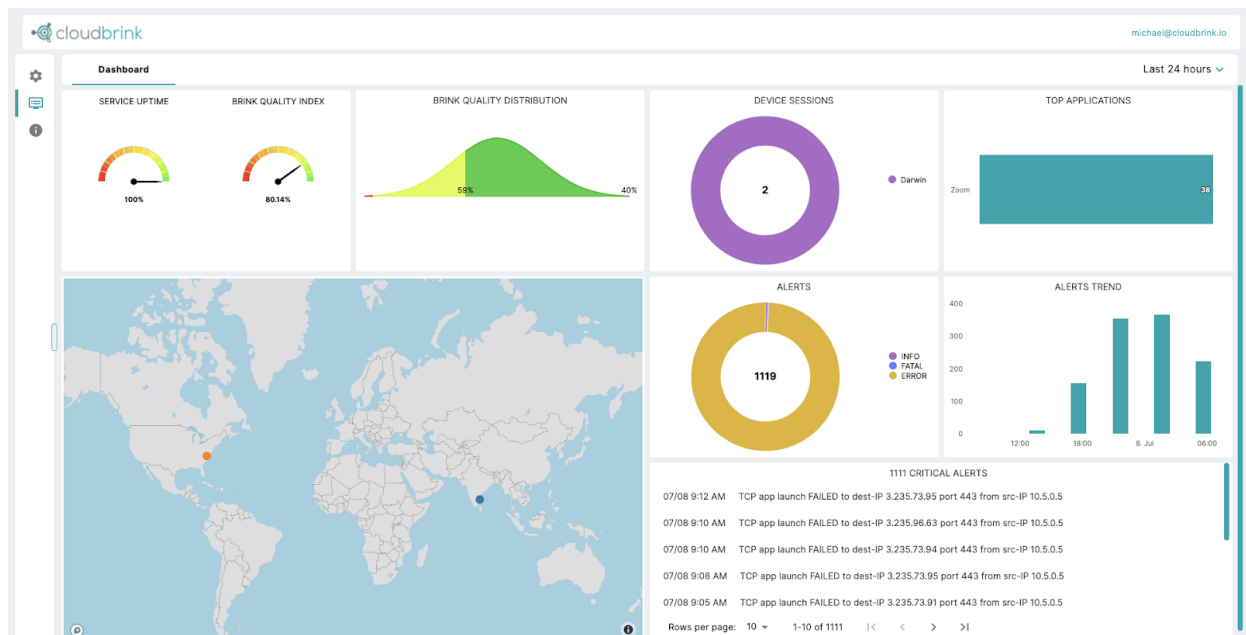


Figure 3: Cloudbrink Portal Dashboard

Connector Configuration

2.1. In the upper left corner of the Cloudbrink Portal, click either the **Gear Icon** or the **Configure** button (depending on whether the left menu is collapsed or expanded, respectively)

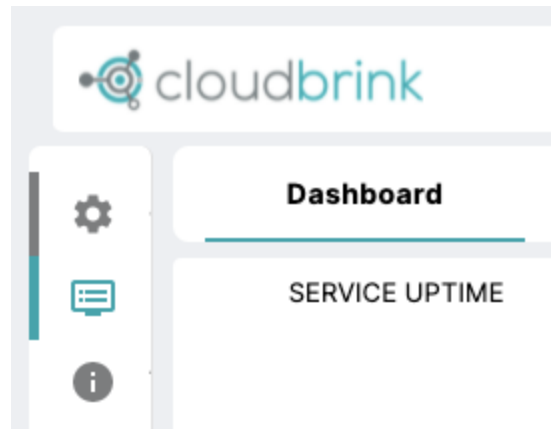


Figure 4: Gear Icon

- 3.1. On the page that appears, click the **Resources** tab

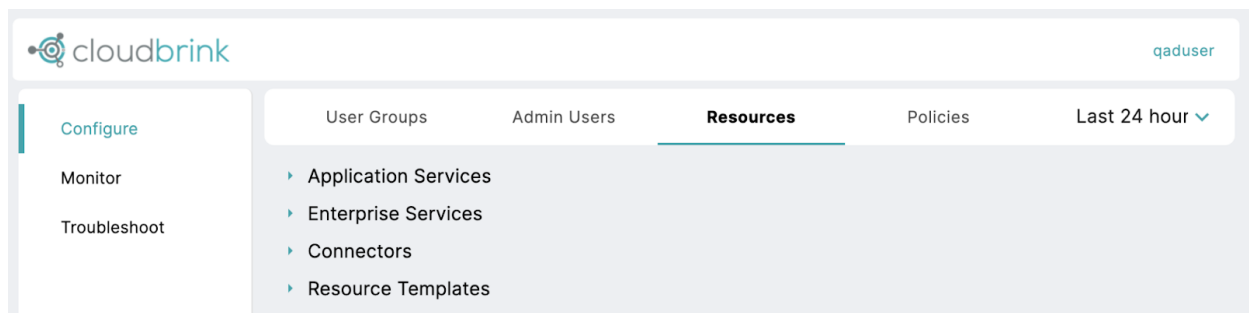


Figure 5: Configure: Resources

- 3.2. On the page that appears, expand the **Connectors** section, and click the **teal +** button

