Cloudbrink Administrator Guide 14.2

Table of Contents

1. Cloudbrink Overview

Cloudbrink offers enterprises a cloud-delivered software-only solution that combines quality of experience (QOE) with zero-trust access controls (ZTNA). Users can work from anywhere using any device of their choice and connect securely to their enterprise private applications that are hosted on a hybrid-cloud environment as well as SaaS apps. Cloudbrink's innovative, unique platform is purpose-built to provide the highest quality of experience for applications in the most secure manner possible.

What are the major challenges that users face when working remotely?

- Collaboration applications such as Teams, Zoom, and Webex do not provide a perfect audio and video quality experience
- Productivity applications such as SharePoint, JIRA, and Workday are very slow, take longer times to load or navigate, and are slow to input or upload data
- Virtual desktops lag in mouse and keyboard movements, sometimes becoming completely unusable
- Email takes a long time to send or receive an attachment

All the Zero-Trust Access (ZTA/ZTNA) and Remote Access (VPN) solutions in the market today concentrate on providing secure connectivity for the users to their enterprise applications. But these solutions don't add any value after providing connectivity. They only maintain the session and track the session status.

End user challenges start immediately as they connect to their enterprise applications. Since the application experience is very slow, user productivity decreases which leads to employee frustration. In extreme cases, this causes users to entirely stop using these applications.

In case of Cloudbrink, the main value-addition is at two levels

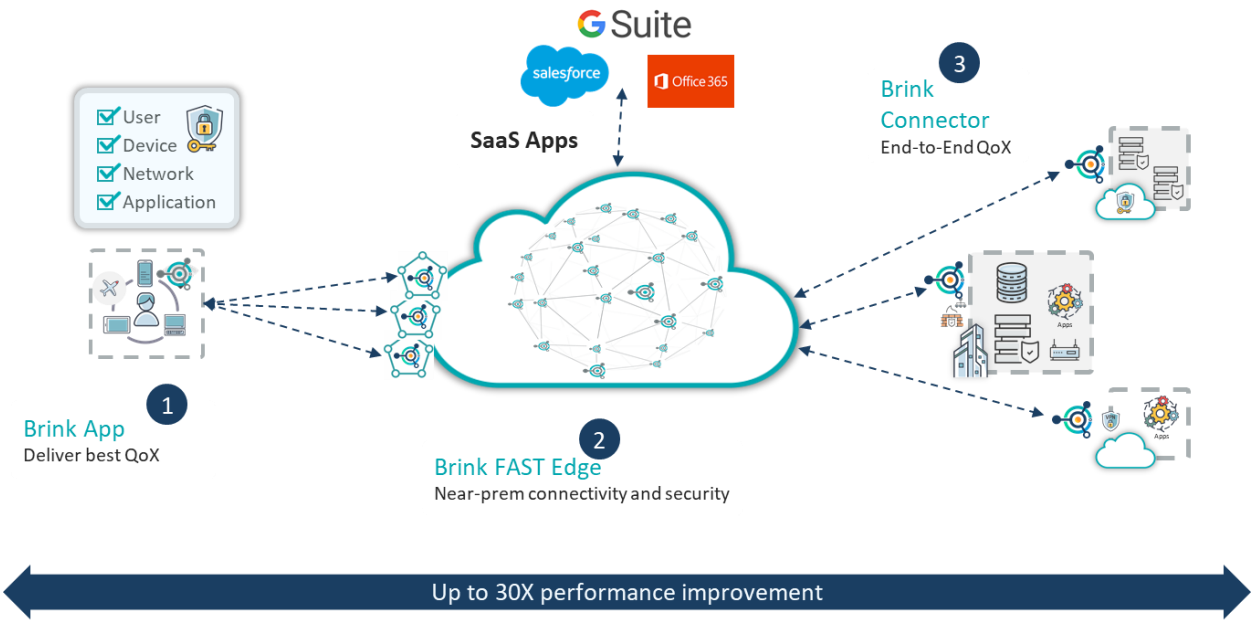
- **Zero-Trust Access to enterprise applications**. Cloudbrink validates user identity, assesses the device posture, and based on the user's security group and roles, provides access to an allow-list of applications (principle of least privilege) that IT administrators have approved.
- **Quality of Experience on the applications**. Cloudbrink tracks the user's experience on applications based on network, location and other parameters and implements several remediation measures to increase the performance of the application, thereby significantly improving the application quality.

1.1. Architecture

Cloudbrink leverages new-age edge networking and distributed control-plane/data-plane architecture to provide a highly elastic and scalable cloud-native software-only solution. Cloudbrink's architecture enables enterprises to provide virtual enterprise access points closest to their users, regardless of their location to provide the fastest connectivity. Cloudbrink accelerates application traffic in the last-mile connection as well as in the middle-mile.

With a highly distributed "follow-the-user" access model coupled with network remediation measures that Cloudbrink provides, end-users experience the highest quality application performance wherever they are, even under suboptimal network conditions.

Picture-1: Cloudbrink Architecture



1.2. Components

Cloudbrink solution consists of below key components

a) Cloudbrink SaaS

Cloudbrink SaaS is the centralized cloud-based management and visibility component of the overall solution. Customers can manage the complete end-to-end solution from the SaaS portal interface. Also, Cloudbrink administrators gain 360-degree visibility into all their users, applications, and networks from the SaaS. This significantly reduces management overhead for IT teams by consolidating visibility into a single platform and eliminates security risks due to blind spots from attempting to consolidate disparate visibility tools.

b) Cloudbrink Agent

Cloudbrink Agent is a client-side component that is installed on the end user devices. Cloudbrink Agent is required for managing the zero-trust access steps on the user side and after successful validation, steering the traffic to the Cloudbrink Edge infrastructure for application optimization and faster delivery. Cloudbrink Agent provides a very simple and intuitive user interface that enables users to quickly start with Cloudbrink and immediately gain quality of experience benefits.

c) Cloudbrink FAST Edge

Cloudbrink FAST (Flexible, Autonomous, Smart, Transient) Edge is the Cloudbrink-managed edge-computing infrastructure service that provides an access point into the solution for end users. Cloudbrink FAST Edge infra is a highly distributed and resilient edge network enabling every single user to have the closest access point regardless of their location or mobility. Edge proximity is a key factor in delivering the best quality of service for end users and Cloudbrink ensures the best proximity for all users.

d) Cloudbrink Connector

Cloudbrink Connector is a lightweight virtual machine that is easily deployed in the customer's on-premises data center, or in their public cloud VPC/VNETs. Customers can have any number of Connectors for resiliency and multiple datacenter support scenarios. The Connectors are required for enforcing the role-based access control for services hosted in the datacenters, along with providing network connectivity and optimal routing and resiliency.

e) Cloudbrink Portal

Cloudbrink Portal is the web-console where IT administrators can manage their Cloudbrink configuration as well as gain insights into end users, applications, and network activity. Portal is a completely cloud-based service with zero administrator maintenance. Cloudbrink Portal can be accessed just like any other

SaaS service, and after secure multi-factor authentication, administrators can access details based on role-based access control definitions.

1.3. Cloudbrink connection flow

The below given flow provides a high-level overview of how a user can access their enterprise applications - SaaS, cloud-hosted, and on-prem - with Cloudbrink.

Flow

1) User installs the Cloudbrink Agent on the endpoint device
2) Cloudbrink Agent will start immediately after installation and prompts user for their enterprise email address
3) The Cloudbrink Agent sends the user's email to the Cloudbrink SaaS
4) Based on domain info from the email, Cloudbrink SaaS will determine the MFA scheme that the administrator has configured and redirects the end user to the appropriate cloud IDP or to the one-time password (OTP) based authentication that Cloudbrink provides natively on the product itself
5) The user performs MFA through the cloud IDP within the Cloudbrink Agent
6) After successful user authentication, Cloudbrink Agent performs the device posture checks configured by the administrator to determine if the endpoint device meets the security policies of the enterprise
    a) Note: The device posture assessment checks are run periodically even after successful login so that any time the device goes out of compliance, Cloudbrink can take remediation action immediately
7) After successful device posture assessment, the Cloudbrink SaaS receives authorization token from the IDP
8) Based on the authorization token and the user's group information, the Cloudbrink SaaS will determine the resource-template (set of applications) that are allowed for the user
9) The resource-template and application-profiles information are sent to the Cloudbrink Agent by the Cloudbrink SaaS
10) Cloudbrink Agent establishes secure connections with the Cloudbrink Edge infrastructure based on Edge proximity
11) The user can access allowed enterprise applications in the same manner as if they were in their office
12) Based on the split tunnel configurations set by administrators, the Cloudbrink Agent steers traffic to its destination
13) Users have complete transparency over how the traffic flows to their applications, without any changes in access methods.

14) Users can access applications hosted on multiple clouds or datacenters without switching between Gateways as it is done with VPN. This eliminates significant overhead for end users as well.

1.4. Secure communication among components

All components in the Cloudbrink solution always communicate over secure channels. Cloudbrink uses Mutual TLS (mTLS) based secure connections to ensure that both ends of the communication are always authenticated and authorized.

Cloudbrink uses TLS 1.3 protocol only at all network segments which provides best available secure communication.

Below are the communication channels that use mTLS 1.3.

1) Cloudbrink Agent to the Cloudbrink SaaS
2) Cloudbrink Agent to the Edge infrastructure
3) Cloudbrink Edge infrastructure to the Cloudbrink SaaS
4) Cloudbrink Connector to the Edge infrastructure
5) Cloudbrink Connector to the Cloudbrink SaaS

2. Configuration

Configuration section below provides details about the features that are supported by Cloudbrink and the corresponding feature configuration entities.

2.1. Cloudbrink Management Portal

Cloudbrink provides customers with a simple and easily accessible web console for managing their account. Customers can define the policies and also get visibility & troubleshooting information from the same management portal.

Cloudbrink management portal is available at https://admin.cloudbrink.com/. Customers can login to their account using the credentials shared by the Cloudbrink Sales/Support team.

The management portal login is protected using a 2-factor authentication (2FA) method. There are two options in the 2FA.

1) **SAML Auth** → If customer is using SAML based authentication by integrating with any standard IDP (Azure AD, Okta, PingID, OneLogin, etc.), then the IDP takes care of 2FA as per customer's security policies.
2) **Local Admin Users** → Customers can add some admin user accounts locally on the Cloudbrink management portal. In this case, the admin user account will need a username, password and email ID. The admin user can login using username + password + the OTP sent to the email ID as part of login process.
    (a) Note: It is important to give a valid email ID for local admin user accounts because OTP will be sent to this email ID for second factor auth.

2.2. First-time Onboarding

When a customer successfully registers with Cloudbrink, a new tenant instance is created which provides a completely isolated environment for the customer. Before a customer can start using the Cloudbrink service for their users, certain prerequisites must be configured on the Cloudbrink SaaS. To ensure that customers don't miss on these prerequisites, the Portal page takes the admin through the prerequisite steps during the first-time login. This is referred to as a First-time Onboarding Wizard.

As part of the First-time Onboarding process, customers are expected to configure below configurations.

1. **Device-user-groups**:- All configuration entities such as Resource-Templates, Policies, etc. are assigned to a Device-user-group entity. A Device-user-group entity is the anchor point that determines access levels for the user based on corresponding role. Therefore, Cloudbrink needs at least one Device-user-group to be configured before any user starts using the service.
2. **Authentication Policy**:- Users are allowed to connect to Cloudbrink service only after successful authentication. Customers can bring in their preferred choice of Identity Provider (eg: Okta, OneLogin) for authentication. Without authentication, users are not able to connect to the Cloudbrink service.
    2.1. Cloudbrink provides built-in One-Time Password (OTP) based authentication support as well. Customer can specify the list of users (email IDs belonging to their organization domain) who can authenticate to Cloudbrink using OTP. OTP will be sent to user's email ID at the login step.
3. **Resource-Template**:- Resource-template the set or group of applications that are allowed for a particular device-user-group. Only those applications that are explicitly added to a resource-template that is assigned to the device-user-group will be intercepted by the BrinkAgent.

After completing the onboarding process, customers can try Cloudbrink by logging into the Cloudbrink service using the Cloudbrink Agent and going through the authentication process.

2.3. Admin Users/Groups

Cloudbrink provides role-based access controls for the administrators managing their Cloudbrink environment, with built-in administrator roles. Customers can assign administrator users to these roles so that there is a granular level of access to the configurations within the administration team. Here are the built-in admin roles on Cloudbrink:

a. **Super-admin**:- Admin user having permissions to do everything on the tenant
b. **Delegated-admin**:- Admin user having permissions to make configuration changes (CRUD operations) as well as Visibility. Delegated admins do **not** have permissions to change subscription status or add more user licenses.
c. **Read-only**:- Read-only users can only view the configuration and other traffic data. No CRUD operations are allowed for the read-only users.

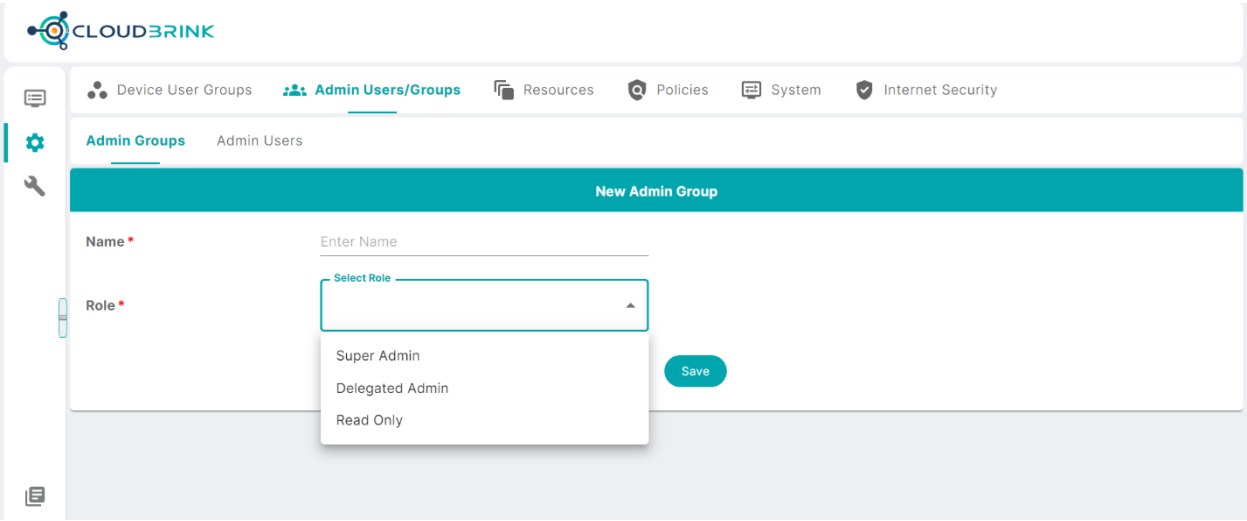
When the customer registers for Cloudbrink service, the primary point of contact (user and email-ID) is given the super-admin role by default. It is expected that this super-admin user logs into the Cloudbrink tenant portal for the first-time and adds other delegated-admins as required. The super-admin is expected to complete the first-time onboarding process as well.

Delegated-admin users are mainly responsible for configuration and monitoring of Cloudbrink as part of their regular IT operations/systems. Delegated-admins have permissions for performing CRUD (create, read, update, delete) operations on the configuration entities. Delegated-admin users can create other delegated-admins as well but not Super-Admins. Delegated-admin users do not have permissions to change the subscription (eg: adding more named-user licenses).

Admin Groups

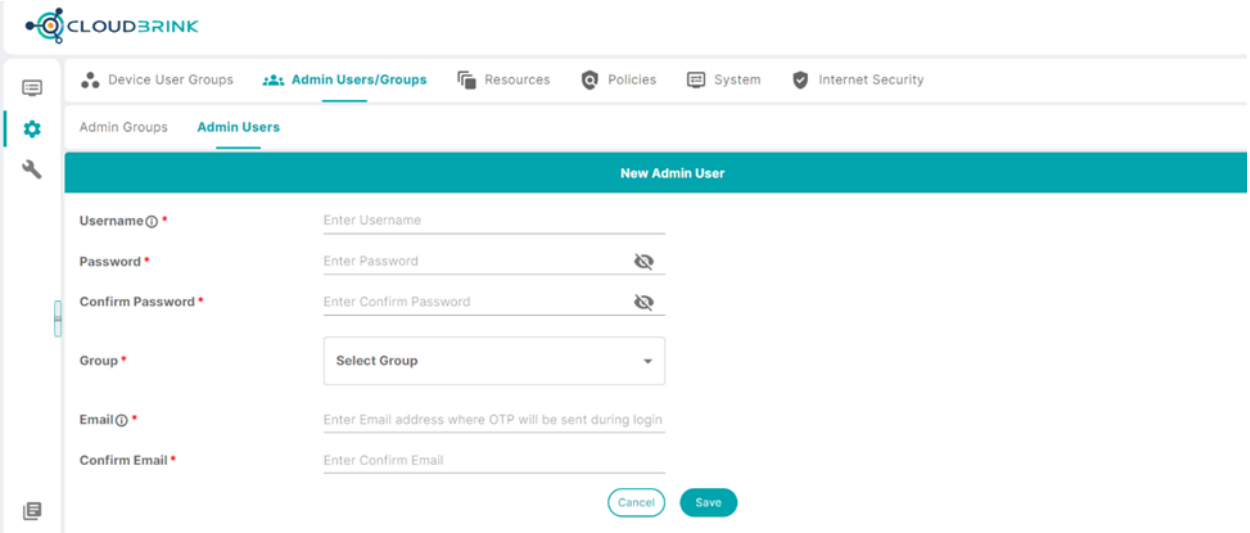
Cloudbrink provides a built-in admin-group by name SuperAdmins, with the role as super-admin. Customer can configure a security group on their IDP with same name (SuperAdmins) and add IT admins who will manage Cloudbrink service to this security group. When Admins attempt to login to Cloudbrink management portal, they would be authenticated by the IDP and based on their group membership info, Cloudbrink will decide if the admin has access to the Cloudbrink portal or not.

Customer can create more admin groups and assign the groups with either SuperAdmin or DelegatedAdmin roles. Same admin groups can be configured on IDP and add admin users to those groups based on the role that must be assigned for each user. Cloudbrink can extract the group info and provide correct level of access to the admins.



Admin Users

If customers don't want to change their IDP due to security team dependencies, local admin users can be created and assigned to the admin groups. In this case, admin users will not be redirected to IDP (because there is no IDP here). Admin users can login to portal by just providing username and password created locally.

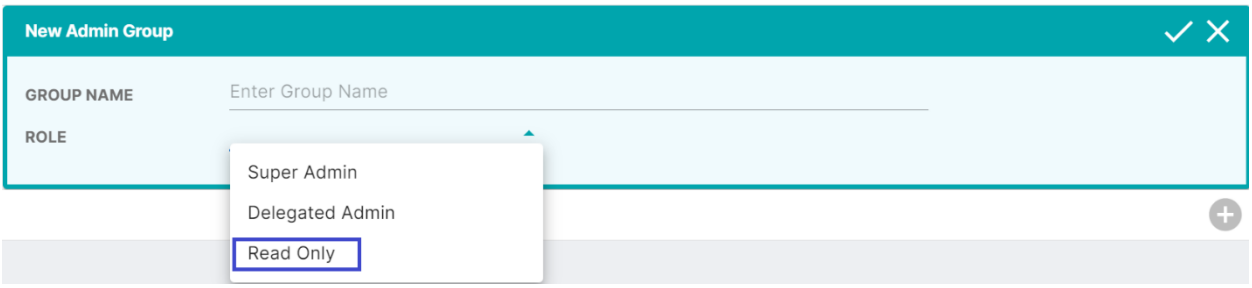


Read-only Admin Role

Cloudbrink now supports “read-only” admin role. The admin users in this role will not be able to “add” or “update” or “delete” any configuration from the Cloudbrink management portal. The read-only admin users can only “view” all the information on the management portal.

a) Customers can use this capability for providing access to admins who are responsible only “monitor” the service and review the service usage.
b) It also helps in cases where customers have admins from several business units but the maintenance of Cloudbrink service is done by one central admin team. All the business unit admins can be provided read-only access so that they can monitor the service usage.

Configure → Admin Groups/Users → Admin Groups → New



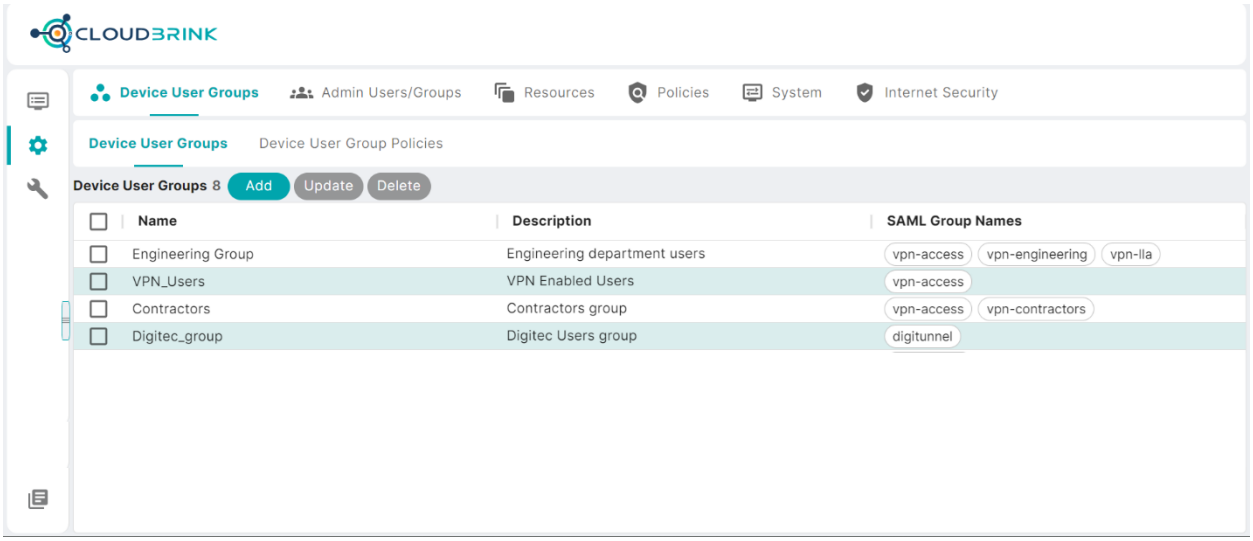
2.4. Device-user-groups

Cloudbrink provides Role-Based Access Control (RBAC) capabilities for end-user access as well as administrator access. When the end-user attempts to connect to the Cloudbrink service to access their enterprise applications, Cloudbrink provides access to only those applications that are explicitly allowed by the administrator for this user role. The user role is determined at the time of login based on the security groups that the user belongs to. Enterprises typically maintain the user-to-security-group mapping in their Active Directory (IDP) or any other Identity Management solution.

Cloudbrink requires administrators to configure Device-user-groups which match exactly to the name of the security-group name that is defined in their Active Directory (IDP) or Identity Management solution. Once the Device-user-groups are configured on the Cloudbrink, administrators can assign other policies (Authentication, Application allow list, etc.) to this Device-user-group config entity. Device-user-group is the role to which a user's session will be assigned to determine what level of access this user has.

At the time of login, Cloudbrink reads the group information from the Active Directory (IDP) or Identity Management solution as part of the Authentication process. Once Cloudbrink reads the group information of the user, based on the Device-user-groups configured on the Cloudbrink, the exact role (user's session) will be determined and provide access to the applications.

Adding user groups that must be part of IDP



2.5. Role-Based Access

As described in the previous section, Cloudbrink provides a highly granular policy infrastructure for customers to ensure users can access only those applications that are explicitly permitted by administrators. Here are the steps to allow a Device-user-group to access an application:

1) Define the Device-user-groups which determine the role of the user when they connect to the Cloudbrink service
2) Define the application sets - referred to as Resource-Templates (see below) - that should be provided to users
3) Assign the Resource-Templates to the Device-user-groups.
4) Ensure that Device-user-groups configured on Cloudbrink are *exactly same* as that of the secure groups configured on Active Directory (IDP) or Identity Management solution
5) Configure "Group Extraction" in the Authentication policy so that Cloudbrink can extract security group information about the user during Authentication step, and assign the correct Application-Templates to the users

Assign resource-template (app set) to the user-groups

2.6. Authentication

Authentication is a critical feature for Cloudbrink. Without secure multi-factor authentication, end-users or administrators can't access anything on the Cloudbrink service.

When an end-user or administrator attempts to connect to the Cloudbrink Agent or portal, Cloudbrink prompts for the corporate email-ID. Once the user provides the corporate email-ID, based on the domain information in the email, the corresponding Authentication policy will be applied. Based on the Identity Provider (IDP) configured in the Authentication policy, the user is redirected to the IDP to perform multi-factor authentication. Only after successful authentication and validation of the token, the user is granted access to applications or portals.

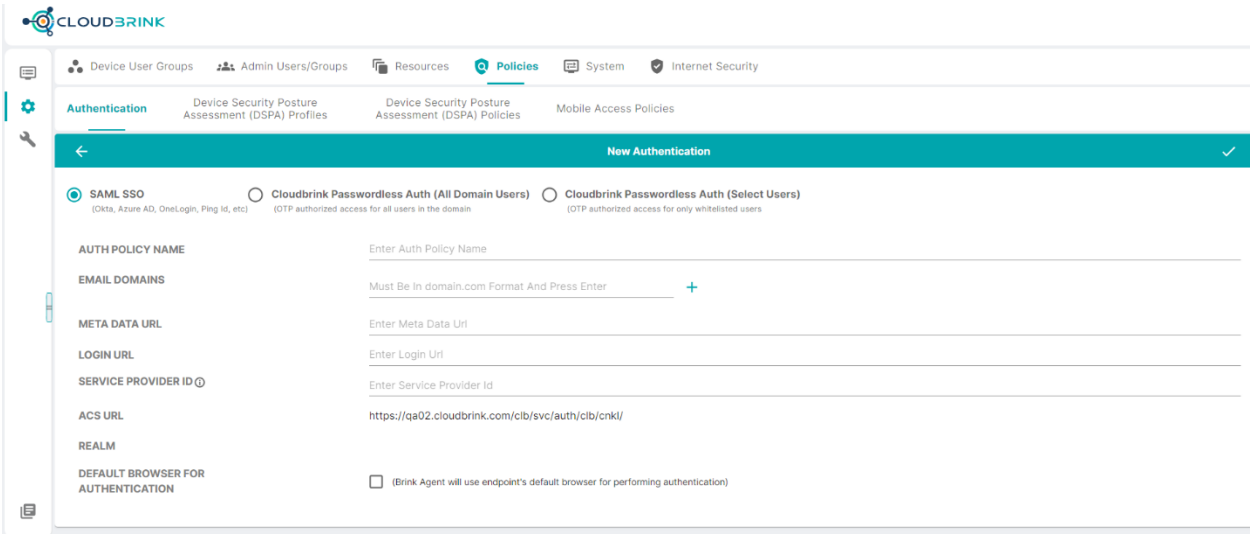
Customers have two options to authenticate users.

i. SAML-based cloud IDP MFA
ii. Cloudbrink native OTP

A) SAML-based cloud IDP MFA

Cloudbrink supports SAML-based Cloud Identity Providers integration. Globally, enterprises are moving towards cloud Identity Providers such as Okta, OneLogin, Azure Active Directory or Ping Identity. Cloudbrink can integrate with all major Identity Providers for MFA.

Below section provides exact details of the SAML configuration. IDP specific integrations are available for customers.



Cloudbrink will act as the Service Provider (SP) and connect to the cloud Identity Provider (IDP) for validating user credentials. To complete user authentication, a trust relationship must be established between the SP and IDP using certificates. Cloudbrink follows the standard process of establishing trust relationships with the IDP.

B) IDP Certificate Management

Cloudbrink offers a high-performance Zero-Trust Security solution to enterprises globally that provides very rich set of security features like multi-factor authentication, device posture assessment, role-based access controls, micro-segmentation within a single data centre and across data centres, SDP-compliant secure access to private apps, etc. IT teams can provide a high-performance remote access solution to their hybrid workforce so that users can work from anywhere without any issues and improve their productivity.

As part of multi-factor authentication, Cloudbrink can integrate with any SAML 2.0 compliant IDP. Cloudbrink supports both signing and encryption of the SAML responses from the IDP. In order to provide better security practices, it is recommended to use both signing and encryption. Enterprises

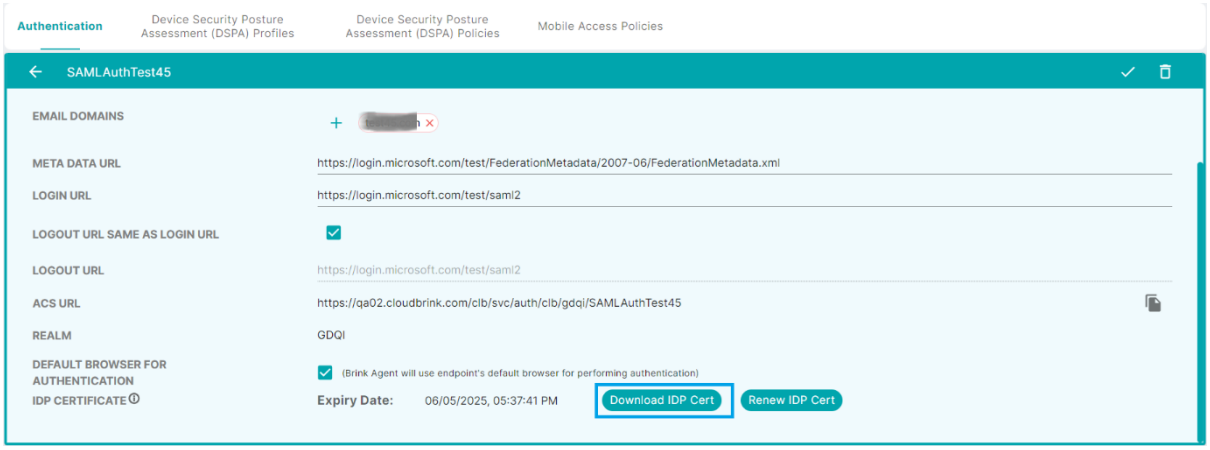
have to use Cloudbrink provided certificates and keypair on the IDPs to support encryption of the SAML response. Below feature is helpful to manage these SAML IDP certificates by the enterprises in an efficient manner.

IDP Certificates Management

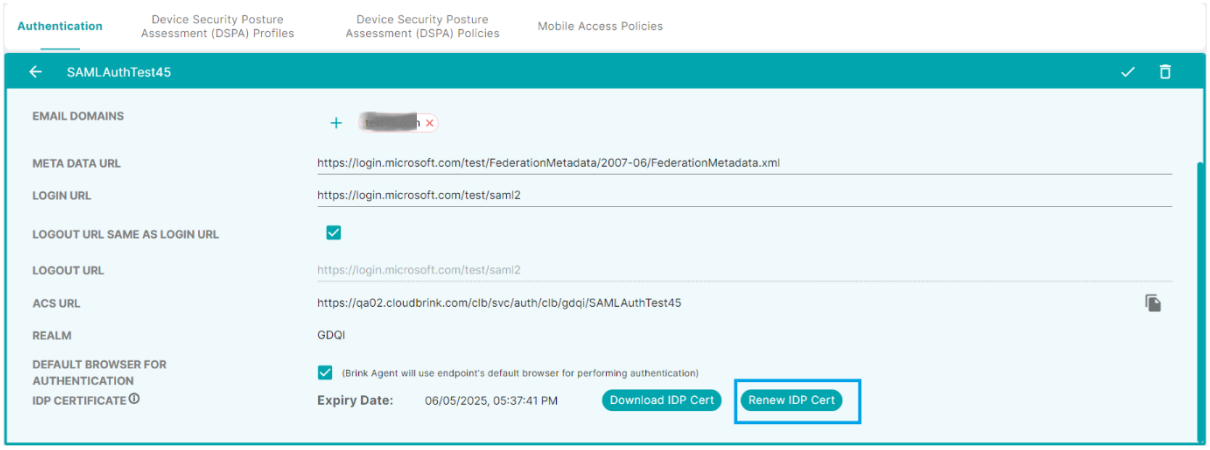
Enterprises can manage the SAML IDP certificates that are used for signing and encrypting the SAML responses from the Cloudbrink admin portal.

Steps to manage IDP Certificates

1. Admin must download the SAML IDP certificate from the Cloudbrink admin portal immediately after creating a new SAML Authentication Policy



2. This IDP certificate must be used on the IDP management console for the SAML app created for Cloudbrink login. The SAML app certificate settings for IDP will be documented in the respective vendor product information section.
3. Few weeks before the IDP certificate expiry date, admin can “Renew” the IDP certificate by clicking on the “Renew IDP Cert” button.



4. Once the certificate is renewed, download the new certificate again (by clicking “Download IDP Cert”) and update the certificate on the IDP SAML app settings.

Using above process, enterprises can always manage the SAML authentication in a highly secure manner.

Note: Some IDPs, Microsoft Entra ID as an example, require both IDP certificate (.cer) and keypair to enable encryption of SAML response. Enterprises can extract the .cer certificate and corresponding keypair from the downloaded certificate using tools like openssl.

C) External Browser for Authentication

As part of the Zero-Trust Security, users must go through the authentication step before connecting to Cloudbrink service and accessing any business application. Currently, BrinkAgent uses an embedded browser to support user authentication for any SAML IDP that customers use.
With the 14.1 release, Cloudbrink supports using the default browser on the endpoint for the authentication step. Using this external browser for authentication is helpful for below use cases.

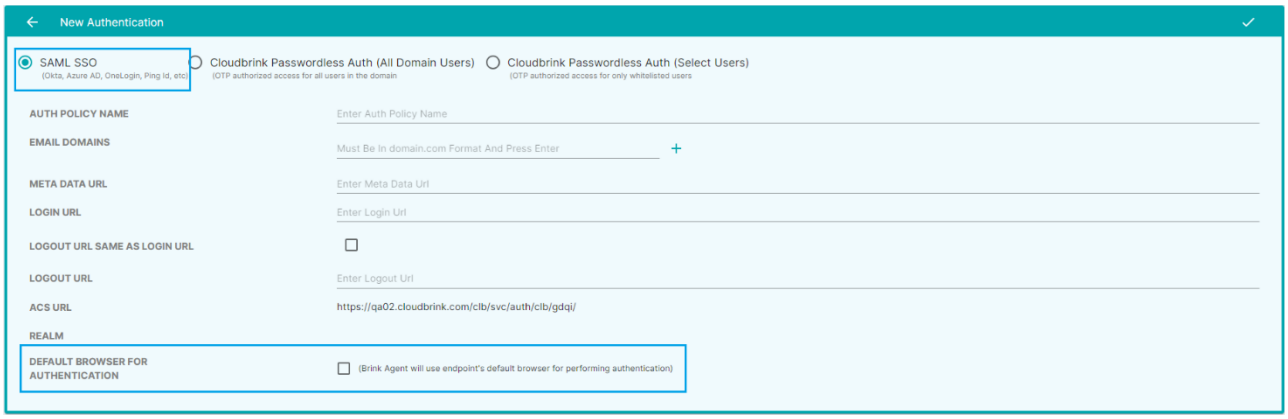
(1) **Microsoft Conditional Access**: Customers using Microsoft Conditional Access policies to control access to Microsoft services can now extend the same policy level protection for all their business apps, including private apps. Cloudbrink integrates with Conditional Access policies and sends the necessary endpoint information to the Conditional Access service. Conditional Access service applies the policies based on the information sent by BrinkAgent (using external default browser on the endpoint) and determines the access level to the user.

    Note: End users must have the Edge browser or required plugins on other browsers for Conditional Access to work successfully. This requirement is common and not specific to Cloudbrink.

(2) **Password Manager apps**: Customers using password manager products to enable their users password-less access to all their applications can use the external browser authentication on BrinkAgent. When external browser is used for authentication, BrinkAgent login also can use password manager for login to Cloudbrink service. Users need not go through the manual login method for Cloudbrink.

Enable External Browser Authentication

Admin can enable the external browser authentication using the below configuration setting available at the SAML IDP policy configuration level. When this option is enabled, BrinkAgent uses the default browser settings on the endpoint to open the IDP login page.
Configuration on Cloudbrink for external browser:



Notes:

a. Default browsers supported on Edge, Firefox, Chrome and Safari
b. After successful authentication on the external default browser, the browser/tab automatically closes after 5 seconds, and control will be taken back to the BrinkAgent
c. External browser authentication is supported only on desktop platforms

D) Cloudbrink native OTP

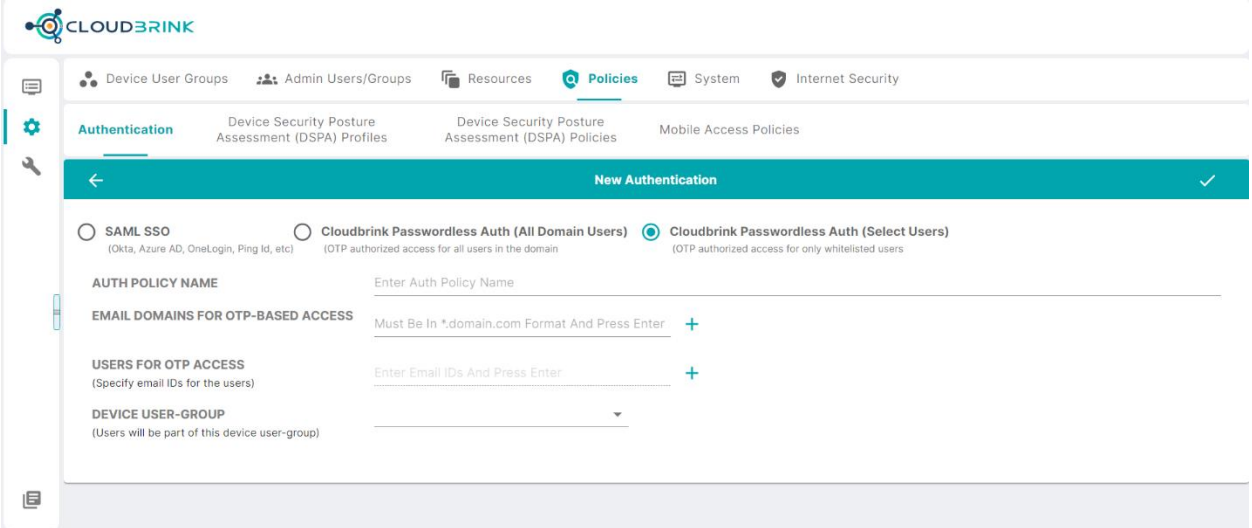
Cloudbrink provides second option for customers to authenticate users or admins. Cloudbrink native OTP method allows users to login by providing email-ID and OTP that Cloudbrink will send over email to the user.

Customers have two options on how OTP method can be used.

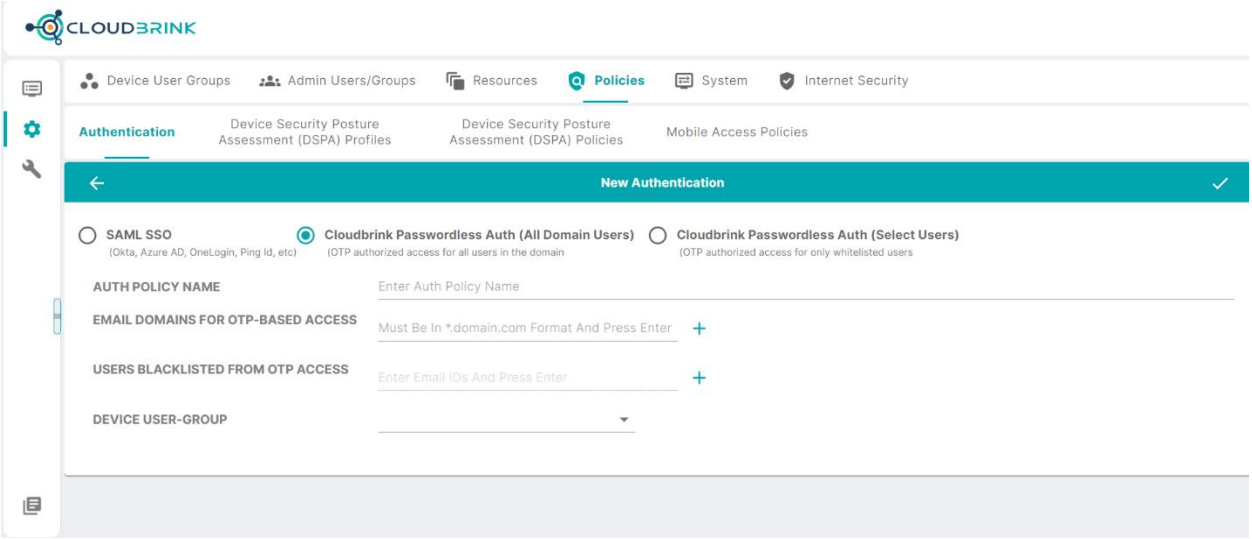
i. Whitelist of users who can use OTP method and use Cloudbrink
ii. Enable OTP for all domain users, and use blacklist option if any users must be selectively disabled

Note: All users using OTP method must be in the same domain name (eg; user1@domainABC.com, user2@domainABC.com, user2@domainABC.com, and so on).

OTP authentication mechanism for whitelisted users



OTP authentication mechanism for overall organization, with blacklisting capability



2.7. Device Posture Assessment (DPA)

Zero-Trust Access solutions are complete only when the end user device is also authenticated, in addition to the user authentication. Cloudbrink provides “continuous device posture assessment” that monitors the end-user device posture on a continuous basis. Customers can use DPA feature to check if the endpoints used by users are meeting all the corporate security policies. Any violation of the endpoint will be immediately detected, and action can be taken on the user session.

Cloudbrink provides all the below types of checks using the DPA feature.

OS Level Categories		
Windows	Mac	Linux
Anti-Virus/Spyware	Firewall	Firewall
Firewall	OS	OS
OS	Disk Encryption	Disk Encryption
Disk Encryption	File	File
Registry	Certificates	Blacklisted Processes
File	Blacklisted Processes	
Patch	Trust Domain	
Certificates		
Blacklisted Processes		

The DPA checks that are configured will be checked periodically, default being every 30min. Customer can configure the interval based on their security policies.

User will be able to access the set of resources admin has configured only when all the DPA checks are successful. Admin can check the status of every user device from the portal UI.

If the endpoint fails any one of the DPA check, admin has the option to specify any one of the three actions defined below.

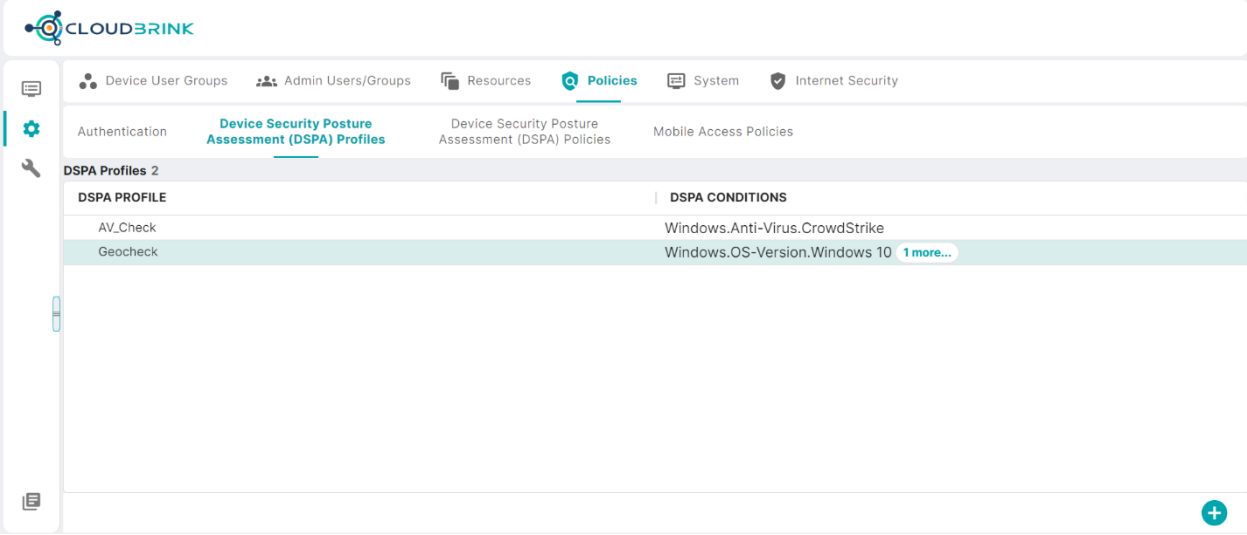
i. **Deny** → if the endpoint fails any one of the DPA check, the user will be logged out from the Cloudbrink session
ii. **Quarantine** → if the endpoint fails any one of the DPA check, the user session will be moved to a quarantine group. User will have access to limited set of resources/applications that the

admin has explicitly configured. When user takes action to fix their endpoint issues, user will get full access.

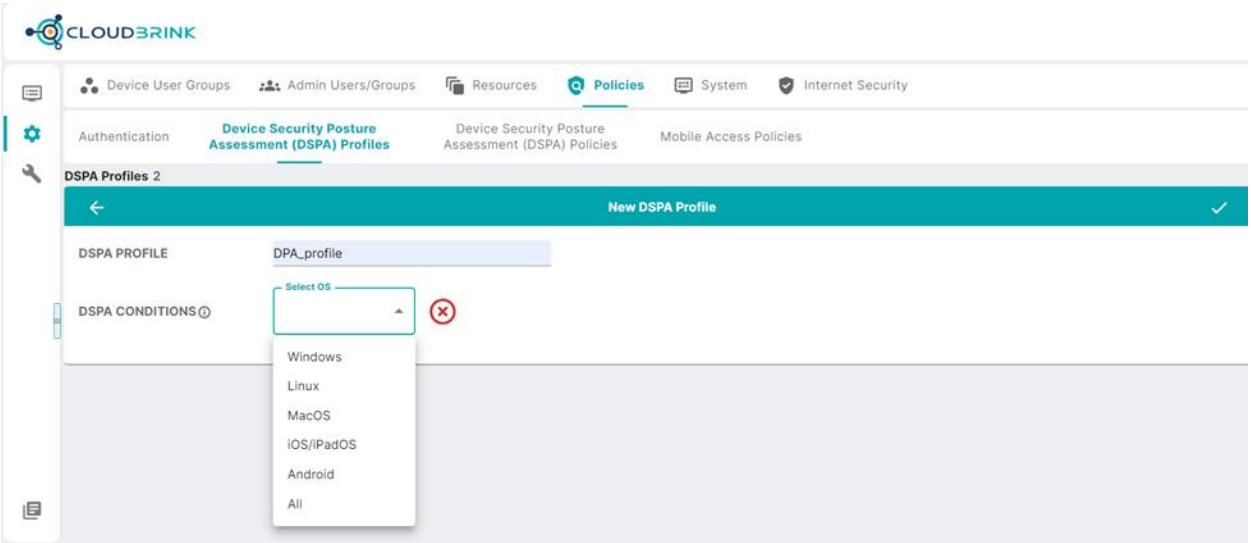
iii. **Log_and_Allow** → in this case, even if user fails the DPA checks, they get full access but a CRITICAL level log message will be generated on the management portal. This option is available so that admins have visibility into users using unsecure laptops though users are not blocked from accessing their applications.

Customers can use DPA feature on both BYOD as well as corporate-managed endpoints. This helps customers to meet their compliance requirements on all types of endpoints.