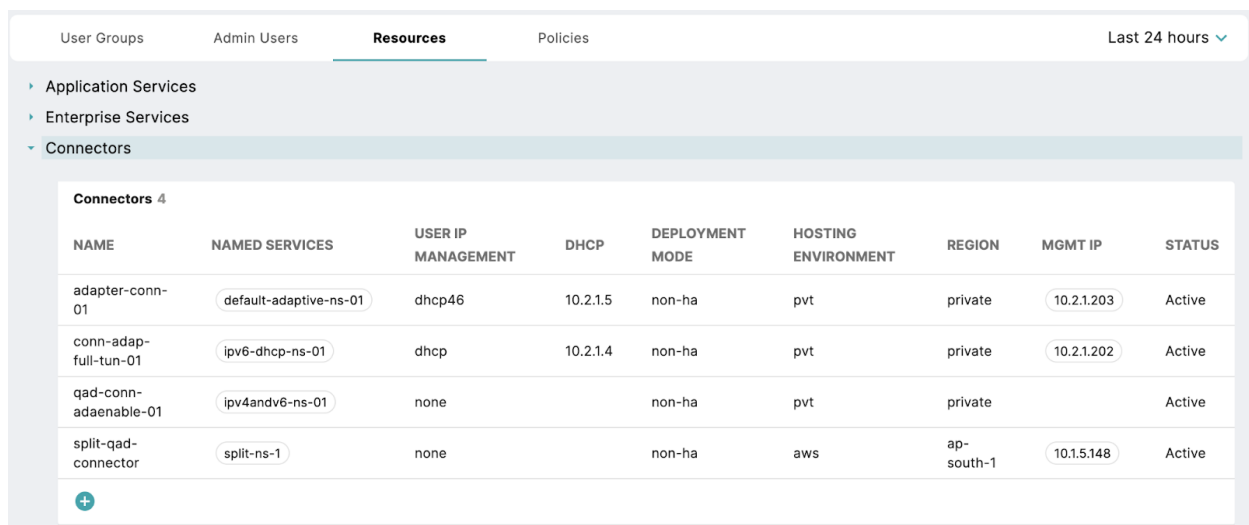
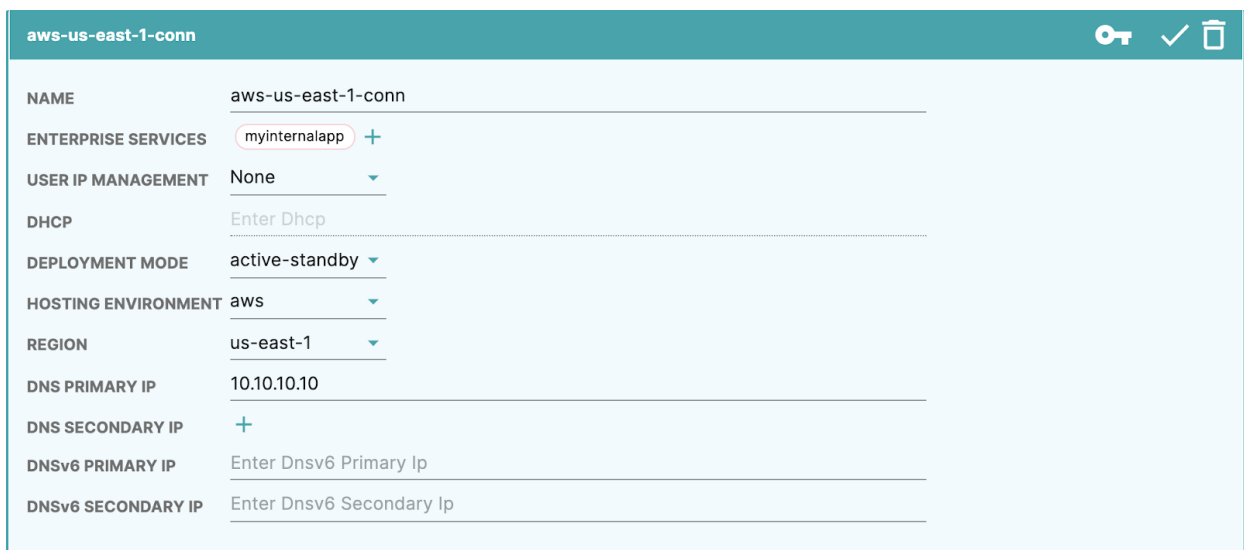


Figure 6: Resources: Connectors

- 3.3. In the configuration pane that appears, fill in the following information and then click the **✓ icon**:

- 3.3.1. **Name:** a friendly name for this connector, data center, or cloud environment
- 3.3.2. **Enterprise Services:** select one (or more) enterprise services that this connector provides access to (see **Create an Enterprise Service** section of the **Publish an Application** guide if you have not created an enterprise service)
- 3.3.3. **User IP Management:** whether to use a **DHCP** server (either v4 or v4v6 dual stack) for internal IP address assignment, or **None** for source NAT
- 3.3.4. **DHCP server IP:** the internal DHCP server which assigns private IP addresses to end user devices (only present if DHCP was selected in the previous step)
- 3.3.5. **Deployment Mode:** whether to deploy a single Connector VM (non-ha) or two Connector VMs (active-standby)
- 3.3.6. **Hosting Environment:** the cloud or data center where the Connector VM will run
- 3.3.7. **Region:** the physical region where the Connector VM will run
- 3.3.8. **DNS Primary IP:** the internal IP of the domain name server for internal name resolution
- 3.3.9. **DNS Secondary IP:** if needed, a secondary internal domain name server (click the + icon to add additional)
- 3.3.10. **DNSv6 Primary IP:** if running dual stack IPv4 and IPv6, the IPv6 domain name server IP
- 3.3.11. **DNSv6 Secondary IP:** if needed when running dual stack IPv4 and IPv6, a secondary IPv6 domain name server IP



The screenshot shows a configuration form titled 'aws-us-east-1-conn'. The form contains the following fields and values:

Field	Value
NAME	aws-us-east-1-conn
ENTERPRISE SERVICES	myinternalapp +
USER IP MANAGEMENT	None
DHCP	Enter Dhcp
DEPLOYMENT MODE	active-standby
HOSTING ENVIRONMENT	aws
REGION	us-east-1
DNS PRIMARY IP	10.10.10.10
DNS SECONDARY IP	+
DNSv6 PRIMARY IP	Enter Dnsv6 Primary Ip
DNSv6 SECONDARY IP	Enter Dnsv6 Secondary Ip

Figure 7: Connector Configuration

Generate Connector Key

Cloudbrink Connectors are hardened Ubuntu 20.04 instances, running with several Cloudbrink software packages. Since these Connector instances are all essentially identical, it's required to have a way to associate the Connector that was just created in the Cloudbrink Portal with the Connector instance that will be created momentarily.

- 4.1. If you're not already in the **Configure: Resources** section, click the **Gear Icon** in the upper left corner of the portal, and in the page that appears click the **Resources** tab.

- 4.2. Expand the **Connectors** section, and click the **teal** ▼ to the left of the Connector that was previously created to expand the Connector.

Connectors 5

NAME	APPLICATION SERVICES	USER IP MANAGEMENT	DHCP	DEPLOYMENT MODE	HOSTING ENVIRONMENT	REGION	MGMT IP	STATUS
 aws-us-east-1-conn	myinternalapp	none		active-standby	aws	us-east-1		Configured

Figure 8: Connector Selection

- 4.3. In the upper right of the teal configuration box, click the **Key** icon.



Figure 9: Connector - Generate Key

- 4.4. In the pop-up that appears, copy the key for use in the next section.

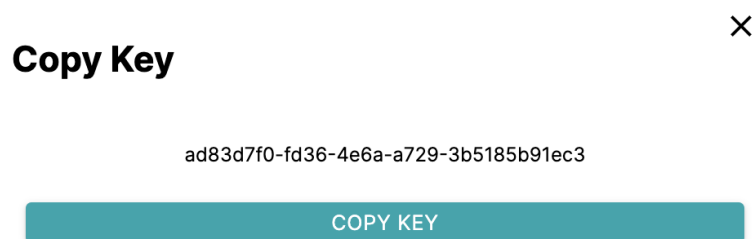


Figure 10: Connector - Copy Key

Cloud Init Customization Script

In order to apply this Connector Key to your Connector instance, a customization script must be executed. While the exact method of running this script varies depending on the cloud or hypervisor, it is typically performed in an automated process with Cloud Init. Specific cloud or hypervisor Connector instantiation documentation is available separately, however on all platforms the Connector Key generated in the previous step is added with the “-o” flag:

```
brink_connector_deploy_cloud.sh -o "<CONN_KEY_VALUE>" ...
```

For example utilizing the Connector Key generated above:

```
brink_connector_deploy_cloud.sh -o
"ad83d7f0-fd36-4e6a-a729-3b5185b91ec3" ...
```

Depending on the underlying platform, additional flags may be required. Utilize the separate Connector deployment documentation provided to deploy the Connector instance, and then return to this document to validate the configuration.

Connector Validation

Once your Connector instance is up and running, it's good practice to return to the Cloudbrink Portal and validate that the Connector was configured successfully.

- 7.1. Back in the [Cloudbrink Portal](#), click the **Gear Icon** in the upper left corner, and in the page that appears click the **Resources** tab, and then expand the **Connectors** section.
- 7.2. Ensure the **Status** value is shown as **Active**. If it is still in a Configured state, the Connector has not been configured correctly, and please contact support@cloudbrink.io.

Connectors 5


NAME	APPLICATION SERVICES	USER IP MANAGEMENT	DHCP	DEPLOYMENT MODE	HOSTING ENVIRONMENT	REGION	MGMT IP	STATUS
 aws-us-east-1-conn	myinternalapp	none		active-standby	aws	us-east-1	10.10.0.220	Active

Figure 12: Connector Operational