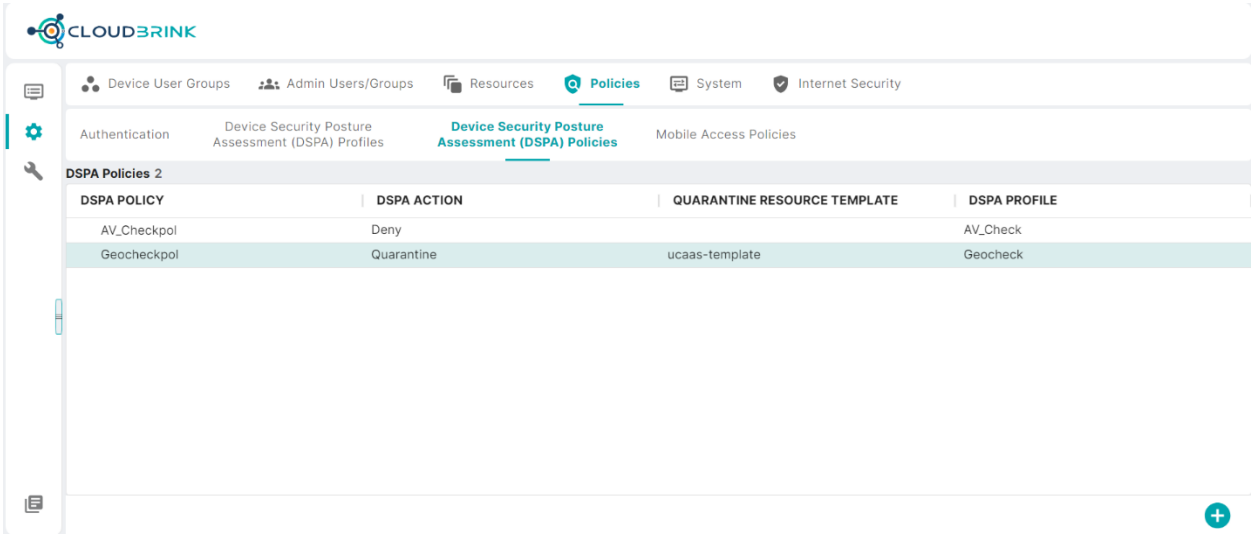
Device posture assessment profiles (checks to be performed)



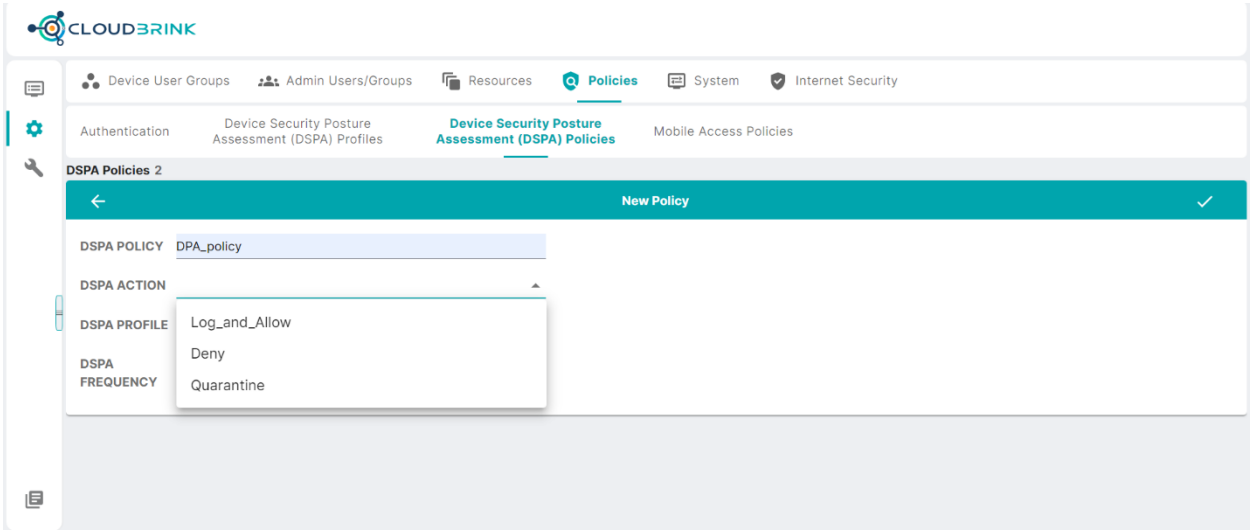
Device posture assessment profile creation



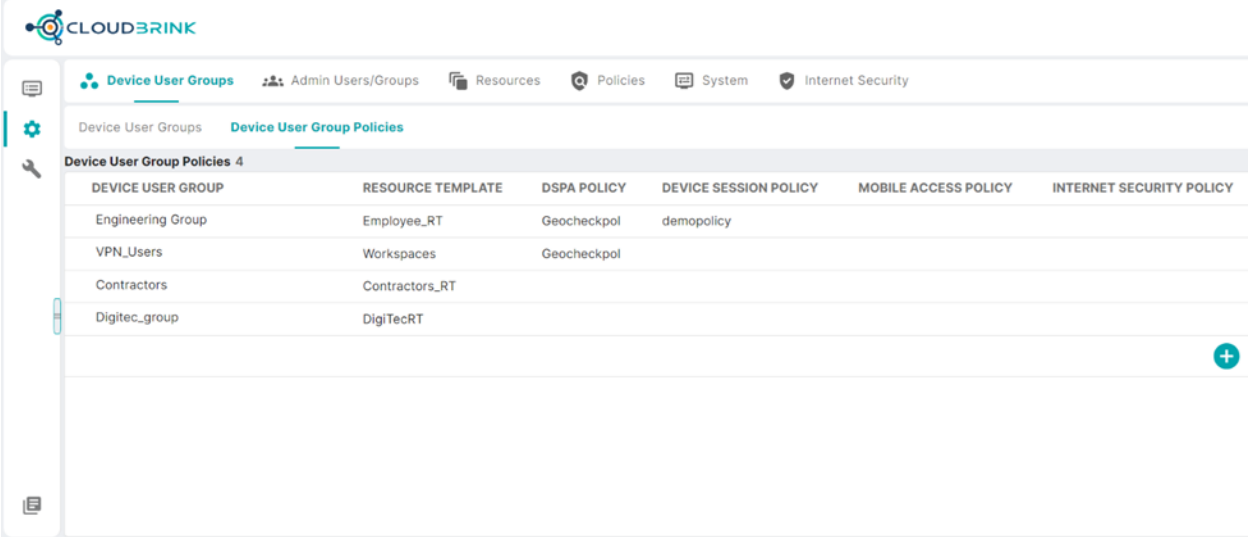
Device posture assessment policies (when to apply the checks)



Device posture assessment policy creation



Enable device posture assessment on per user-group level



Device Posture Assessment (DPA) Enhancements 13.1

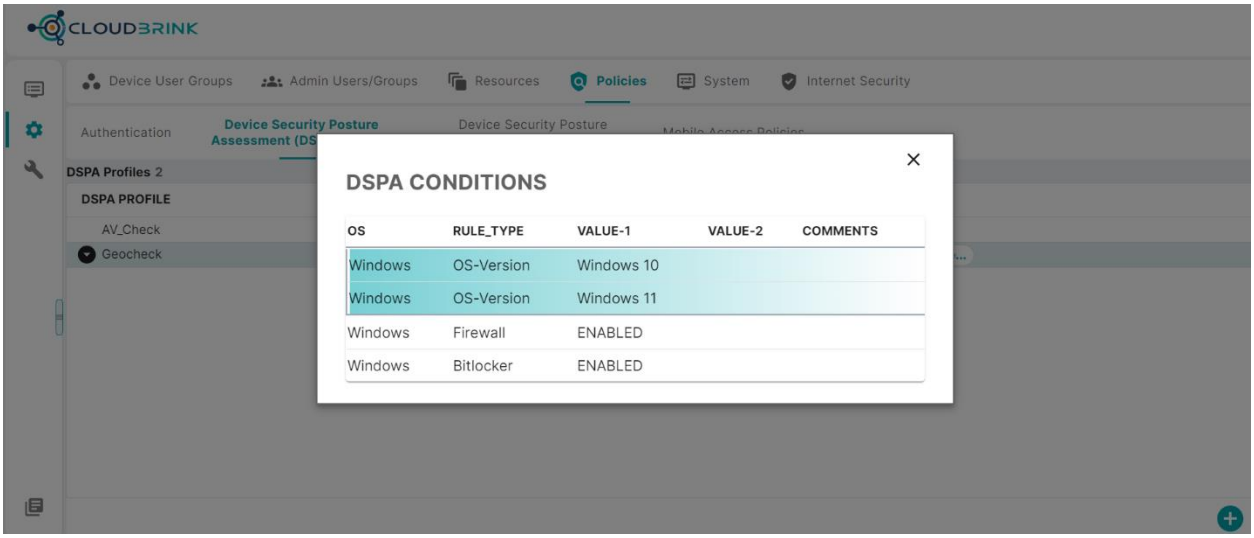
“OR” conditions

Device posture assessment checks now support ability for creating “OR” conditions. Customers can check for multiple values for the same parameter. When any one of the values is present on the endpoint, the condition is considered successful.
For example, customers want to check if user has *either* AV-1 *or* AV-2 anti-virus installed or not.
Similarly, customers want to check if user has *either* Windows-10 *or* Windows-11 OS running or not.
A set of OR conditions can be grouped along with other checks with an implicit AND operation across them.
For example, expressions such as {(A OR B) AND C} or {(A OR B) AND (C OR D) AND E} are possible.

Configuration

While creating the Device Security Posture Assessment profile, admin can create a “OR group” of checks and then, add AND conditions to this OR group.

Upon adding multiple checks with a mix of OR-groups and other checks, final profile would look like below as an example.



In the above example, the overall DPA check is successful if the endpoint has Windows OS version of *either* Windows 10 *or* Windows 11 AND disk-encryption ENABLED AND firewall is also ENABLED.

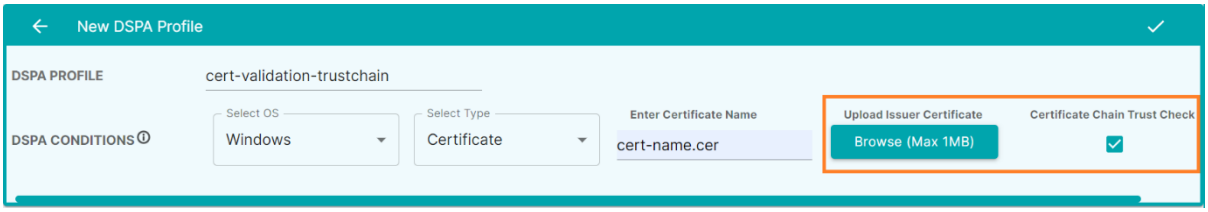
Certificate trust check validation

As part of the certificate validation posture assessment check, the capability is enhanced to validate the complete trust chain of the certificate with the issuer root certificate. As part of the validation, Cloudbrink will check if the user certificate is issued by the proper Issuer, cert expiry time period as well as trust chain.

Note: Issuer certificate must be in the .PEM format

Configuration

As part of the certificate check configuration in the device posture assessment profile, admin can now upload the Issuer Root Certificate. Once the cert is uploaded, the “Certificate Chain Trust Check” is automatically enabled.



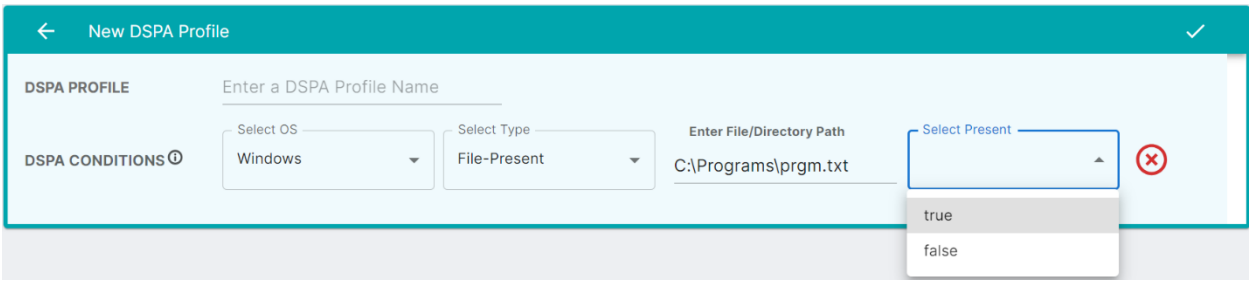
The Issuer Certificate must be a proper PFX format root certificate that has been used for issuing the user certificates (in above example, cert-name.cer).

Device Posture Assessment (DPA) Enhancements 13.4

Presence/Absence of File/Directory/Registry

Customers can now check for the presence or absence of a specific file or directory or registry-key.

Config



When “True” is selected, DPA checks for the specified file name and considers DPA as success if the file is present. If “False” is selected, DPA check is successful if the file is absent.
Note: For checking the presence/absence of directory, the path must end with a “\” (or “/” based on the OS)

Custom Scripts

To give more flexibility as part of the device posture assessment, Cloudbrink now supports custom scripts in the DPA policy. Customers can develop their own scripts to check for any specific artifact on the endpoint and use the scripts as part their DPA configuration.

Config

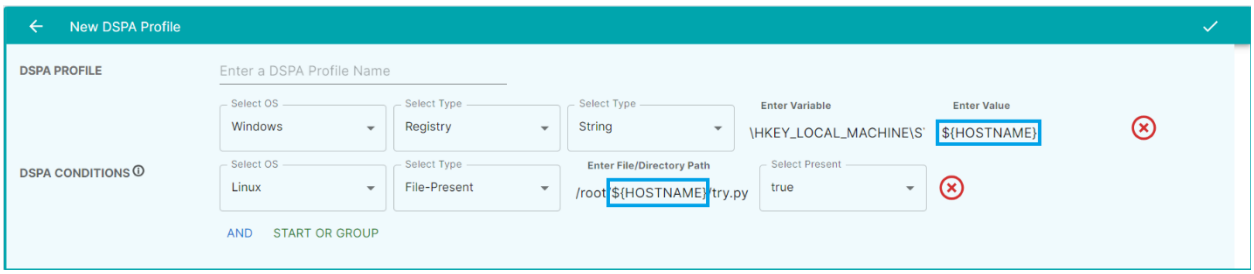
- Admin can build the script offline and upload it on the admin portal or directly type the script on the text window that pop-ups after clicking “Set” button above.
- The expected output is the result of the script that will be matched using regex method.
- The execution time limit is the time before which the script must be executed. If the script runtime is longer than the limit, the DPA check is considered as fail.

Environment Variables

Customers can use two environment variables in specifying the DPA rules. The two variables supported are ${HOSTNAME} and ${USERNAME} that return the hostname of the endpoint and current logged username of the endpoint respectively.

Customers store certificates or set registry-keys in paths that include either the username or the hostname. Since each endpoint will have different hostname and username, a common DPA rule can be configured only if the path can support environment variables.

Config



Wherever the variable is specified, Cloudbrink DPA engine will replace that variable with actual hostname or username and evaluate the checks.

2.8. Mobile Access Policy

With 13.1 release, Cloudbrink will support two new features that will augment the Brink Apps on mobile platforms iOS/iPadOS and Android.

A. Mobile Access Policy
B. Mobile Device Posture Assessment

Mobile access policy is a new configuration entity on Cloudbrink administration portal that allows customers to define separate sets of applications accessible over mobile platforms and desktop platforms. The applications that users typically access over laptops are different than applications over mobiles, though there are a subset of common applications. For example, users access datacenter servers (eg: SSH, RDP) on laptops but not mobiles whereas E-mail client is a common application on both platforms.

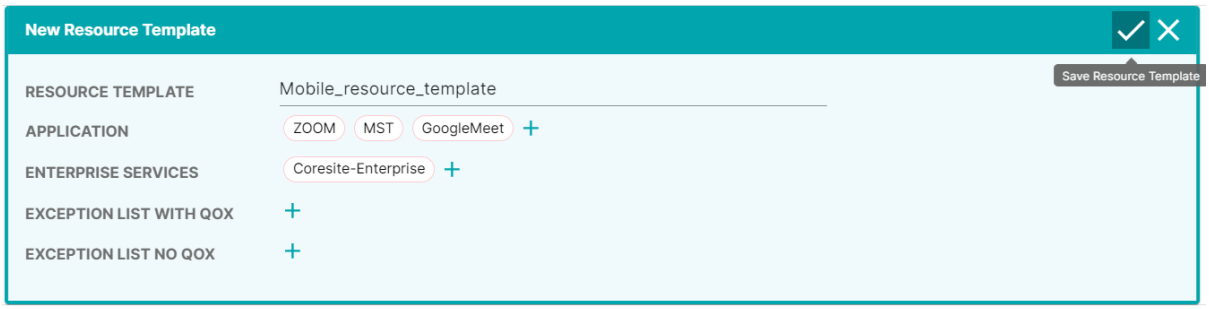
To provide the flexibility for customers to define application sets for laptops and mobiles, Cloudbrink mobile access policy configuration can be used.

NOTE: If Mobile Access Policy configuration is not used, mobile platforms also will use same application set (resource-template) as that of the laptops.

Configuration

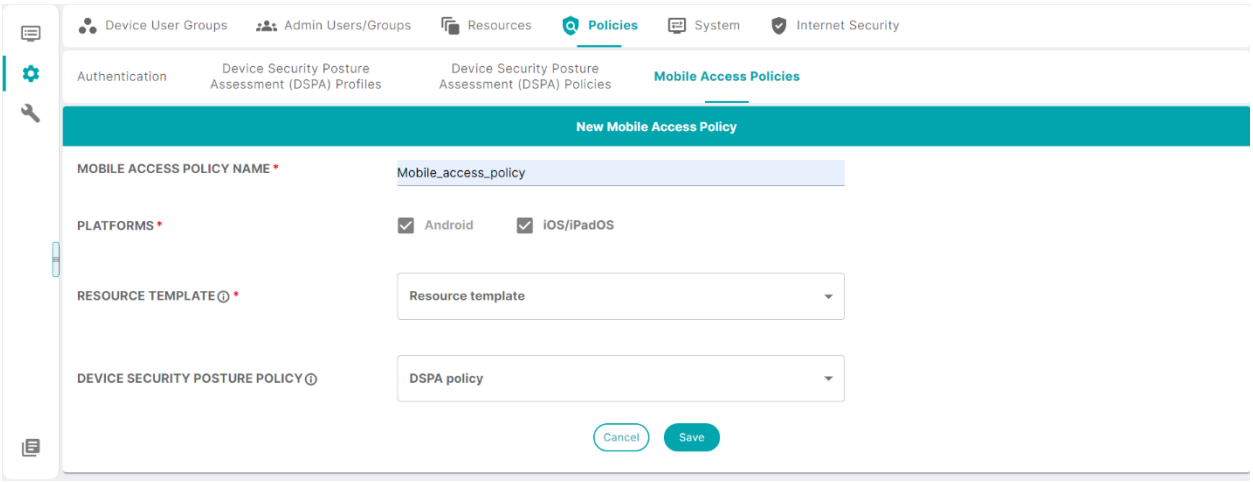
Step-1: Create a new resource-template for mobile platforms

Configure → Resources → Resource Templates



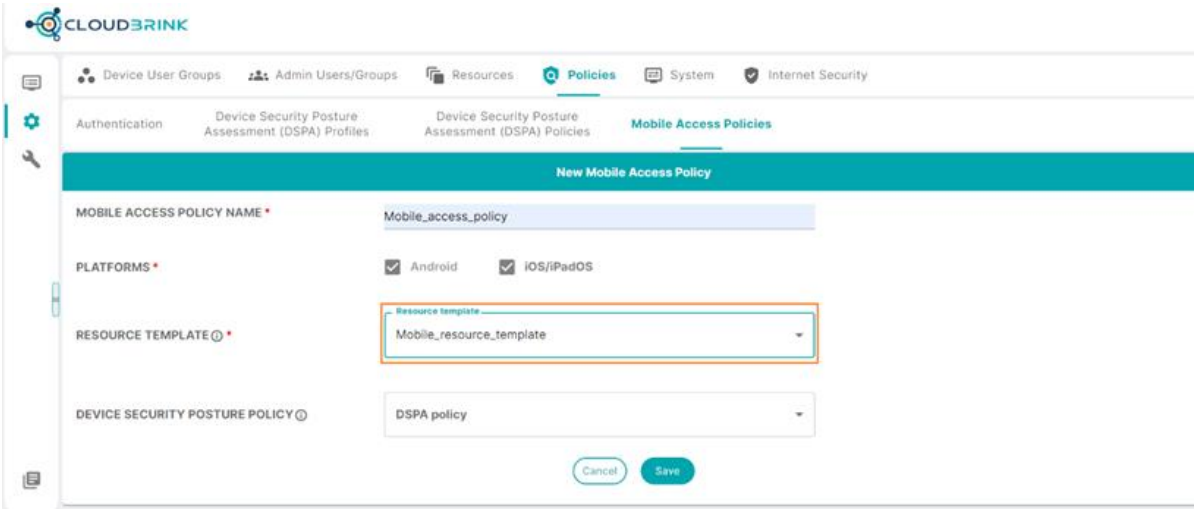
Step-2: Create a new mobile access policy

Configure → Policies → Mobile Access Policies → Add



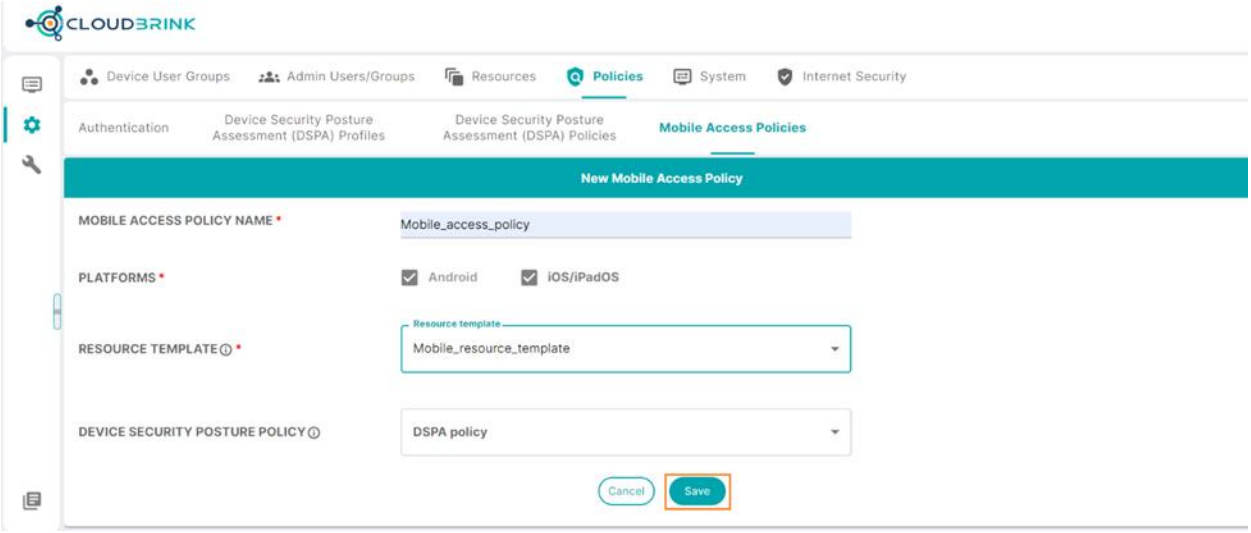
Step-3: Select the newly created resource-template for mobile platforms from the drop-down

Configure → Policies → Mobile Access Policies



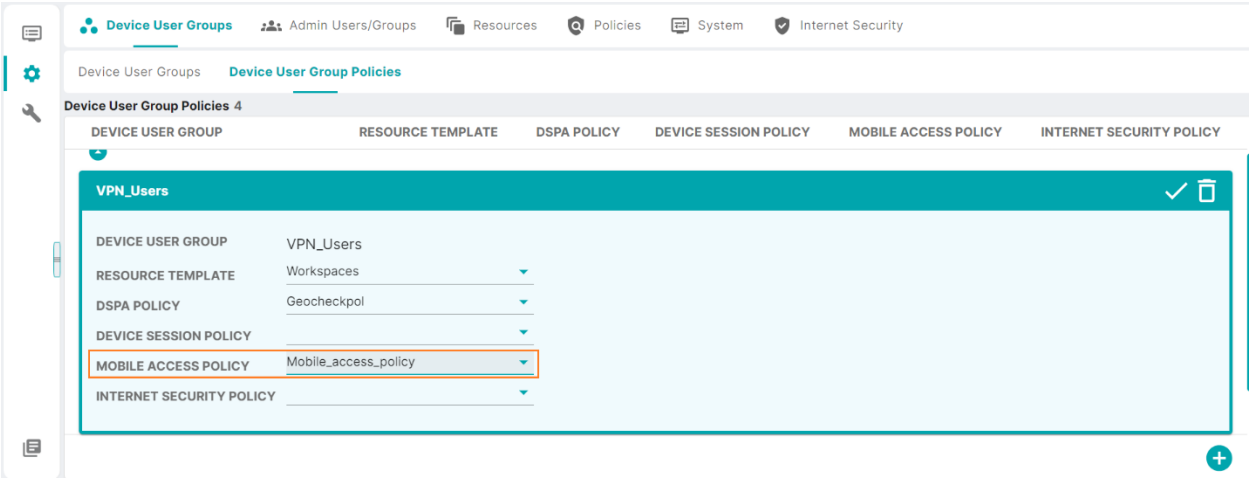
Step-4: Save the newly created mobile access policy

Configure → Policies → Mobile Access Policies



Step-5: Assign mobile access policy to a device-user-group

Configure → Device User Groups → Device User Group Policies



With the above sample configuration, users belonging to “VPN_ODBT” device-user-group will be able to access apps defined in resource-template “VPN Template” from their laptops and apps defined in resource-template “Mobile_resource_template” which is selected in the Mobile_access_policy from their mobile devices.

2.9. Mobile Device Posture Assessment

Customers can strengthen their security posture by ensuring only trusted devices are used by the users to access business applications. As part of the Cloudbrink Zero-Trust Security stack, Cloudbrink now supports device posture assessment for mobile platforms.

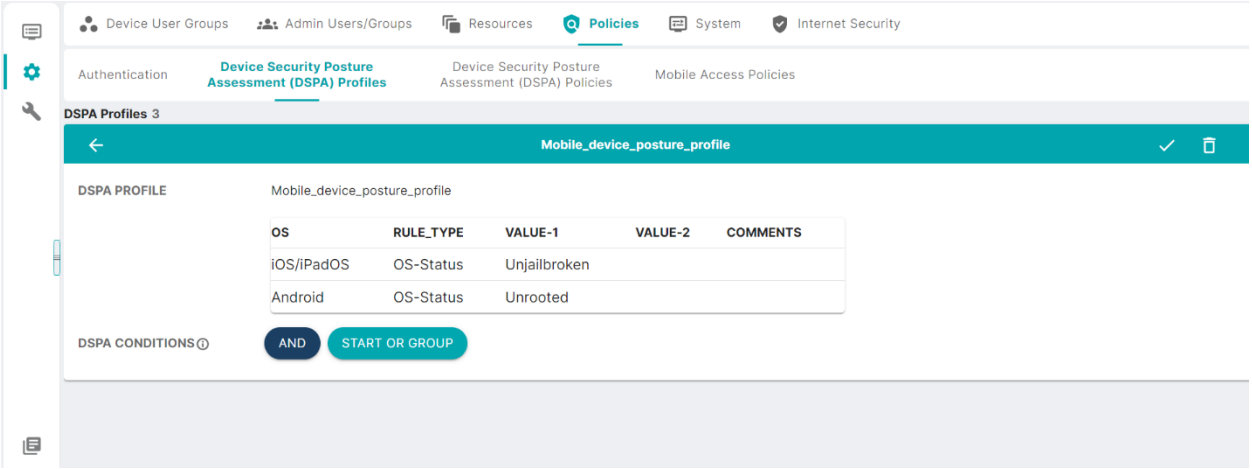
The advantages of the current device posture assessment feature for laptops are extended to mobile platforms as well.

1. **Continuous device posture assessment**: The device posture checks that sysadmin has defined are executed periodically (the interval is configurable, default is 30min) even if the user is not logged out of Cloudbrink. This will ensure that Cloudbrink can detect out-of-compliance devices in the shortest time possible.
2. **Quarantine/Deny/Log_and_Allow actions**: Customers have choice to treat non-compliance devices in different ways. Customers can either block the non-compliance device completely (Deny action) or put the device in a quarantine state with limited app access (Quarantine action) or simply allow full access but notify the administrator about non-compliance state (Log_and_Allow action)

Configuration

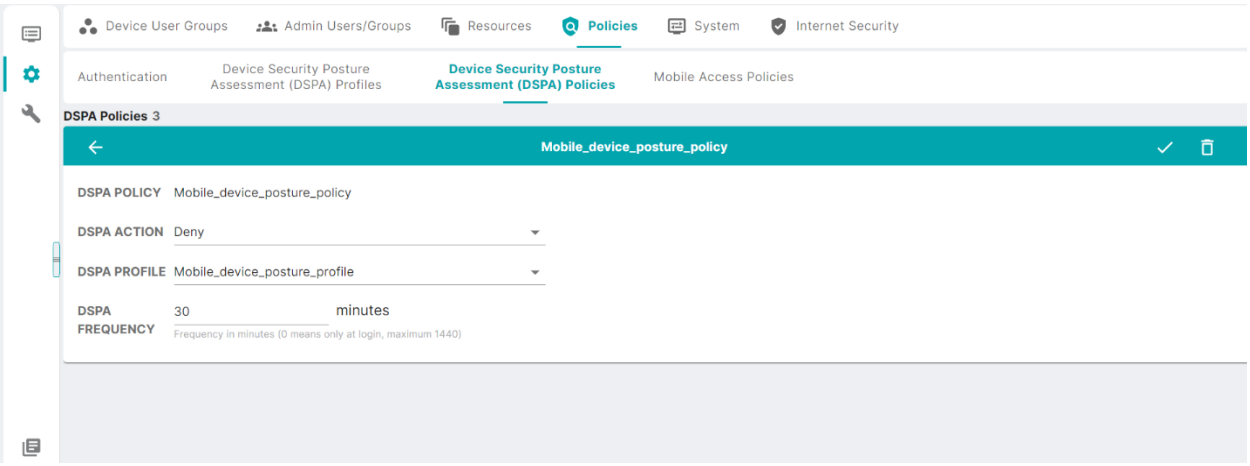
Step-1: Create a new Device Posture Assessment profile with Mobile DPA checks

Configure → Policies → Device Security Posture Assessment (DSPA) Profiles



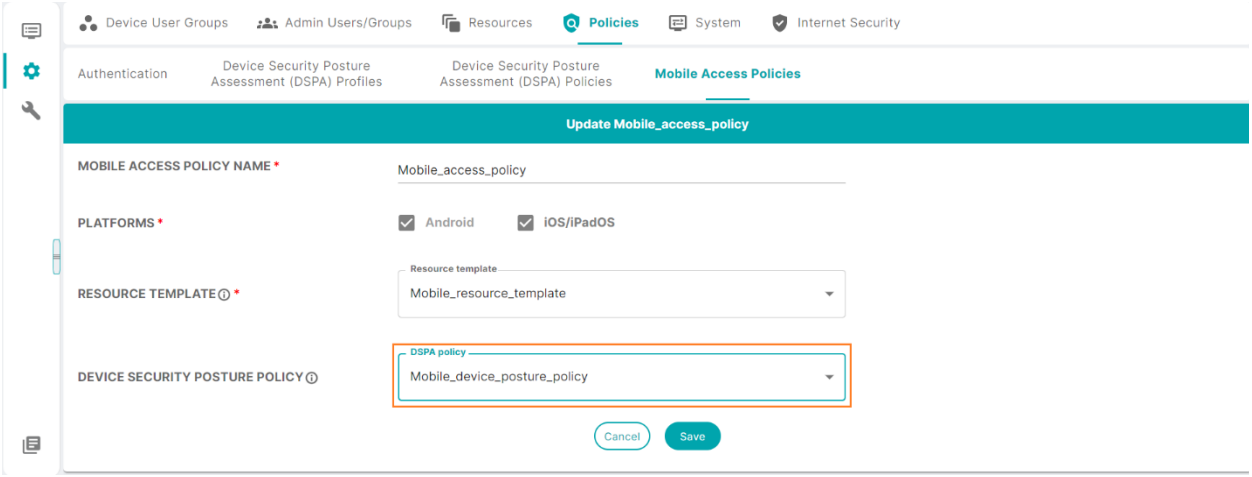
Step-2: Create a new Device Posture Assessment policy by using the profile created in step-1, and set continuous check to 30min

Configure → Policies → Device Security Posture Assessment (DSPA) Policies



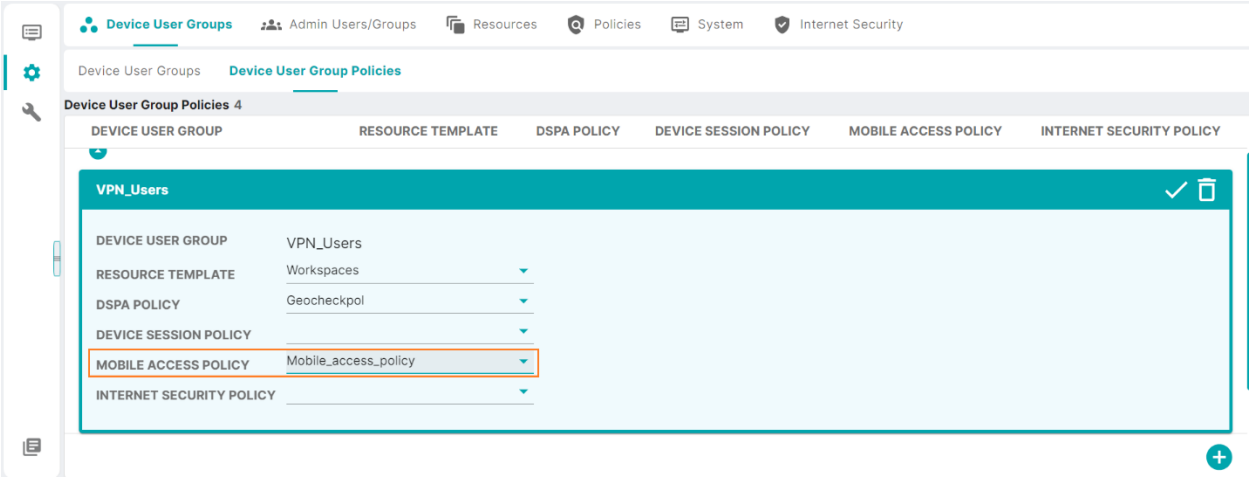
Step-3: Update the existing Mobile Access Policy (or create a new mobile access policy if not already exists) and select the newly created Device Posture Assessment policy from the drop-down

Configure → Policies → Mobile Access Policies



Step-4: Assign the Mobile Access Policy to a device-user-group if it is not already assigned

Configure → Device User Groups → Device User Group Policies



With above configuration, users can access business apps defined in the Mobile_resource_template only if their device is not jailbroken (iOS/iPadOS) or rooted (Android). If the device is jailbroken/rooted, access will be denied (Deny action) to these business apps.

2.10. Applications and Resource-Templates

Applications are the services that the end users access to perform their duties. There are different types of applications that Cloudbrink supports.

a) **SaaS applications** :- SaaS applications are those apps that customers subscribed to for their users. Examples are Office 365, Workday, Salesforce, Zoom, etc.
b) **Cloud-hosted applications** :- These apps are customer self-managed applications that are hosted on a public or private cloud. For example, customers might use AWS VPC to host some of their application servers. Users are expected to access these applications to perform their job.
c) **On-premises data center hosted application**s:- Many customers maintain their own data centers with hardware and virtualization infrastructure for hosting applications. Users need to access these applications hosted in on-prem data centers as well.

Resource-Templates:- Resource-Templates are groups of applications which can be assigned to the Device-user-groups. Administrators must configure the set of applications (resource-templates) they wish to be made available to their end users. These applications should be grouped into Resource-Templates, which are then assigned to the Device-user-groups, so only those users who are part of the Device-user-group can access the applications.

Types of Applications/Services

Cloudbrink uses the classification below for applications/services, so that customer's use cases can be met with minimal and simple configurations.

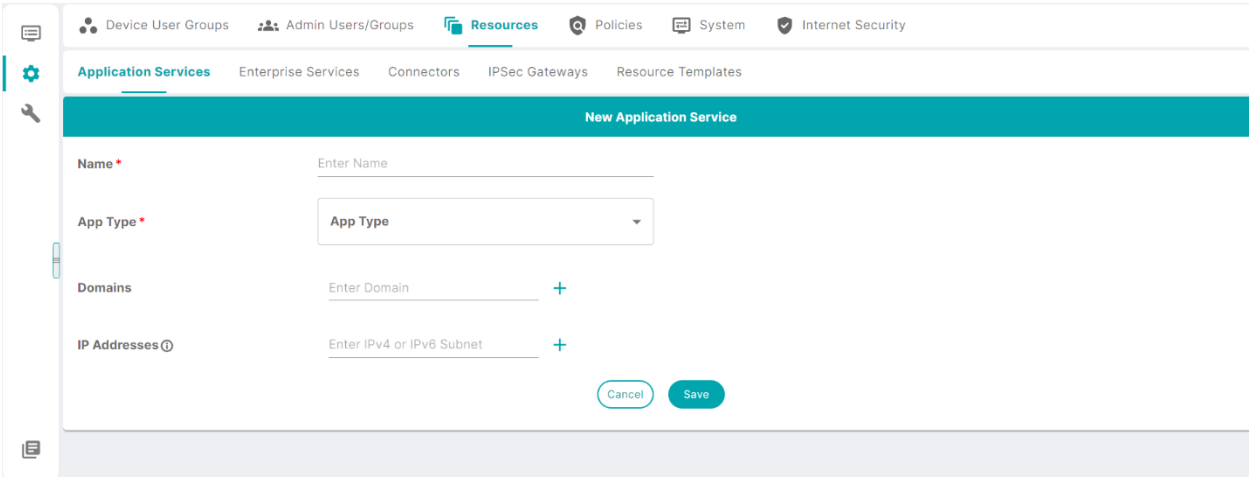
Application Services

Application-services are SaaS applications that are reachable directly over the Internet. Cloudbrink provides a set of built-in SaaS applications (aka. Standard apps) so that customers can directly use them to create resource-templates.

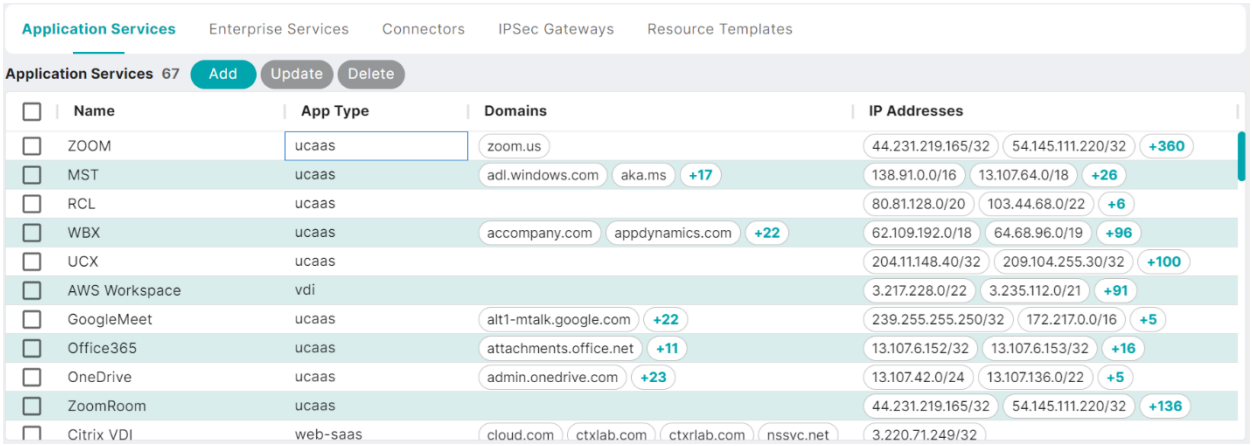
In addition to the built-in SaaS applications, customers can configure other SaaS application details that their enterprise uses. For example, Zoom is pre-configured but if a customer is using Salesforce, customer have to configure Salesforce application on the Cloudbrink portal.

As part of application-service configuration, customer must specify the domain name or public IP addresses of the application that will be used by Cloudbrink to identify the data traffic from this application. Below are the details of each parameter.

- **Name** → Name of the application service that is being created
- **App Type** → App-type indicates what is the type of the application service being created. Admin can select one of the built-in standard-app as reference to indicate the type. App Type provides a drop-down from which admin can select one of the standard-app.
    - For example, if admin is a new standard-app for Box service which is a document sharing service, the App Type could be OneDrive.
    - If there is no clear standard-app, admin can select generic profile “Web-SaaS” or “UCaaS” as the App Type
- **Domains** → The list of domain-names that could be used for identifying the application service traffic
- **IP Addresses** → If the SaaS application service provides the list of public IP addresses where their service is available, that IP ranges can be added here. This is an optional parameter.



Built-in standard apps and customer-added custom/internet apps



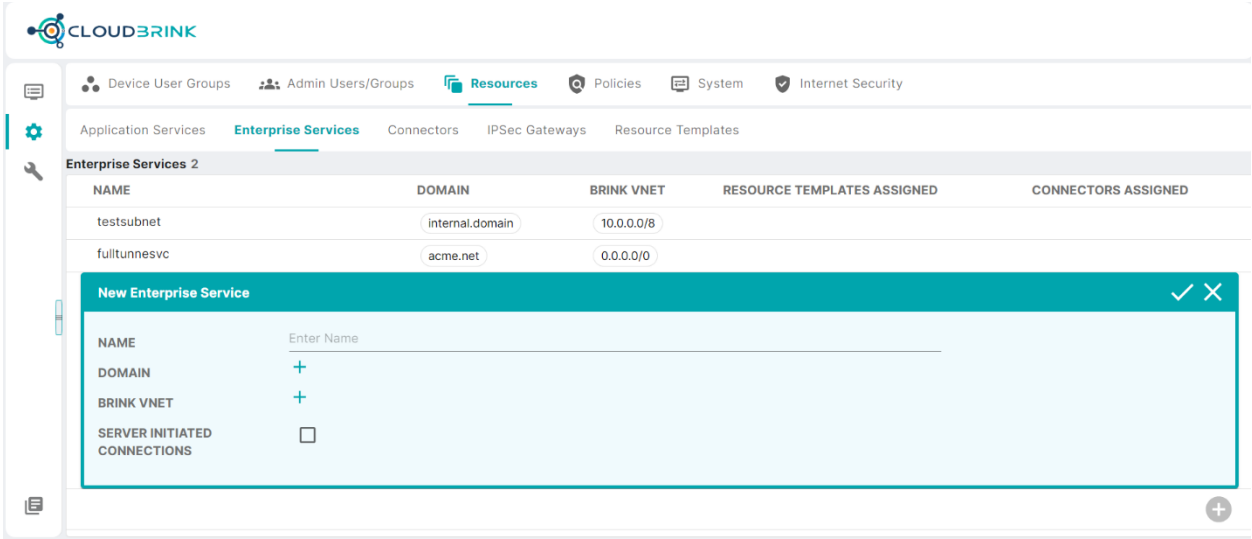
Enterprise Services

Enterprise-services are the private applications that are hosted inside the physical on-premises datacenter or public/private cloud VPC/VNETs by the customer.

Customers can specify the enterprise-services using the IP range or domain-names of the private applications. These enterprise-services will be used in the resource-template configuration to decide which private apps a user can access.

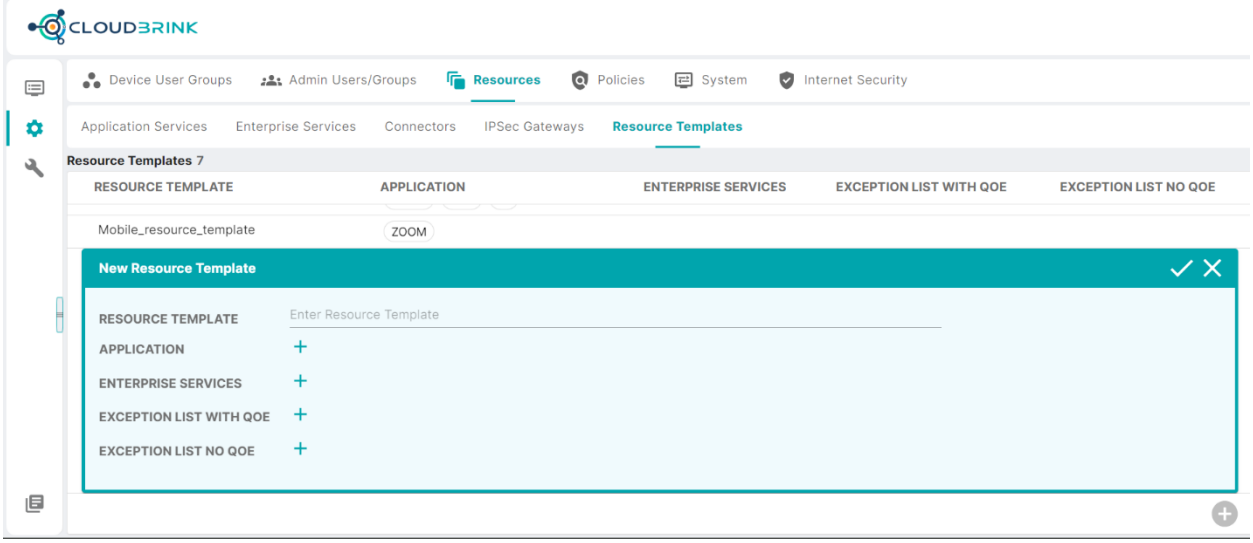
The enterprise-services must be associated with the Connector also so that Cloudbrink can determine which datacenter is hosting these enterprise-services.

Private apps hosted in customer-managed datacenters (on-prem or cloud)



Below given are configuration pages where admin can add the SaaS applications, Cloud-hosted and on-premises hosted applications, create a resource-template and finally assign the resource-template to a device-user-group.

Resource-template creation that groups set of apps



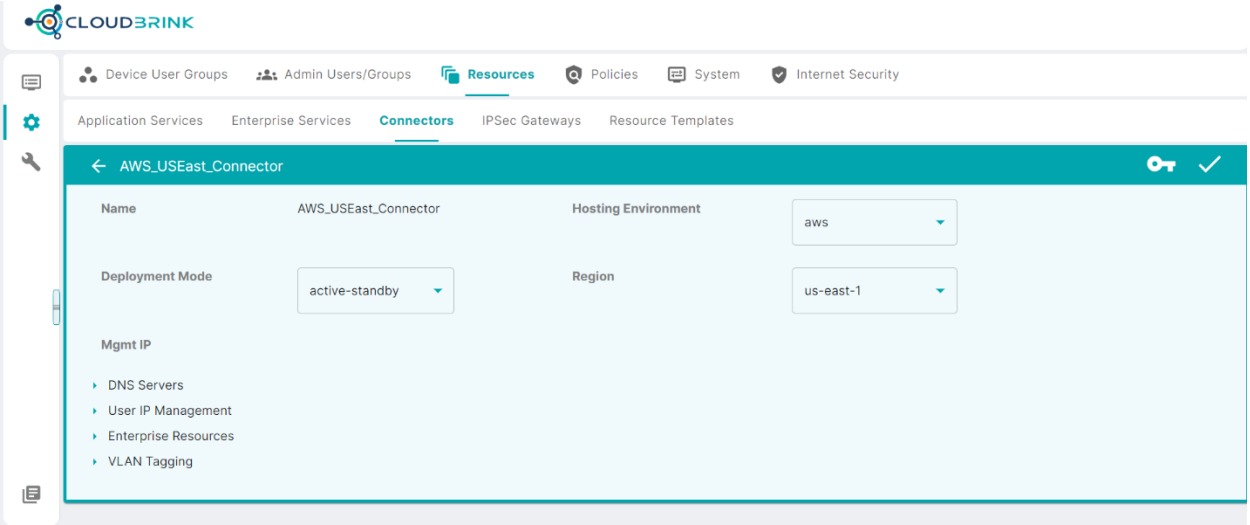
3. Connector Management

Cloudbrink Connector component is a virtual appliance deployed in the customer premises (physical data centers, public/private cloud VPCs). Cloudbrink Connector is required to provide connectivity to the applications/services hosted inside these datacenters/VPCs/VNETs, as well as to enforce the access control policies and enterprise private IP and DNS management.

The complete lifecycle management of the Connector component will be done from the Cloudbrink Administration portal by the customers. There is no configuration or management activity that is needed on the Connector directly.

Cloudbrink Connector VM always establishes an outbound mutual TLS 1.3 secure connection to the Cloudbrink SaaS and Cloudbrink Edges. Since this communication is outbound (from datacenter to Internet), there is no need to open any Firewall ports on the Internet side by the customers. This is exactly in alignment with the Cloud Secure Alliance (CSA) definition of Software-Defined Perimeter black cloud concept that is recommended as the future of datacenter secure access.

Connector environment related info



Management-IP (MGMT IP) field under the Connector details provides the IP address assigned to the Connector VM. In case of standalone or HA pair, the Connector VM instance which is acting as “Primary” (actively handling user traffic) is shown in GREEN color.

3.1. Use Cases

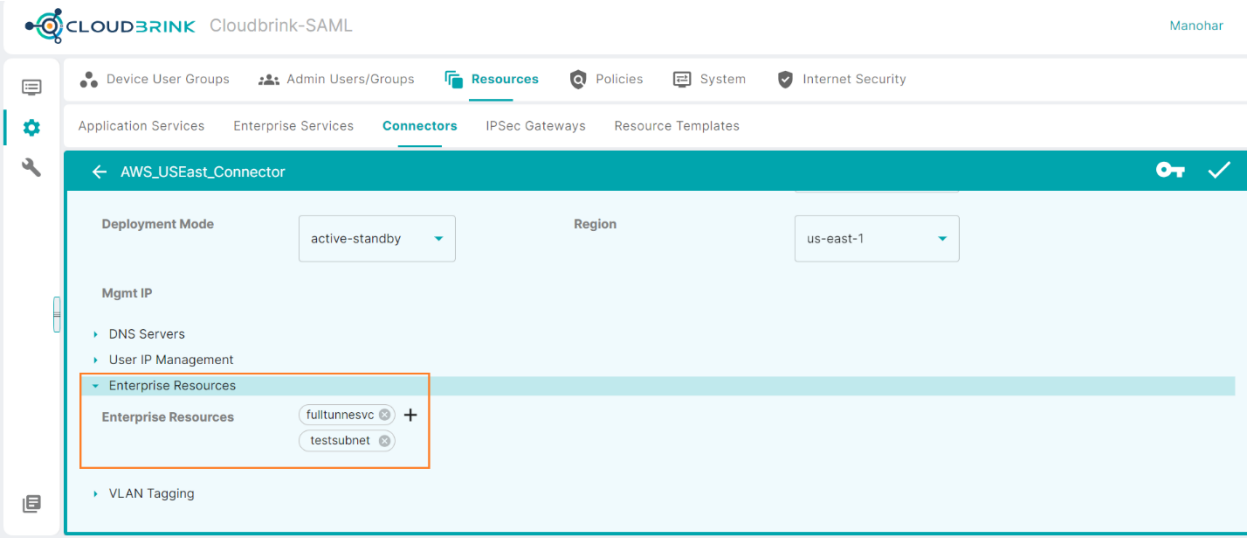
Below are the use cases where customers will need a Cloudbrink Connector.

3.1.1. Connectivity for data-center applications

Customers have deployed self-managed applications in their own data centers - either physical data centers or co-location or public and private clouds such as AWS VPC or Azure VNET.

In such a deployment scenario, a Cloudbrink Connector should be deployed in the data center or cloud to provide end-to-end connectivity from the user up to the application. Once Connector is deployed successfully on the customer premises, Connector will initiate outbound connections to the nearest Cloudbrink Edges as well as Cloudbrink SaaS for management plane traffic. After successful registration and connection to the Cloudbrink Edge infrastructure, traffic from the end-users to the data-center applications will flow via the Connector.

Associate datacenter apps (Enterprise Services) with Connectors



3.1.2. Enterprise Private IP for Remote users

Some customers want to assign datacenter private IP addresses for remote user connections coming into their data center. The intranet or private IP addresses for remote user connections will help in tracking and auditing user activity inside the data center. In some cases, these intranet or private IP addresses are whitelisted on internal firewalls for providing access to restricted subnets.

Cloudbrink supports four options for managing the private IP addresses for remote users.

i) Source NAT
ii) DHCP v4
iii) DHCP v4v6
iv) Static IP Pools

Source NAT

In this method, all user sessions share the same private IP address that is assigned to the LAN interface of the Connector VM. Since the private IP address is shared among all user sessions, whitelisting of IP address for access or auditing is not possible in this method.

DHCP v4

Cloudbrink Connector will act as the DHCP client on behalf of the remote user connection and fetch the intranet IP address from the DHCP server inside that data center. Once the DHCP server issues an intranet IP address for the remote user connection, the Connector will own the IP address on behalf of the remote user and uses this IP address for all user traffic inside the data center.

For the Connector to fetch the intranet IP address from the DHCP server, administrators must provide DHCP server information as part of the Connector configuration on the Cloudbrink management portal. If DHCP server IP is specified, Connector uses unicast DHCP requests to fetch the IP address. If DHCP server IP is not specified, Connector uses broadcast DHCP requests.

DHCP v4v6

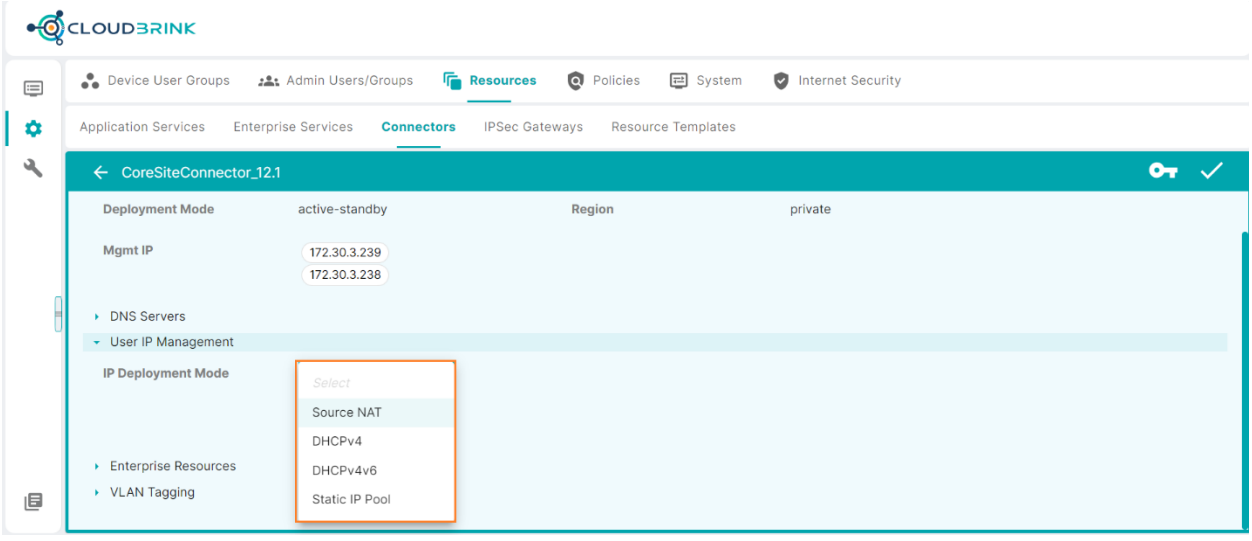
This option is similar to DHCP v4 option but in this case, Connector will try to fetch both IPv4 as well as IPv6 private addresses for the user session. Customers must use this method if they want users to access IPv6 based applications hosted inside their datacenters or cloud VPCs.

Static IP Pools

Customer can manually configure a range of private IP addresses from which Connector will issue IP addresses to the remote user sessions. It is like DHCP method where Connector itself is acting like a DHCP server without relying on any external DHCP server.

Customer can specify static IP pools for both IPv4 and IPv6 addresses and assign the pools to specific device-user-groups.

User IP management options



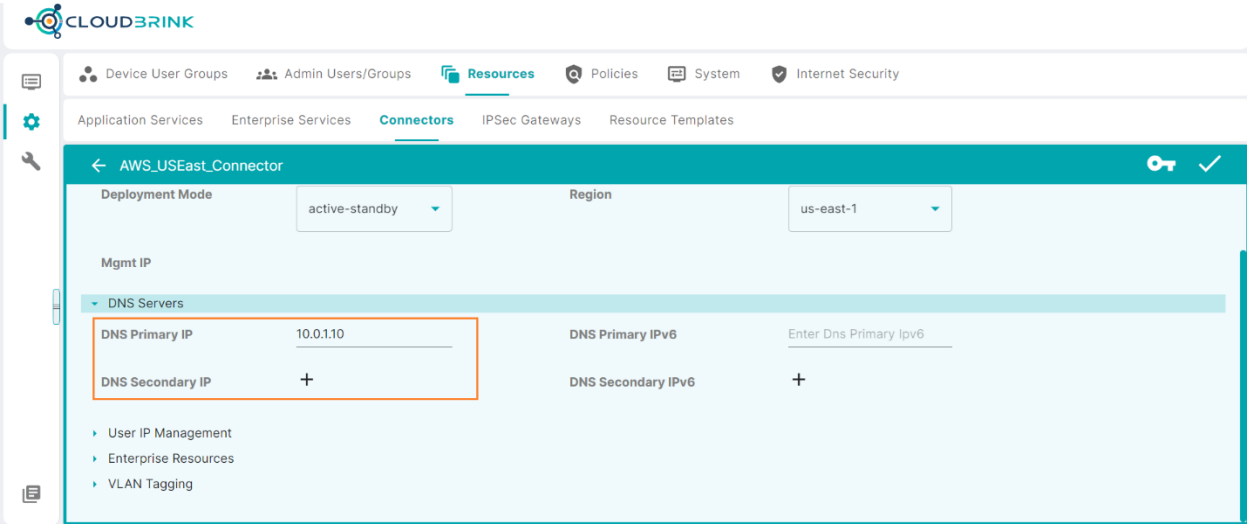
3.1.3. Enterprise DNS support

When customers deploy self-managed applications inside their datacenters, the domain names for these applications are resolvable only by the enterprise's DNS server. Public DNS servers cannot resolve these domain names since they're private domains.

To enable intranet application access using domain names, Cloudbrink supports DNS resolution using enterprise DNS servers inside the datacenters. When an end user attempts to connect to intranet applications using domain names, the Cloudbrink Agent intercepts the intranet domain name requests and forwards the requests to the Connector component deployed inside the datacenter. The Connector component resolves the domain name on behalf of the user and returns the IP address information to the Cloudbrink Agent. In this way, remote users can use enterprise DNS for intranet name resolution.

Customers must provide primary DNS server IP information as a mandatory parameter in the Connector. Secondary DNS servers also can be configured on the Connector. Secondary DNS servers will be used to resolve the private domain names when the primary DNS server is not reachable or not responding.

Enterprise DNS server configuration

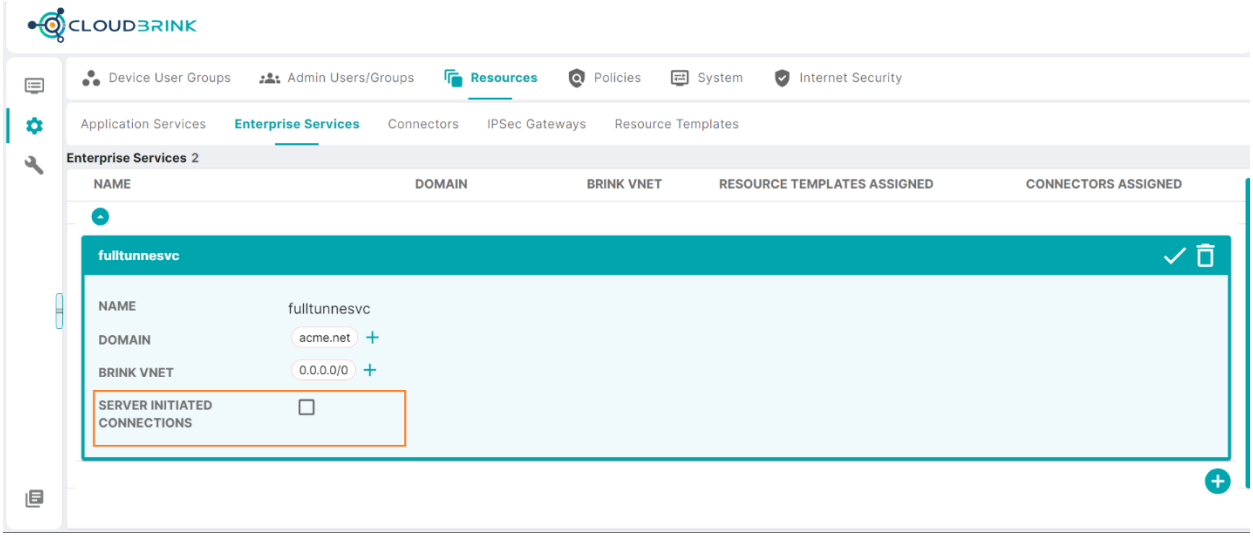


3.1.4. Server-initiated connections

Customers have few applications inside the datacenters that require to open a new TCP or UDP connection back to the remote user endpoint. Such reverse connections are referred to as server-initiated connections.

Cloudbrink supports server-initiated connections. Admins have to enable the server-initiated connections capability on a per enterprise-service level.

Server-initiated connections enable button

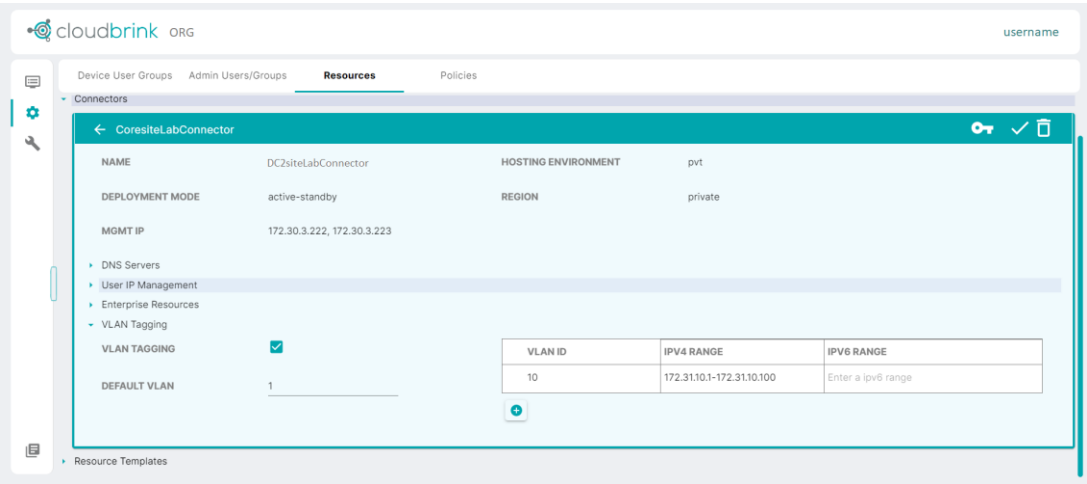


3.1.5. VLAN Tagging

Customers would have some datacenters which are partitioned using VLANs. In such cases, customers would like to ensure that even remote user endpoints communicate within the same VLAN. To enable such capability, Cloudbrink supports VLAN tagging feature.

Admins can configure VLAN tags and specify the private IP range which will be associated with the specific VLAN tags. When the Connector assigns a private IP address to the remote user session, the VLAN tag associated with this private IP address will determine the VLAN for the remote user endpoint. Once this is determined, Connector will allow traffic only if the destination IP address also belongs to the same VLAN such that remote endpoint communicates only to that VLAN IP.

VLAN tagging configuration on per VLAN basis



3.1.6. Automatic Connector Selection

Some customers have redundancy planned across datacenters. These customers deploy same applications/services across multiple datacenters located in different geographical regions. In case one of the datacenters is unreachable for whatever reason, users will be redirected to the other active datacenter. This avoids any downtime for the users to access their applications/services.

To support above use case, Cloudbrink provides a feature called automatic connector selection. In this case, customers define the enterprise-services on Cloudbrink and associate these enterprise-services on all the Connectors which are deployed in the redundant datacenters.

When a user logs in to Cloudbrink service from the Agent, Cloudbrink determines the datacenter (corresponding Connector) which is geographically closer to the user location and connects the Cloudbrink Agent to that datacenter.

If the datacenter goes down, all users who were supposed to connect to that datacenter will be redirected to the next closest datacenter. Since the same enterprise-services are available on all datacenters, users will never experience any downtime.

3.2. Private IP on Local Interface

The Cloudbrink Connector will assign an enterprise private IP address which is part of the local datacenter network to the remote user sessions. This private IP is used for traffic communication between the Connector and backend resources. The private IP address can be assigned by Connector in multiple ways as discussed in section 3.1.2 of the Cloudbrink Admin Guide.

Usecase

By default, this private IP address is used only within the datacenter communication and not used on the Brink App. There are some applications used by the customers which use the IP address assigned to the endpoint's local interface for authorization at the server-side. In such as scenario, the endpoint's local interface IP address and the private IP address assigned for the remote user session from this endpoint do not match, and server authorization would fail.

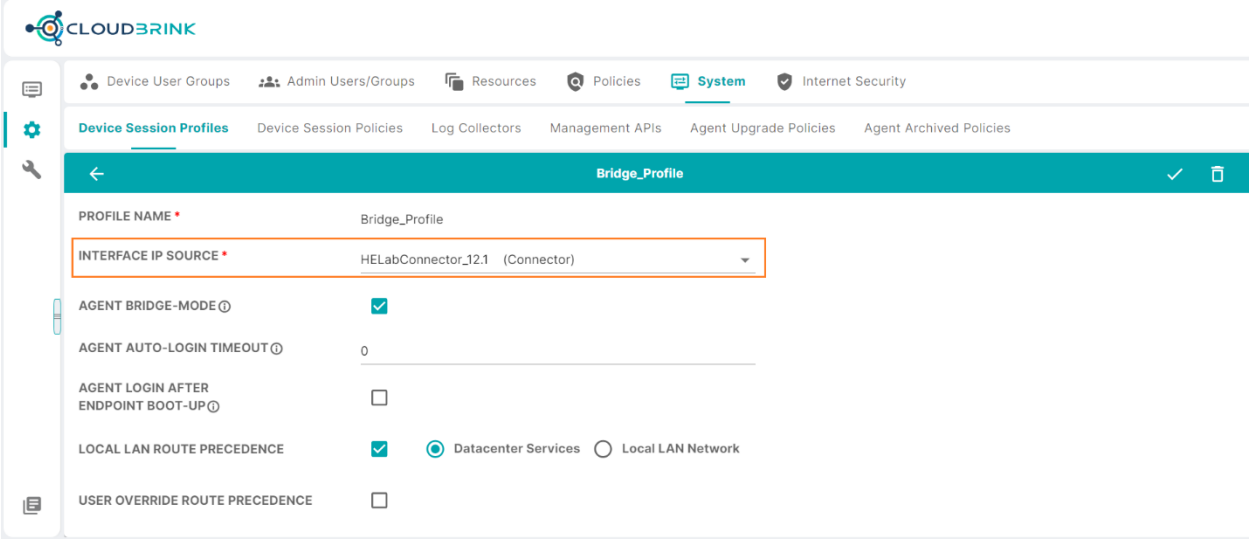
To support use cases as described above, Cloudbrink added support for "enterprise private IP on local interface" feature. Customers can now enable Brink App to configure enterprise private IP address on the endpoint's local interface. Once Brink App configures the private IP on local interface, user applications that rely on local interface IP address can now successfully authorize with the server.

Cloudbrink supports hybrid-multi-cloud connectivity which enables users to connect to all their on-premises and cloud-based datacenters simultaneously. In such a scenario, customers must select one specific Connector from which the private IP address will be fetched and used on the endpoint local interface.

Configuration:

Step-1: Configure Device Session Profile

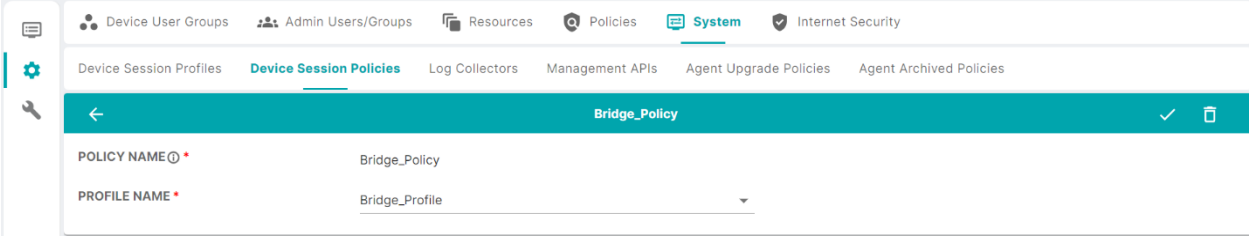
i. Navigate to Admin portal → Configure → System → Device Session Profiles and add a new profile.
ii. In the window to add new profile, provide a profile-name and select the Connector which will issue the private IP address that will be configured on the local interface.



Note-1: By default, Cloudbrink assigns "Brink IP" (Cloudbrink auto-generated IP) on local interface. Customer can select that option as well under the "Interface IP Source" drop-down instead of a Connector.
Note-2: Cloudbrink supports ability to connect to multiple on-prem and cloud datacenters simultaneously. But only one private IP can be assigned to the local interface of the user endpoint at a time. Hence, admin must select that Connector which would assign the private IP that must be used on the local interface.

Step-2: Configure Device Session Policy

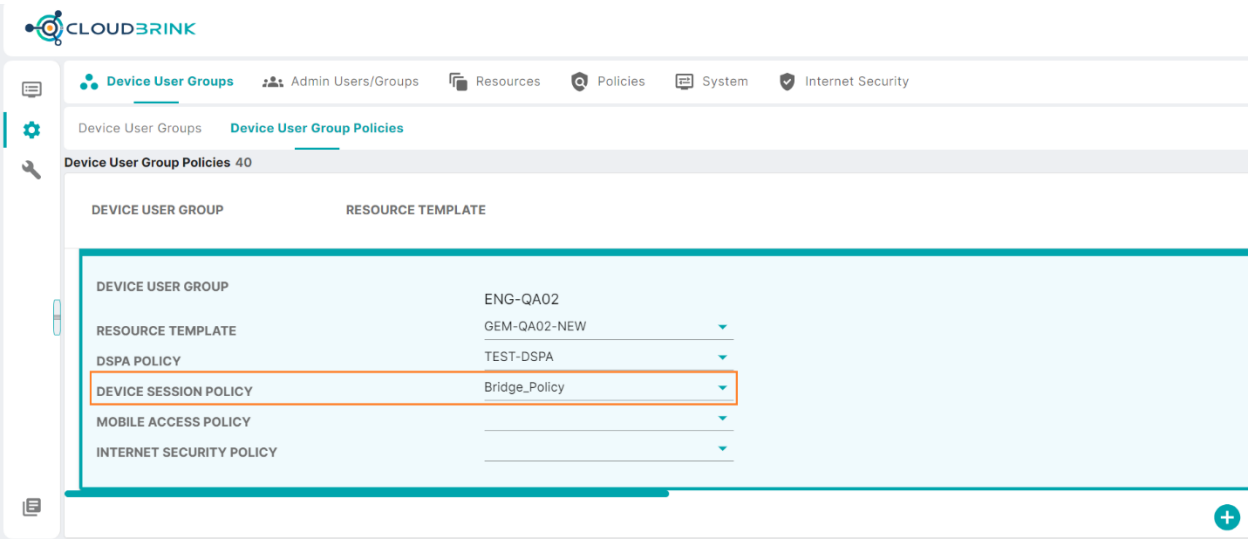
i. Navigate to Admin portal → Configure → System → Device Session Policies and add a new policy
ii. In the window to add a new policy, provide a name for the session-policy and select the profile created in the previous step from the drop-down.



Step-3: Assign the Device Session Policy to the Device User Group

i. Navigate to Admin portal → Configure → Device User Groups → Device User Group Policies, and select the device-user-group to which the device session policy must be assigned

ii. In the window for assigning policies, select the device session policy created in the previous step for "DEVICE SESSION POLICY" field



With above configurations, all users belong to the specified Device User Group will have their endpoint local interface configured with the private IP address of the datacenter which has the Connector selected under "INTERFACE IP SOURCE" in step-1.

3.3. Specifications

The Cloudbrink Connector is a virtual machine hosted in the customer's premises for supporting apps hosted in the data center or cloud VPC/VNETs.

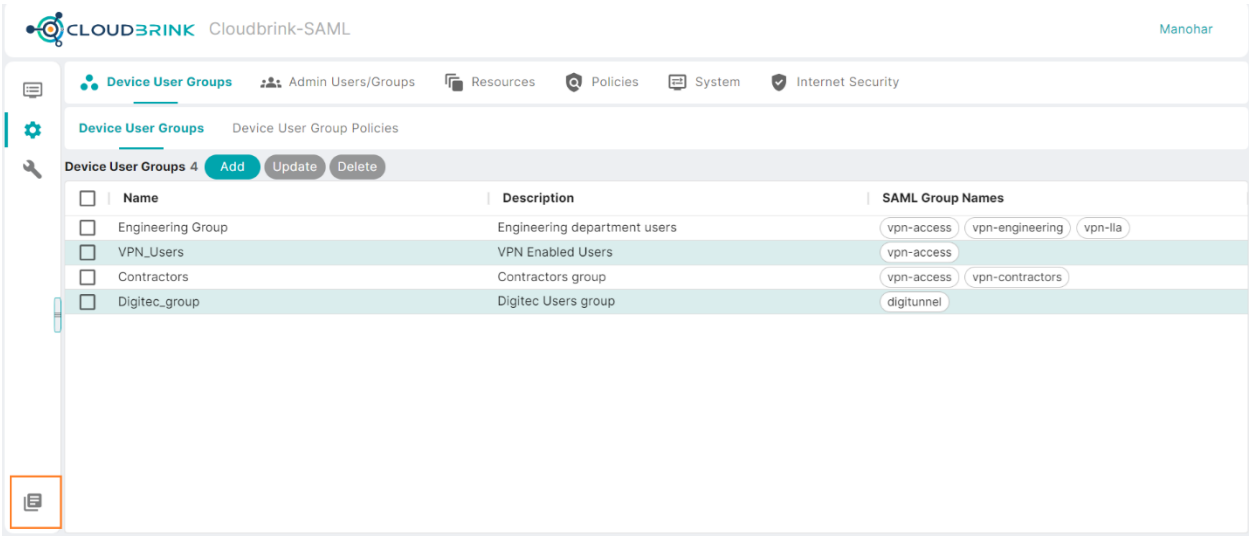
Platform	Cores	RAM	Hard disk
ESXi	8	16GB	50GB
KVM	8	16GB	50GB
Hyper-V	8	16GB	50GB
AWS	8	16GB	50GB
Azure	8	16GB	50GB
GCP	8	16GB	50GB

3.4. Deployment and Provisioning

The step-by-step procedure for deploying the Connector is provided in the below “How-To” guide.

The How-To Guides are available under the Documentation section of the Cloudbrink management portal.

Documentation section on the management portal



3.5. Upgrade

Cloudbrink releases new software for all components at regular intervals. Cloudbrink Connectors which are deployed inside the data center can also be upgraded from the Cloudbrink SaaS. Admins can check

the version and health status of the Connector component from the Cloudbrink SaaS portal, and upgrade to newer versions.

Currently, Cloudbrink offers Connector management as a service to the customers so that customers need not worry about upgrades of Connectors. Cloudbrink will coordinate with customers to upgrade during customer's maintenance window.

3.6. Resiliency

Cloudbrink Connector component is needed for providing secure zero-trust access to private applications hosted inside the customers private networks. Cloudbrink supports access to private networks in a physical on-prem datacenter or virtual CSP hosted datacenter such as VPC/VNET on AWS, Azure or GCP.

From 14.2 release, Cloudbrink will support Connector deployments in Active-Active mode on AWS, apart from the earlier modes of Standalone or Active-Standby. The Active-Active mode of deployment is available on AWS only for the 14.2 release.

NOTE: Detailed deployment guide for Connectors in general or for Active-Active Connectors on AWS, please refer to the Documentation section (How-To Guides) on the Cloudbrink Admin Portal

4. Cloudbrink Agent

Cloudbrink Agent is the client-side component of the overall solution that will be installed on the end user devices – desktops and laptops. The Cloudbrink Application is required for authentication, device posture checks, and secure end-to-end connectivity, all through a simple user interface.

4.1. Supported Platforms

Cloudbrink Agent is supported on the below platforms.

Client Platform	**Version Supported**
Windows	Windows 10, 11
Mac OS X	macOS 12.x, 13.x and 14.x
Linux	20.04 LTS and 22.04 LTS Kubuntu 20.04 LTS

FreeBSD	FreeBSD OS 14.x LTS
iOS	iOS 17.x, 16.x and 15.x
Android	Android 14.x, 13.x and 12.1.x
Chromebook	ChromeOS 120 LTS

4.2. Download and Installation

Customers can download the latest version of Brink Agent at the below link. Once users install the Agent, admin can manage the Agent versions of their users using the "Agent Upgrade Policies" from the management portal.

https://cloudbrink.com/brink-app-download-latest/

4.3. Brink Agent UI Auto-Start

Customers can control if the Brink Agent UI needs to start automatically or not after the installation process is complete. By default, the Brink Agent UI pops-up after installation and prompt user for login info. But, if customer do not want the UI to pop-up after installation, it can be controlled via the methods specified below.

Use case: When customers are updating the Brink App on end-user devices using an MDM solution (eg: Intune), and don't the users to be interrupted with installation success or login prompts during this update, this capability is helpful.

Windows:

It will be an additional command line option that will be passed to the installer command.

Example:
> msiexec.exe /i BrinkAgent-13.2.143.msi NO_GUI=1

MacOS/Linux:

Rename the installer/package file to include NO_GUI string at the end.

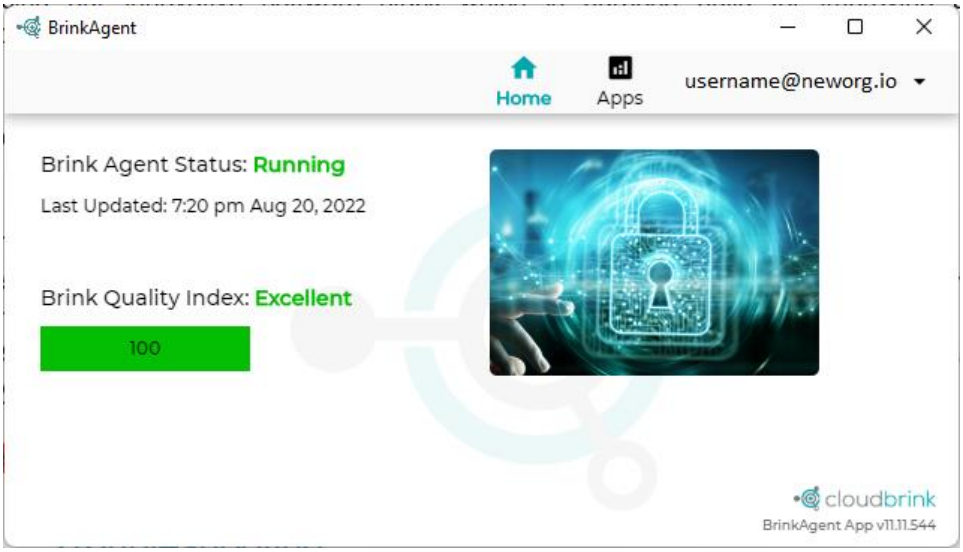
Example: BrinkAgent-13.2.143_NO_GUI.pkg

4.4. End User Brink Quality Index

The Cloudbrink Agent provides a simple user interface for end users to check what level of Brink Quality Index they are receiving. Brink Quality Index is a measure of the QoX that Cloudbrink delivers using our innovative software stack which is purpose build for improving app performance.

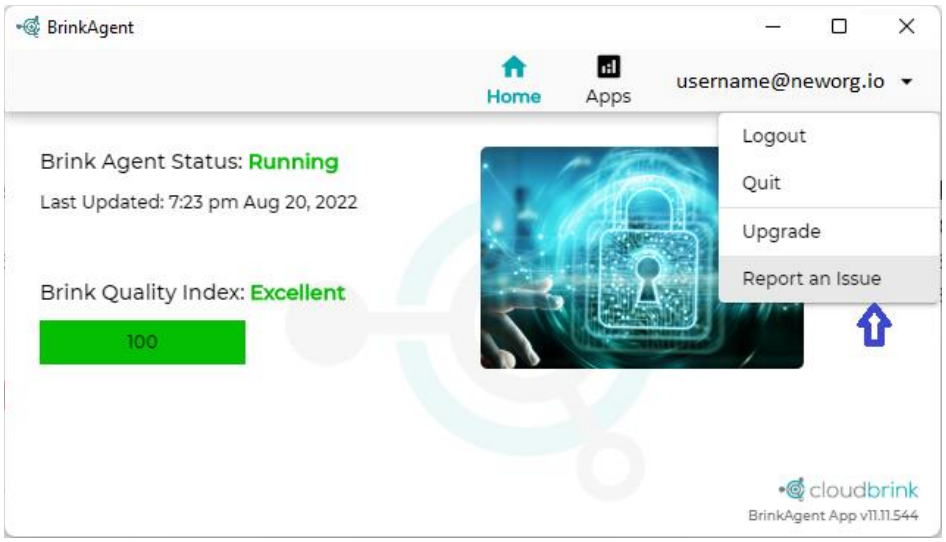
Brink Quality Index is a quantitative measurement which ranges from 0 to 100. Below is the interpretation.

- 80-100 → EXCELLENT (user is receiving best possible QoX over Cloudbrink)
- 60-79 → GOOD (user is receiving next-to-best possible QoX over Cloudbrink)
- 40-59 → AVERAGE (user is receiving optimal experience only, possible because of very high physical network issues such as packet drops)
- 0-39 → POOR (user is receiving poor experience because physical network issues are very high and even with Cloudbrink, network can't recover from bad conditions)



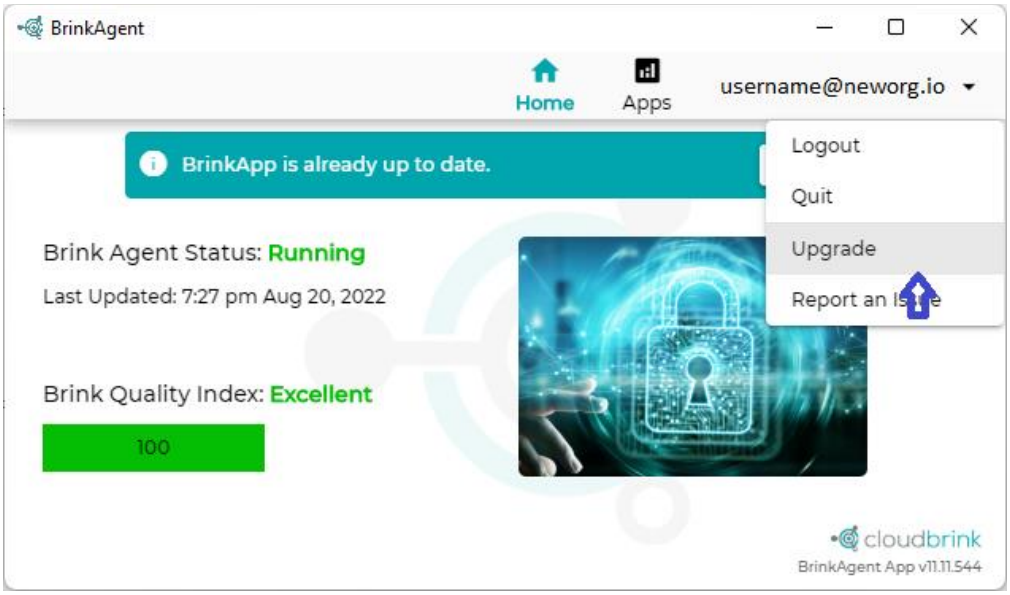
4.5. Troubleshooting

When an end user encounters any issue, it is very simple to report the issue to Cloudbrink. The Cloudbrink Application window provides a "Report an Issue" button in the drop-down window. Once a user clicks this button, the Application collects all needed logs and uploads a compressed bundle to the Cloudbrink service. This option also allows the user to download the compressed file so that they can email it to their administrator.



4.6. Brink App Upgrade Policy

With Cloudbrink, Agent management on the endpoints is made very easy for IT teams. Cloudbrink Agent provides an “in-app” upgrade option so that users can simply trigger the upgrade option from the Agent and get to the latest software. There is no need for IT teams to push the new software using distribution tools or share the Agent over file drives with all users.



Sysadmin can define the Brink App upgrade policy from the admin portal of Cloudbrink. The Brink App Upgrade Policy infrastructure provides highly flexible and granular controls for admins to define whatever upgrade policies that meet their organizational needs.

Upgrade policies can be defined at different levels.

1. Upgrade policy applicable for the whole organization
2. Upgrade policy applicable for a specific security group or business unit within the organization
3. Upgrade policy that can override the organization-level policy and specify different behaviour for specific security group
4. Upgrade policy that can override the organization-level or security-group level policy and specify different behaviour for specific users (list of email IDs) or specific platforms (Windows/Mac/Ubuntu)

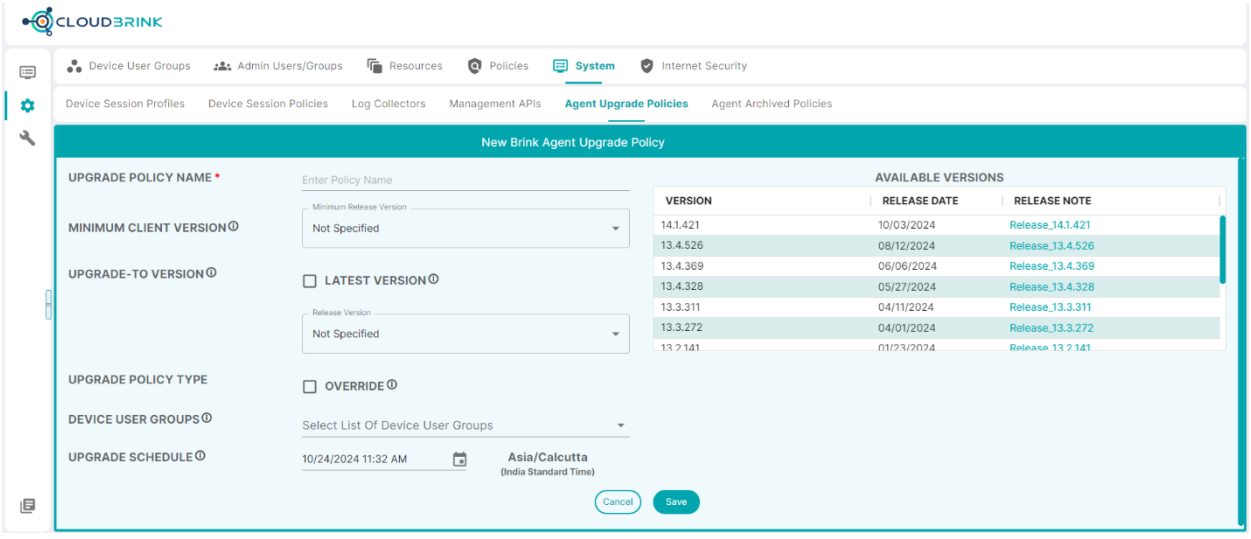
NOTE: Admins can define a “minimum client version” criteria so that all the users of the organization are mandatorily at the certain minimum software version. This helps in avoiding any user using a very older version of the Brink App that can lead to security risks.

The upgrade policy provides support for defining a scheduled date-time in future from which the policy will become activated. This helps the admins to define the policy at any time of their convenience but triggering the upgrade policy at another time which is most suitable for upgrades.
The below section provides details of each configuration parameter in the upgrade policy.

Brink App upgrade policy configuration parameters

Brink App upgrade policy config is available under below path.
Cloudbrink Management Portal (admin.cloudbrink.com) → Configure → System → Brink App Upgrade Policy

By clicking “ADD” button, admin can define the upgrade policy using below configuration window.



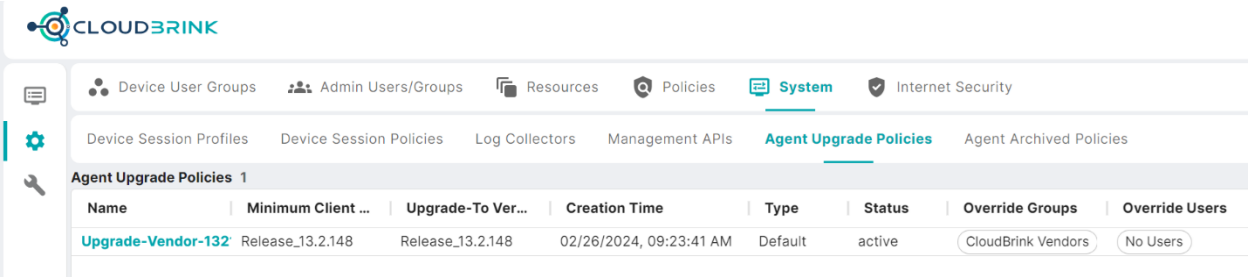
Configuration parameters description table

Parameter	Description
Upgrade policy name	Name for this policy
Minimum client version	The minimum Brink App version that is allowed to connect to Cloudbrink service. Any user using a Brink App that is lower the minimum client version will be forcefully upgraded
Upgrade-To version	When a user is upgraded, the version to which they will be upgraded is decided based on this parameter. It can take two values a. Latest version → Brink App will be upgraded to whatever is the latest version that Cloudbrink has released at that time b. Release version → admin explicitly selects this version from the drop-down. Brink App will be upgraded to this version. Note: Admin can't select both latest-version checkbox and a value for release-version at the same time
Upgrade policy type	Default → when "Override" checkbox is unchecked, it is called as default policy. Override → when "Override" policy is checked, it is called as override policy. <u>Details:</u> **Default**: • Default policy can be applied to the overall organization-level or security-group level • This policy will be Active forever (until admin deletes/modifies the policy) • Default policy ensures that the upgrade policy is applied to any endpoints that are registered in the future as well. For example, a new employee joins after one month of defining the upgrade policy and connects to Cloudbrink from the new laptop. This laptop (Brink App) will be checked against default policy. **Override**: • Override policy can be used to specify a different behaviour other than that is specified in the default policy • When override option is checked, admin can specify a different minimum client version and upgrade-to

	version for the security-group or specific users (list of email IDs) or platforms (operating system) NOTE: Default policies are active until deleted/modified but override policies are application for the “already registered” endpoints only. Once all the “already registered” endpoints are upgraded according to the Override policy, the policy will go to “Completed” state and will not be applicable for newly registered devices.
Device user groups	List of device-user-groups (security groups) to which the policy is application. If none of the device-user-groups are specified (empty list), the policy is applicable for the overall organization.
Platforms	Available only “Override” option is checked The policy is applicable for only those platforms (operating systems) specified in this parameter
Override users	Available only “Override” option is checked The policy is applicable for only those users (list of email IDs) specified in this parameter
Upgrade schedule	The time at which the policy will be activated.

Summary table

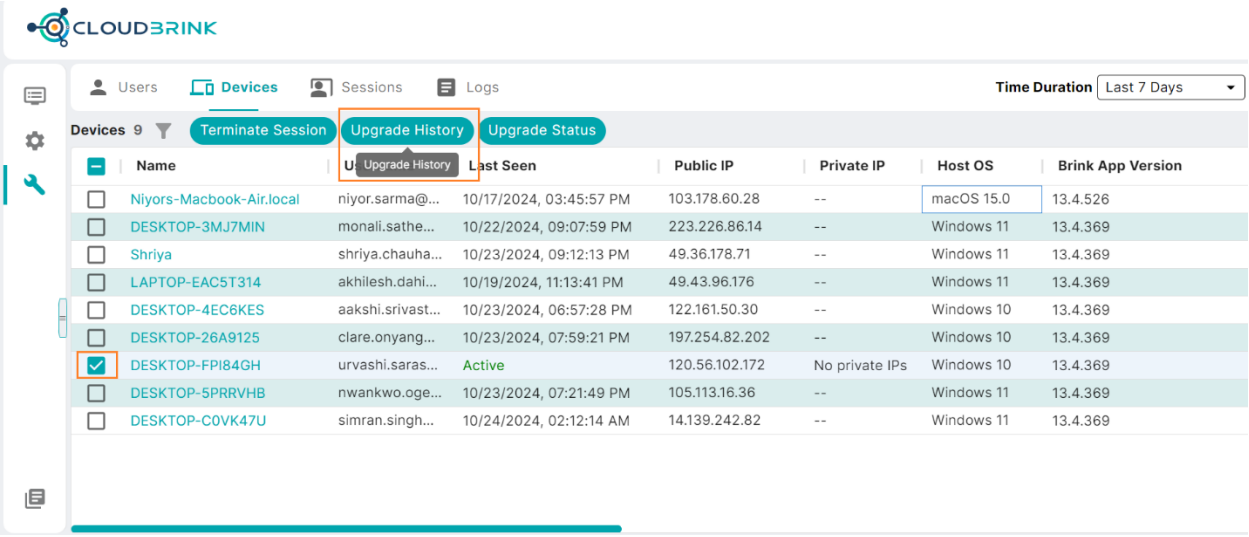
All the configured Brink App upgrade policies will be displayed in the summary table. The summary table provides the “Status” information of each of the policy.



4.6.1. Brink Agent Upgrade History

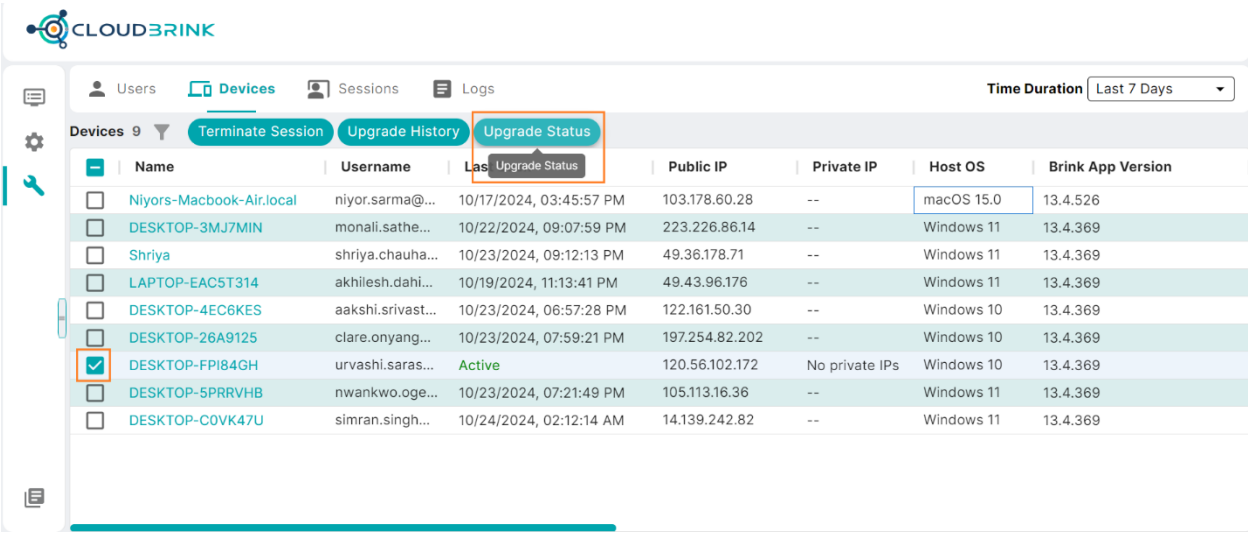
Customers can view the history of the upgrade events that the Brink Agent underwent on a specific device. Admin can select a device from Troubleshoot → Devices tab and select “Upgrade History” option to see the last 5 upgrade events, the versions in the upgrade and final status of the upgrade event.

This is very helpful for admins to determine if any user is facing issues with Brink Agent or access related issues due to upgrades.



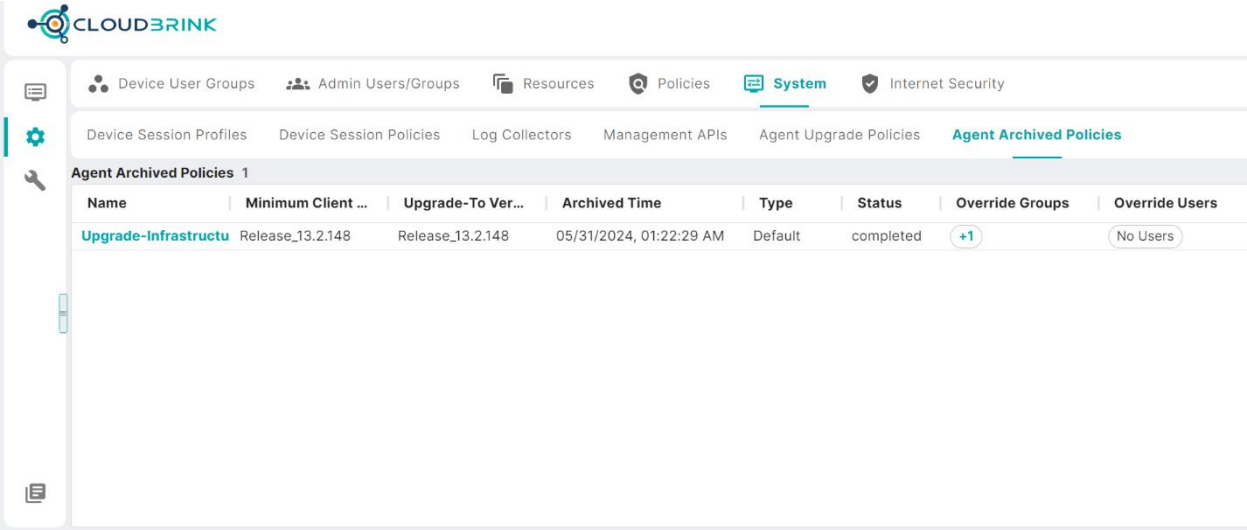
4.6.2. Brink Agent Upgrade Status

Admins can also view the status of the last upgrade event of the Brink Agent on a specific device.



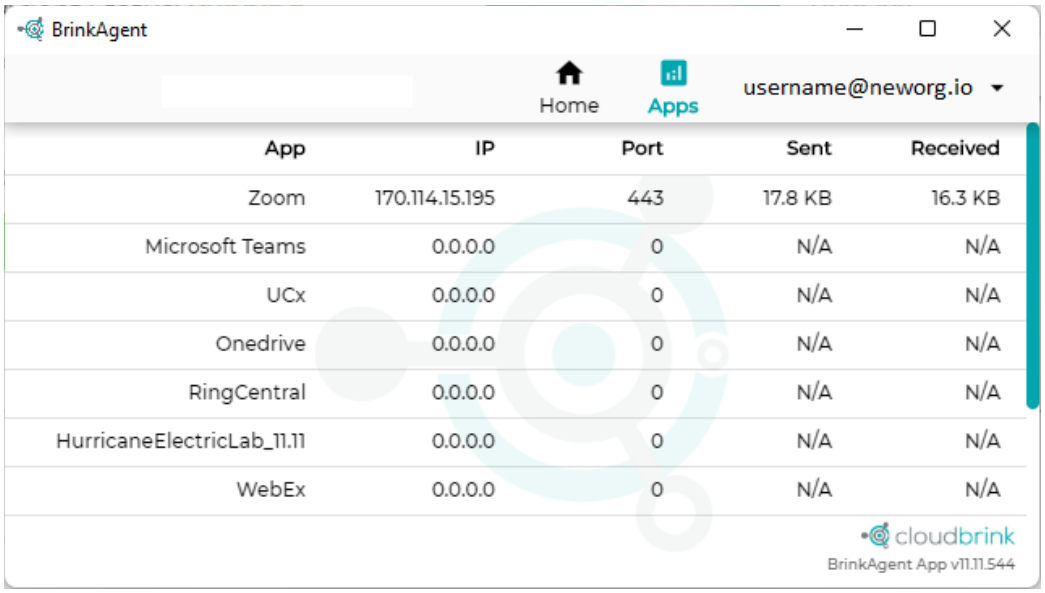
4.6.3. Upgrade Policy Deletion

When a customer deletes an existing upgrade policy, the policy will be moved to “Archived” section on the admin portal. This is useful for customers to check the previously used policies in the future for any reference or troubleshooting.



4.7. Applications

Cloudbrink Agent provides application view where users can see all the applications that the admin has enabled for them, and which apps are actively transmitting data traffic. If user can see a particular application on the Apps tab but the app is not working, user knows that there is an issue with configuration or data path. If an application is not listed in the Apps tab, user knows that admin did not enable that particular app to this user.

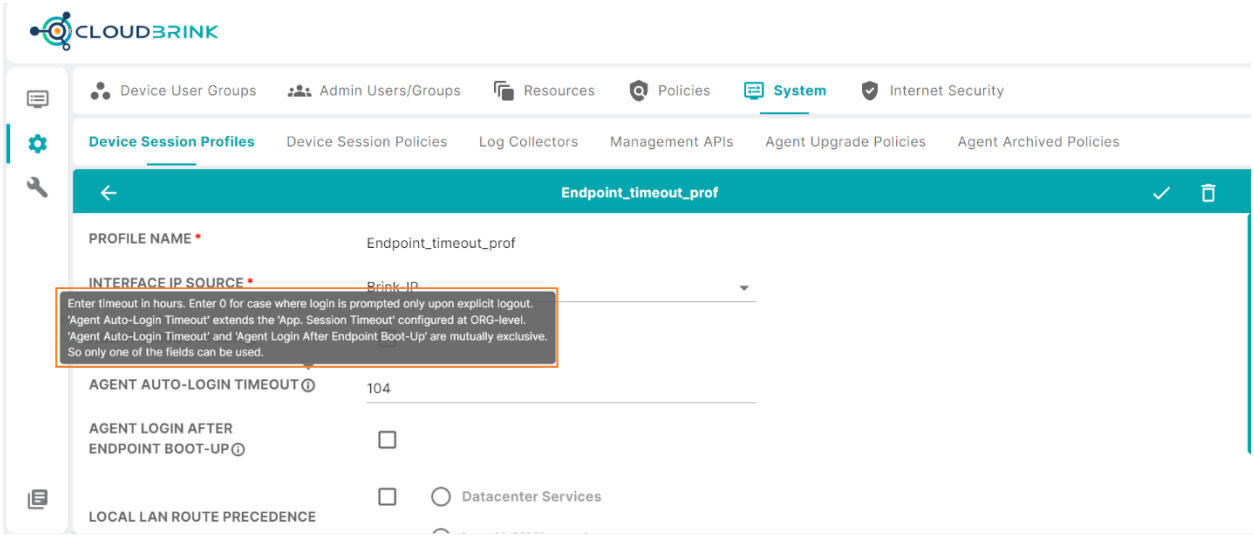


4.8. Brink App Auto-Login

Auto-Login feature enables customers to configure different timeouts for different device-user-groups for Brink App re-login. Within the timeout duration, Brink App with automatically login without any user intervention upon endpoint reboot/restart, power-on, sleep/wake-up, hibernate and network changes. This feature allows users to have a very seamless user experience at the same time, ensuring that user identity is verified at regular intervals as defined by the corporate security policies.

Configuration

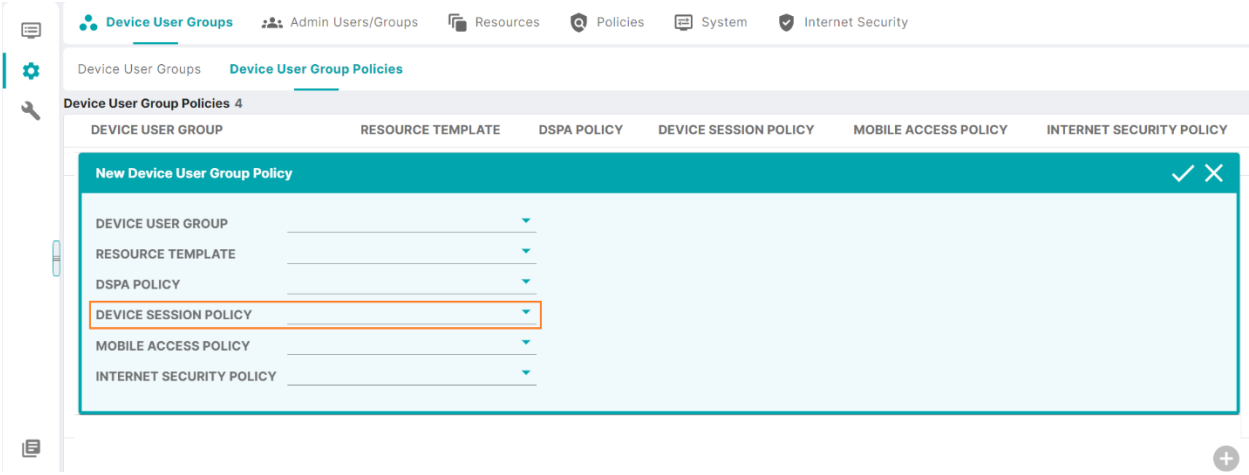
Step-1: AutoLogin timeout has to be set in “hours” in the Device Session Profile config entity.



Notes:

- If auto-login timeout is not set for a device-user-group, the default value set at ORG level will be used. Default value is 24-hours.
- If auto-login timeout is set to 0 (zero), Brink App will automatically login without any user interactive forever, until the user explicitly logs out of the Brink App.
- Any other value defined for auto-login timeout in hours, Brink App will continue automatic re-login until the timeout period and then, prompt the user for re-login.
- Auto-login feature is supported on all desktop and mobile platforms – Windows, Mac, Ubuntu, iOS, Android and Chromebook

Step-2: After creating the device-session-profile and device-session-policy, the policy must be associated for device-user-groups for the auto-login to take effect.

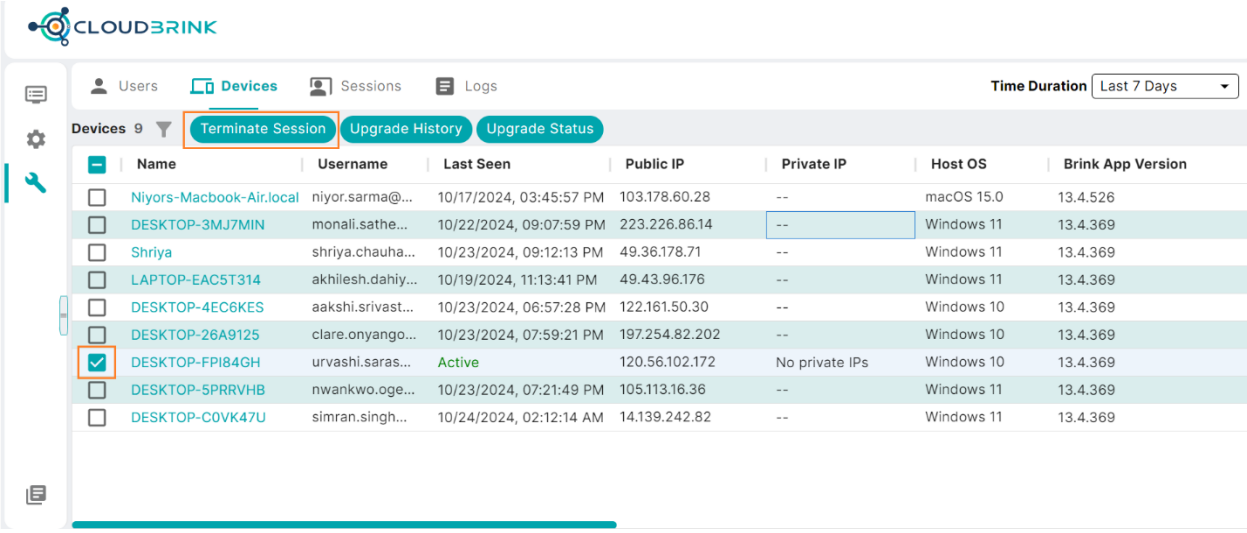


4.9. Brink App Session Termination

Security or Infosec teams in customer organizations need ability to terminate an existing “Active” session when there is any unwanted or concerned activity from the specific user or specific device.

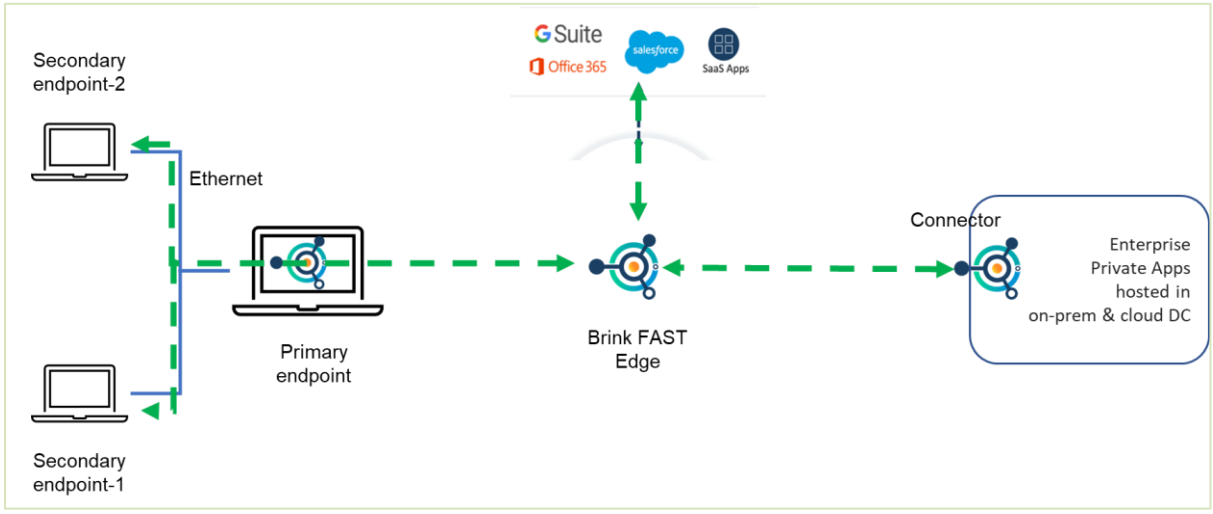
Admins can terminate an active session from the Cloudbrink management portal. Only “Active” sessions can be terminated using this capability.

Troubleshoot → Devices → Terminate Session



5. Bridge-mode feature

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



Bridge-mode feature must be enabled by the sys-admin at each device-user-group level before the users can use the option to connect secondary endpoints. Some important points related to the bridge-mode feature are given below.

a. Bridge-mode feature is supported on Windows platforms only. Primary endpoint must be a Windows 10/11 OS.

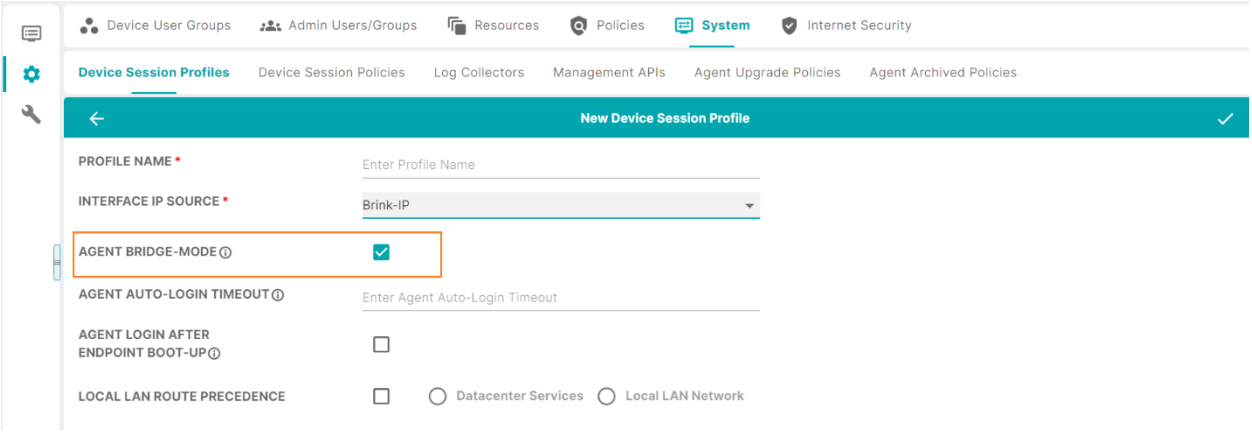
b. Secondary endpoints can be any OS (Windows, Linux or Mac)
c. If secondary endpoint is connected to the primary endpoint using a L2/L3 switch, some features such as physical interface flap on secondary endpoint are not detected on the primary endpoint (Brink App)
d. Users must carefully select the physical interface of primary endpoint to which secondary endpoints are connected, to create “bridge”
e. Users must not use WAN interface (internet providing interface) to be used in the bridge-mode
f. After setting up bridge-mode on Brink App on the primary endpoint and plugging in secondary endpoint to the primary, ensure that on secondary endpoint the interface is flapped (DOWN/UP) so that secondary endpoint generates DHCP request
g. It is recommended that setup the “Bridge” on the primary device first and then, connect the secondary endpoint to that interface
h. It is recommended to disable Windows “ICS” feature on both primary and secondary devices before using Cloudbrink Bridge-Mode feature

Given below are the steps that sys-admin and end-users must follow to use the bridge-mode feature.

Configuration

Step-1: Create device-session-policy to enable bridge-mode setting

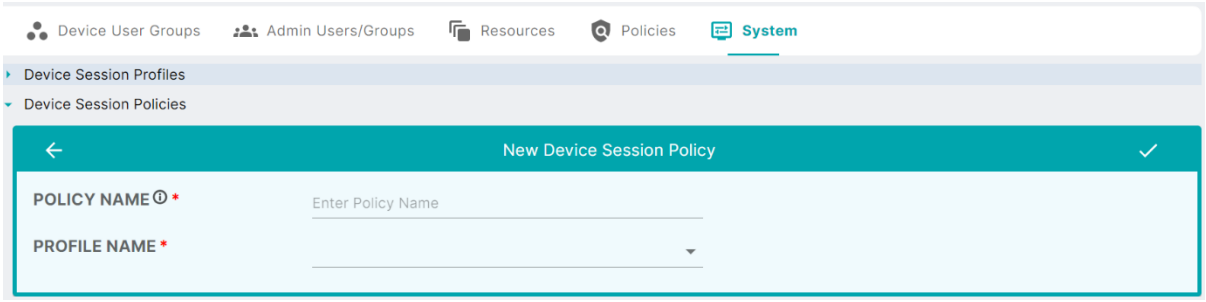
i. Navigate to Configure → System → Device Session Profiles and add a new profile
ii. In the window to add a new profile, provide a profile-name, select the Connector that will assign enterprise private IP to the primary and secondary endpoints, and enable the bridge-mode



Note: 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.

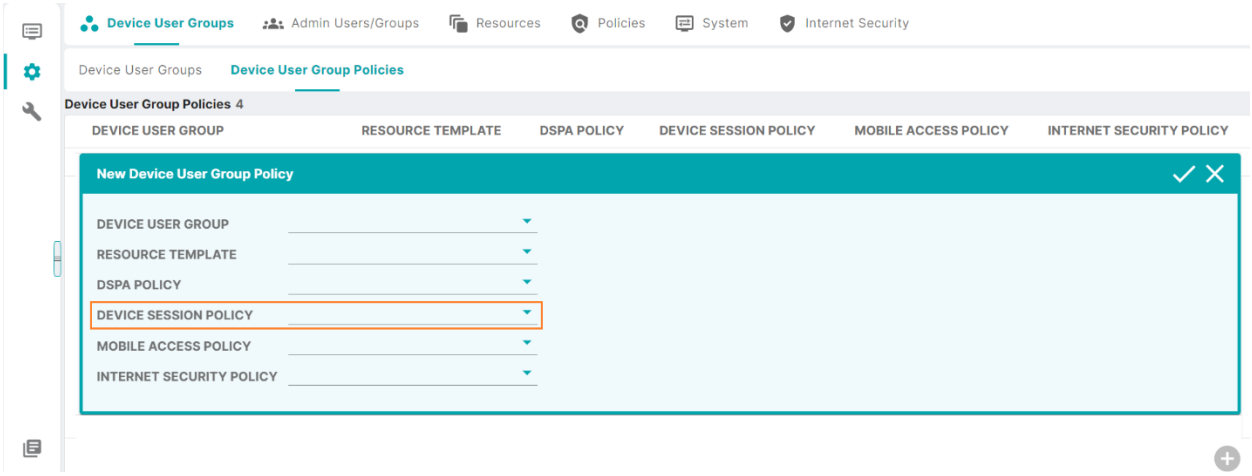
Step-2: Configure Device Session Policy

i. Navigate to Admin portal → Configure → System → Device Session Policies and add a new policy
ii. In the window to add a new policy, provide a name for the session-policy and select the profile created in the previous step from the drop-down



Step-3: Assign the Device Session Policy to the Device User Group

i. Navigate to Admin portal → Configure → Device User Groups → Device User Group Policies, and select the device-user-group to which the device session policy must be assigned
ii. In the window for assigning policies, select the device session policy created in the previous step for “DEVICE SESSION POLICY” field

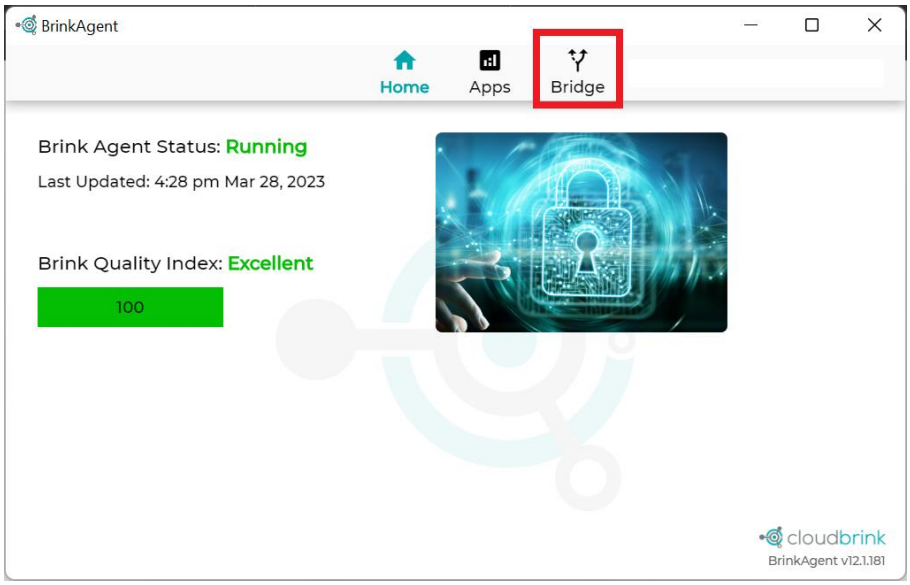


This completes the configuration from the sys-admin side. Once the bridge-mode is enabled for a device-user-group, users belonging to that security group will see new option “Bridge” on the Brink App.

Configuration on end-user side:

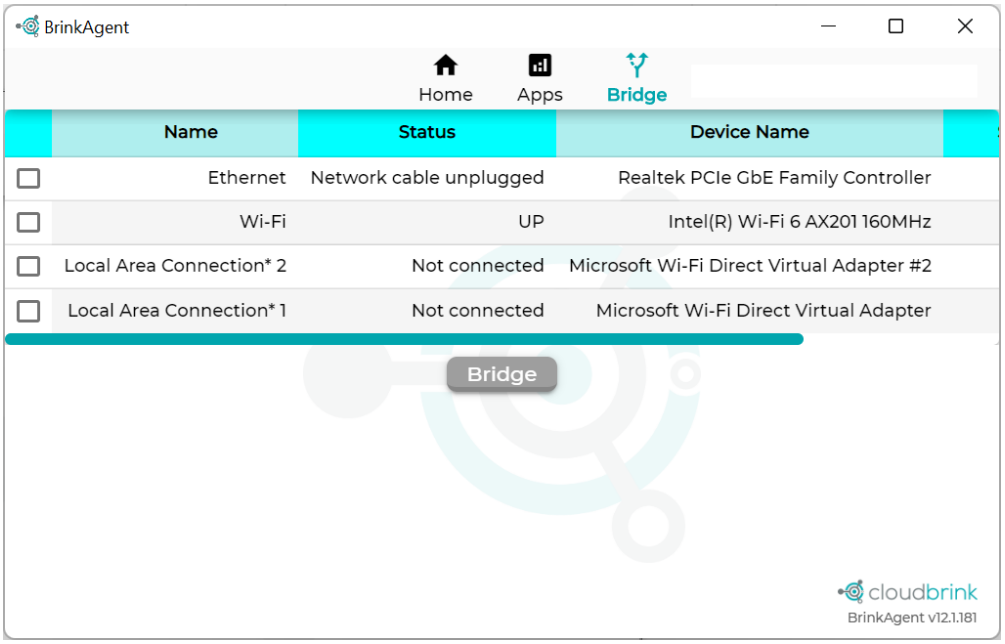
Step-4: User adds interfaces to “Bridge”

End-user will see a new tab on the Brink App called “Bridge” once bridge-mode is enabled.



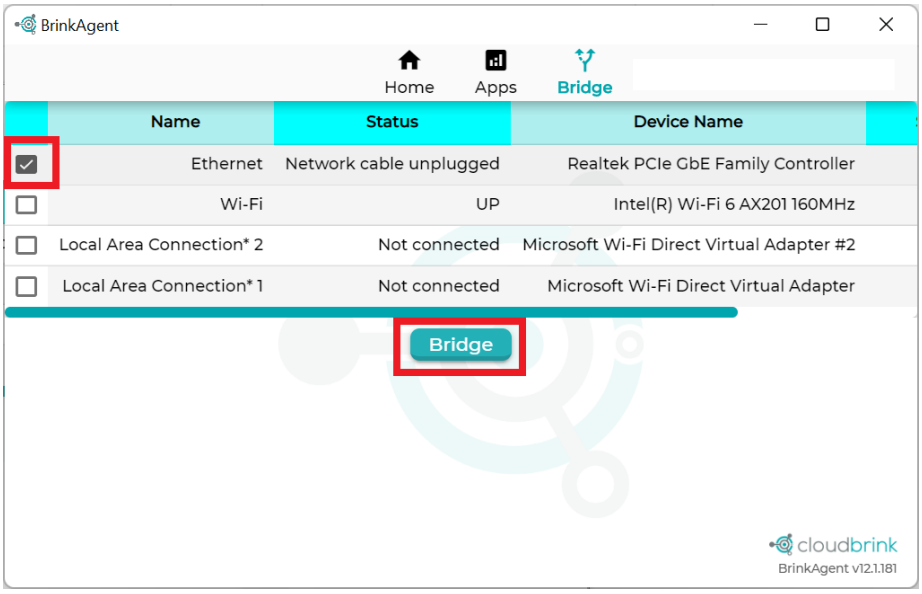
Step-5: Bridge tab on Brink App

User can navigate to the “Bridge” tab and see all available interfaces on this primary endpoint.



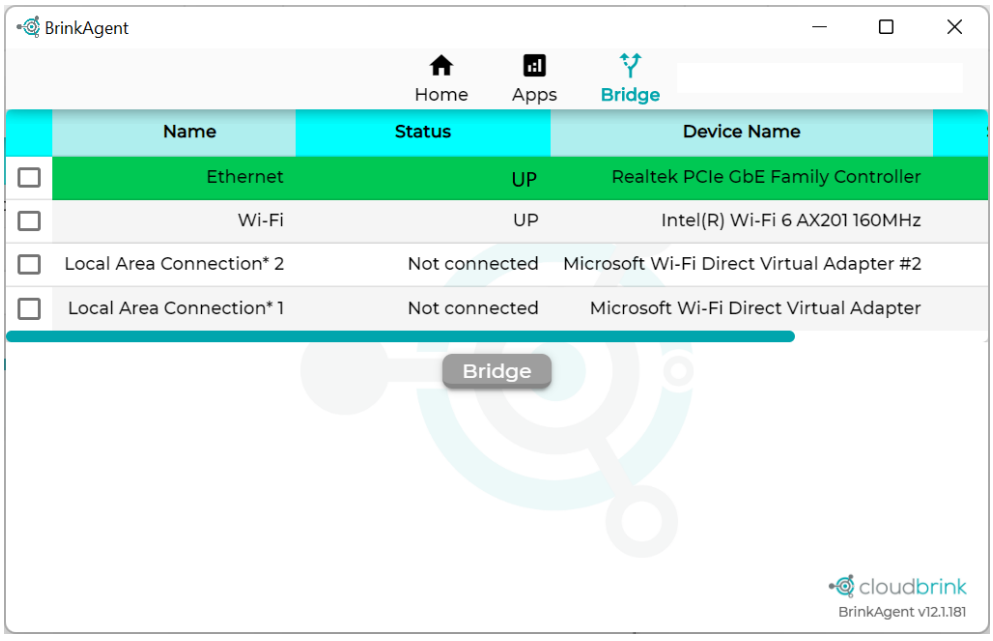
Step-6: Adding interfaces to Bridge

User must select the interface to which secondary device has been connected and click on “Bridge” button



Step-7: Connect secondary endpoints

Once interface is successfully added to the “Bridge”, user can connect the secondary endpoint to this interface and start accessing enterprise apps from the secondary endpoint as well.



6. Log Retrieve API

Cloudbrink provides customers with centralized visibility and management control. Customers can define all their policies from a single cloud-based management console. Similarly, customers can view all the data about their users, endpoints and apps from the single console even though users are accessing all types of apps – SaaS, public/private cloud hosted apps and on-prem datacentre hosted apps.

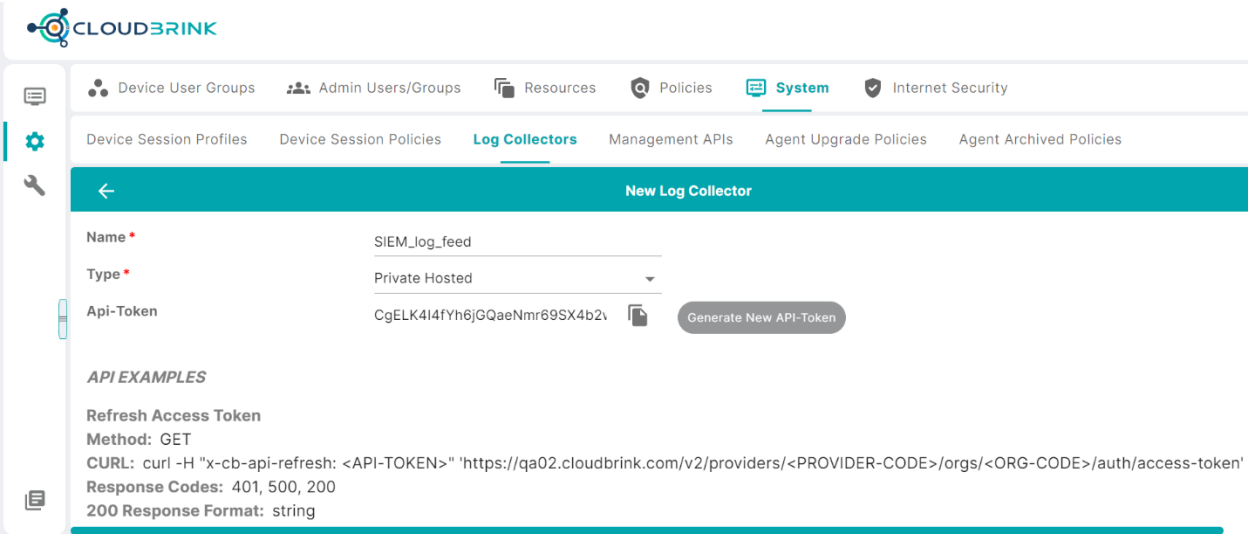
Cloudbrink generates user activity related log messages that are available on the centralized visibility console. Some customers have requirement to retrieve these logs and store in their local log-storage infrastructure for reasons such as log retention policies of the organisation or industry, further analysis by their centralized analytics infrastructure, etc.

Cloudbrink now provides a secure way of retrieving the log messages seen on the visibility portal to the customers' local storage system using a API client script. Customer must use a script as API client to authenticate and then, retrieve the log-messages at regular intervals.

Configuration

Step-1: Create a API-client entity from management console

i. Navigate to Configure → System → Log Collectors → New Log Collector
ii. Add a new Log Collector by providing a name to the log collector entity, TYPE will be set to "Private Hosted" by default, and generate new api-token



Step-2: Create client script to call the Log-retrieve API using the above token

Customer can use any scripting language that can call RESTful APIs by using the above the token. Below is the sample HTTP request-response to use the API client.

1) Get access-token from API-token

```
curl --request GET \
  --url 'https://wren.cloudbrink.com/v2/providers/clb/orgs/{customer-ORG-code}/auth/access-token?valid_mins=60' \
  --header 'Content-Type: application/json' \
  --header 'x-cb-api-refresh:
BQE6qfEUr9/ltgy7jxv3ZckieNHmVxD8dBqnjU3D2rRSOMI0iEKhlFO9pKf3pJxWjPAwbT2Ec5785eyz4Ygf2WtJd5S8h7
64tHT4TUOwcQN7qIK4jTxeT5MM3lBdg4acqt+i2A8uUvWSEpp90M4KVCM+l7ck4NQDvp2mqqRptk1//z6bCU321itB8Vvq
J9LISsSQSLvkO9T7tVY4Si1h4rtY7gM7kQ76ztPiGpTy9ci82Uy9X8E/U9k1LVzHJmjB4Yv3AcxXf8nbjD67yKJGsK2BDr
1q9bjYSI9uog=='
```

The response to above request contains the access-token in the response body

```
"BgGm/dWRFAfv43iPUfJGzaH8QhtLAFR9SKPbe32qGvtXKS1doDkyWVr3uUCVxEBfafprfO44v5kYhBZjaPYWs2JEvOICC
8KKeLgbX/upMy9psvvwFb2PdNkwl5yB9qhQ3sjJseam1bW0fDpifMd8jpOrf4/TPKZLKkY9u/m7rvI5ejR4Icw+KEsO72h
oV7TBBsPXAI1qDeU7rp8NgwunECxfSzCtc9vzmGVYV1gHxaKajRHDvVcBwwsQDF1yTOm2HWyAvuES69/FzTEZYHLpBH17A
R3jkxsjuKJJk1HYI6XdLSPn1YdBy4A/1uInRQeYwCIaJilYrAa06TwfguZYOQ9SBx4gCZho+vosHlBoDJVDFzlwzexcjMf
al1f+NTRkPvxPOZh8hTilxm1Z0oFnOyKV5tkk105AzFUVKKqT5NZiFxkumCS6sPGrb9+X5ivZzBNtBgpsmvNNEmlmX7hFr
4PYvVqfo+Br/u1wQOKXuFs+DoZdUQRjVkEf0mzcZgsR0XA3SzoPSyajCOy6RMc="
```

2) Retrieve log data using above access-token.

```
curl --request GET \
  --url 'https://wren.cloudbrink.com/apis/siem-proxy/v1.0/providers/CLB/orgs/{customer-ORG-code}/logs?cont_token=640bdb3a70e11bda24c8c95e&limit=1000' \
  --header 'Authorization:
BgGm/dWRFAfv43iPUfJGzaH8QhtLAFR9SKPbe32qGvtXKS1doDkyWVr3uUCVxEBfafprfO44v5kYhBZjaPYWs2JEvOICC8
KKeLgbX/upMy9psvvwFb2PdNkwl5yB9qhQ3sjJseam1bW0fDpifMd8jpOrf4/TPKZLKkY9u/m7rvI5ejR4Icw+KEsO72ho
V7TBBsPXAI1qDeU7rp8NgwunECxfSzCtc9vzmGVYV1gHxaKajRHDvVcBwwsQDF1yTOm2HWyAvuES69/FzTEZYHLpBH17AR
3jkxsjuKJJk1HYI6XdLSPn1YdBy4A/1uInRQeYwCIaJilYrAa06TwfguZYOQ9SBx4gCZho+vosHlBoDJVDFzlwzexcjMfa
l1f+NTRkPvxPOZh8hTilxm1Z0oFnOyKV5tkk105AzFUVKKqT5NZiFxkumCS6sPGrb9+X5ivZzBNtBgpsmvNNEmlmX7hFr4
PYvVqfo+Br/u1wQOKXuFs+DoZdUQRjVkEf0mzcZgsR0XA3SzoPSyajCOy6RMc=' \
  --header 'accept: application/json'
```

Response body to above request is the log data from Cloudbrink

```
[
        {
                "log_level": "AUDIT",
                "message": "Access Token validation successful",
                "message_timestamp": "2023-03-11T01:37:11.129Z"
```

```
        },
        {
                "log_level": "AUDIT",
                "message": "Access Token validation successful",
                "message_timestamp": "2023-03-11T01:37:36.361Z"
        }
]
```


3) When access-token expires, API-token can be used as per step-1 and get the new access-token. Repeat steps 1 & 2.

Note: Customers can delete an existing API-token client from the management portal. Once deleted, any existing scripts using the API-client token will stop receiving the responses.

7. Cloudbrink IPSec Peering

Cloudbrink IPSec Peering feature allows customers to connect remote users to their existing IPSec infrastructure which can be a datacenter or branch IPSec gateway, an SD-WAN cloud gateway or branch edge appliance. Customers can deploy Cloudbrink for remote users and take advantage of the application performance and zero-trust security capabilities without any change to their existing networking infrastructure and still provide access to the applications in these networks.

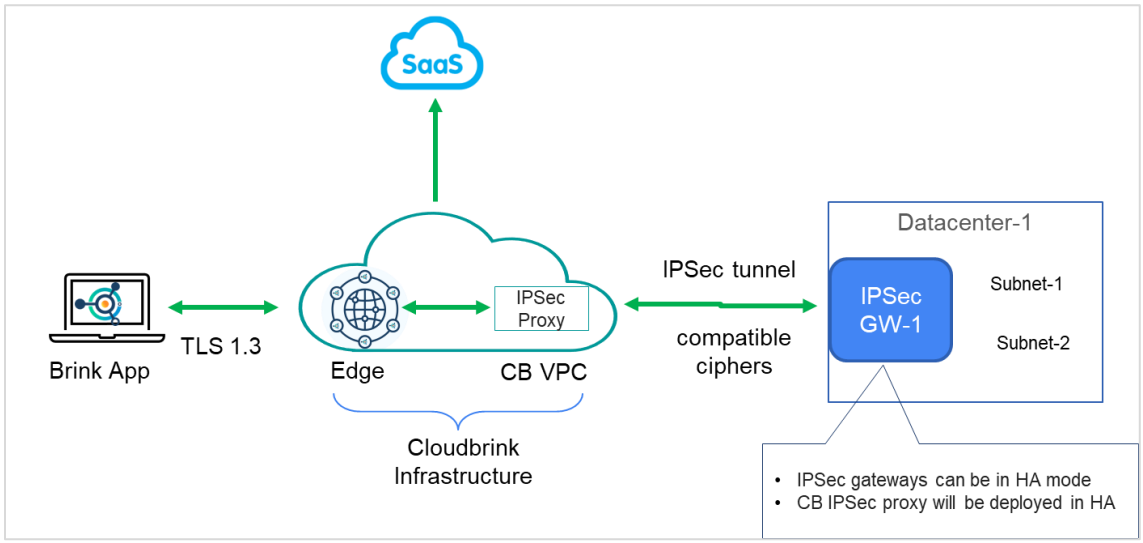
Customers need to provide a high-performance zero-trust access solution to remote users because user productivity is significantly impacted if the applications are responding slowly. Cloudbrink can improve the application performance by overcoming the last-mile networking challenges (eg: unreliable networks in hotel, airport, shared home WiFi) and providing best user experience.

Customers wants to deploy Cloudbrink for remote users but also want to ensure that this deployment is smooth and doesn't require major changes to their existing networking infrastructure inside their on-prem datacenter or branches. With Cloudbrink IPSec Peering feature, customers can terminate their remote user connections via Cloudbrink on to their existing IPSec solution that is already deployed inside their datacenters or branches.

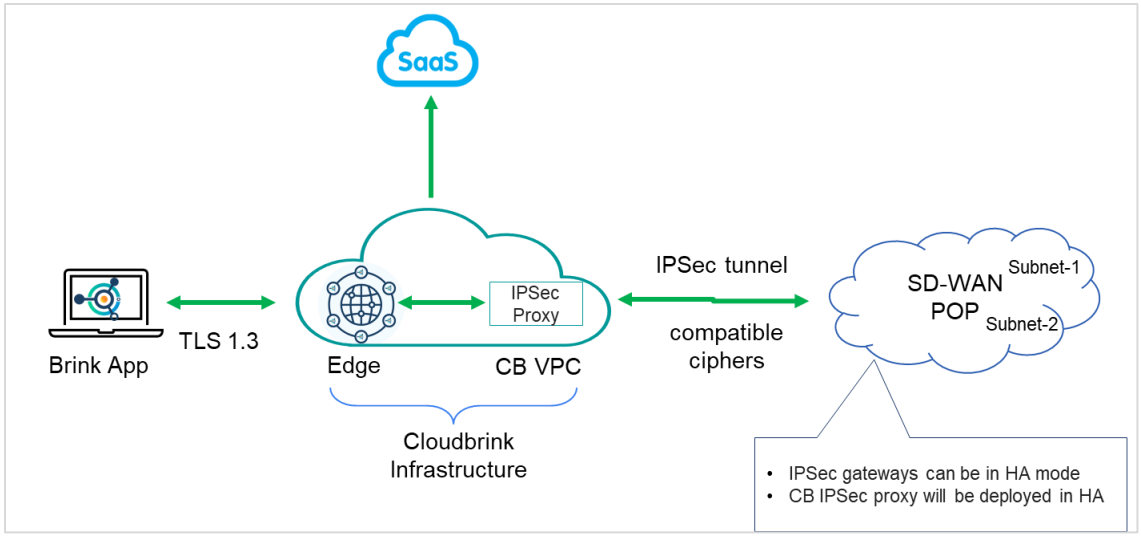
With this feature, customers can benefit from Cloudbrink application performance improvements, zero-trust security for remote users and with no changes to their existing networking infrastructure.

Sample topologies for IPSec Peering deployments

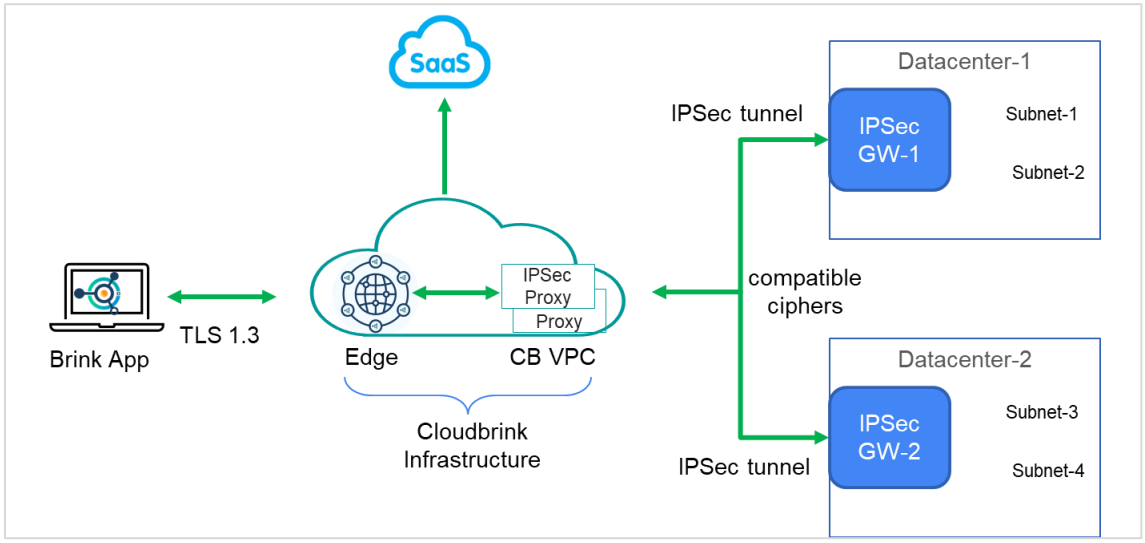
Sample topology-1



Sample topology-2



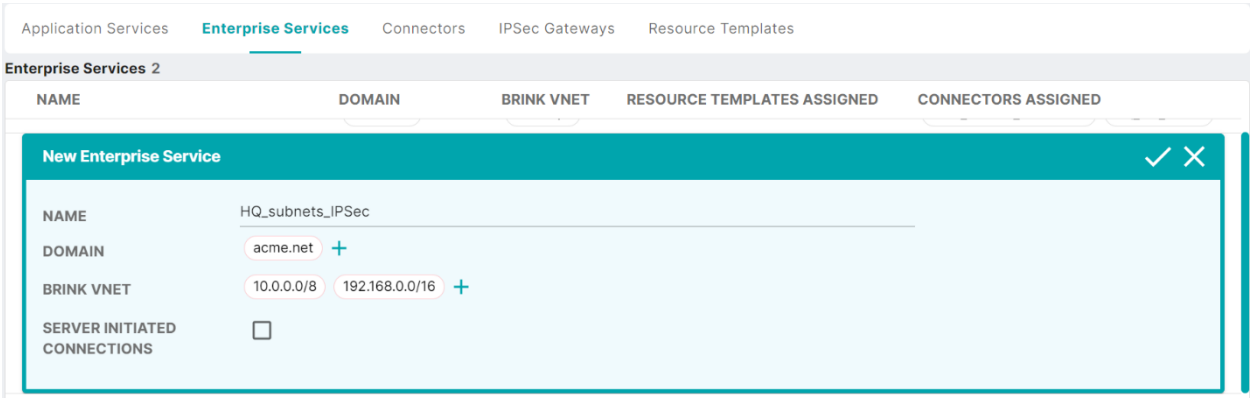
Sample topology-3



Configuration

Step-1: Configure the enterprise-services that represent the networks behind the IPSec Gateway(s) that users need access to.

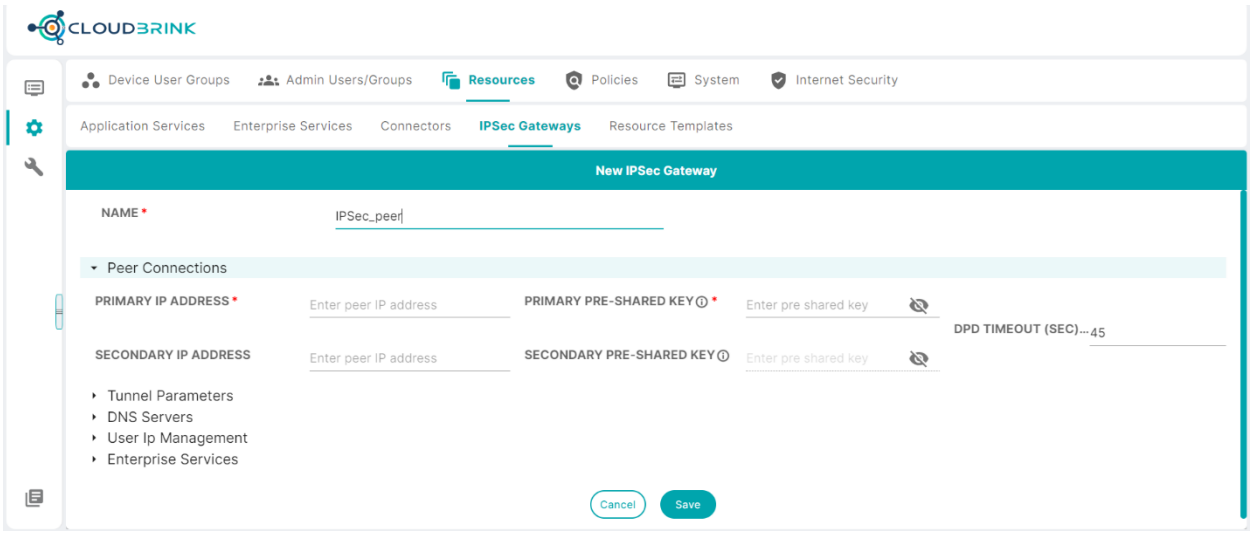
Configure → Resources → Enterprise-Services



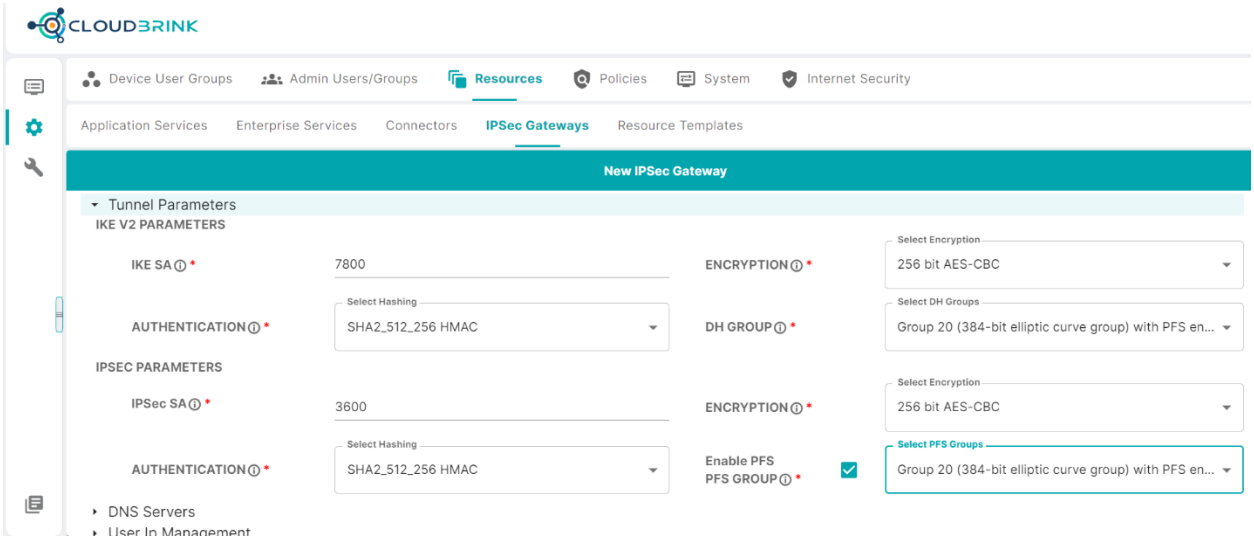
Step-2: Create a new IPSec Gateway by providing the peer IPSec gateway public IP address(es), primary/secondary details, cipher suites to be used for IKE and IPSec, DNS and enterprise-services info (created in step-1).

Configure → Resources → IPSec Gateways →

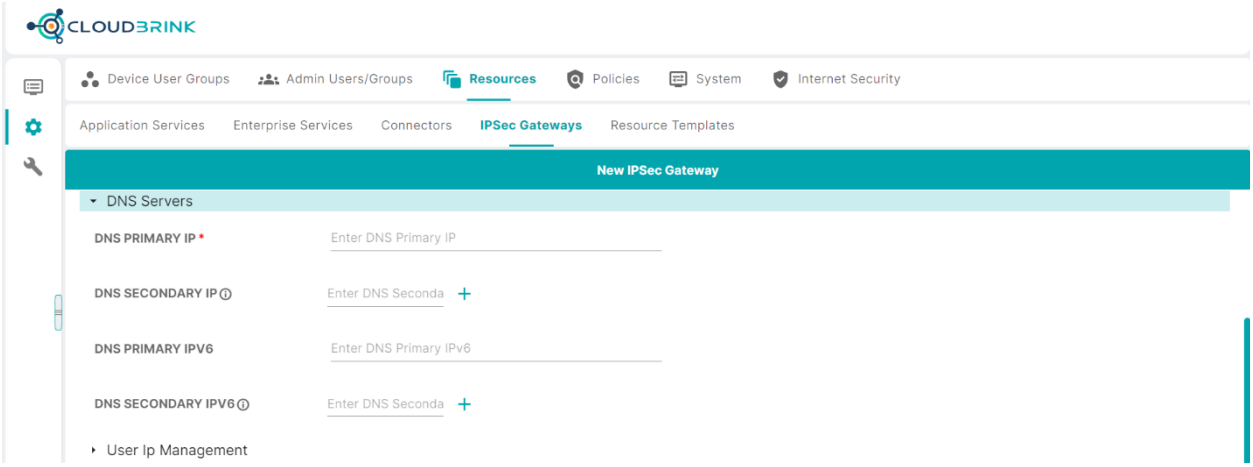
a. Peer Connections



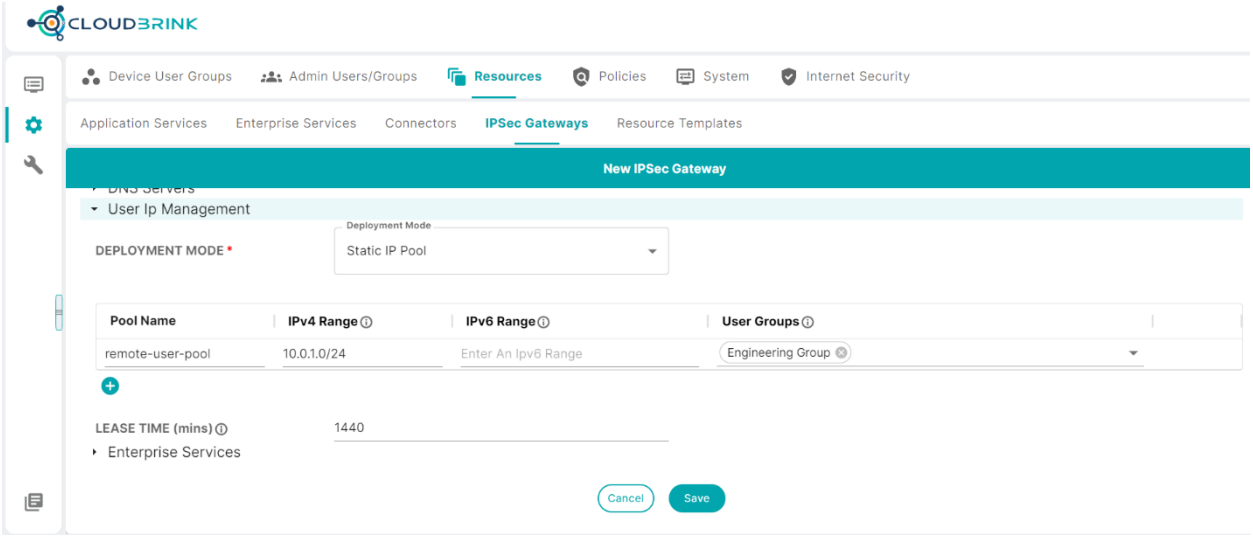
b. Tunnel Parameters



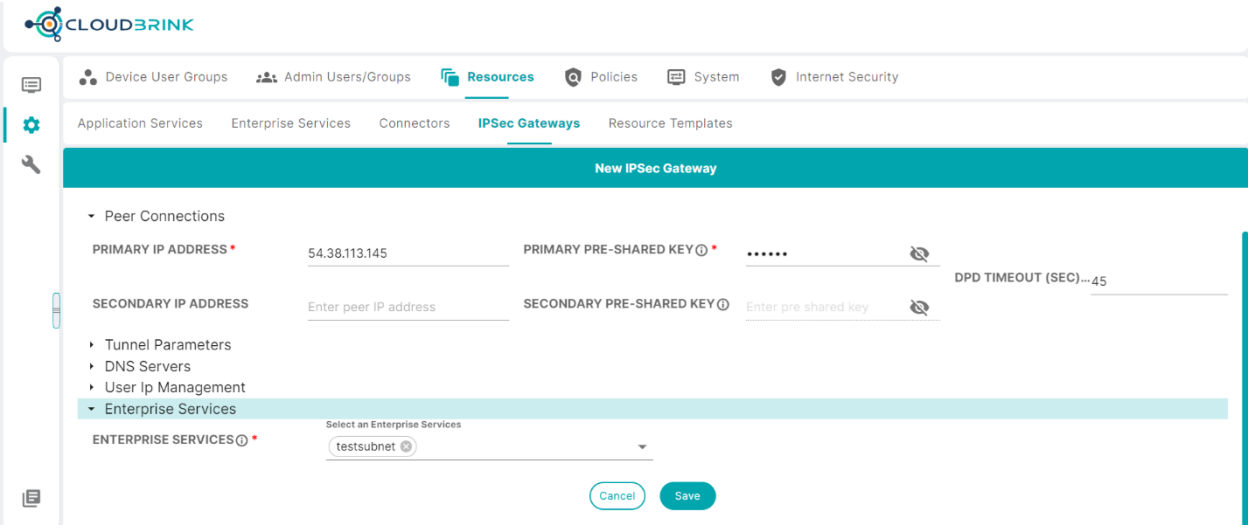
c. DNS server



d. User IP Management

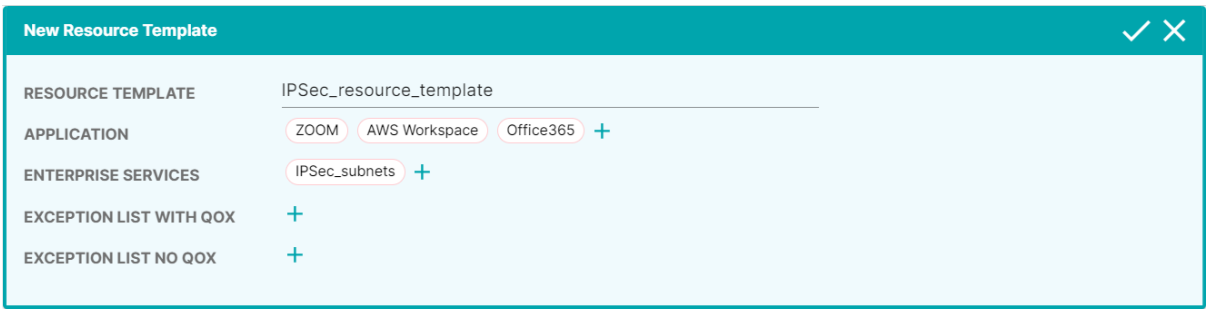


e. Enterprise-services



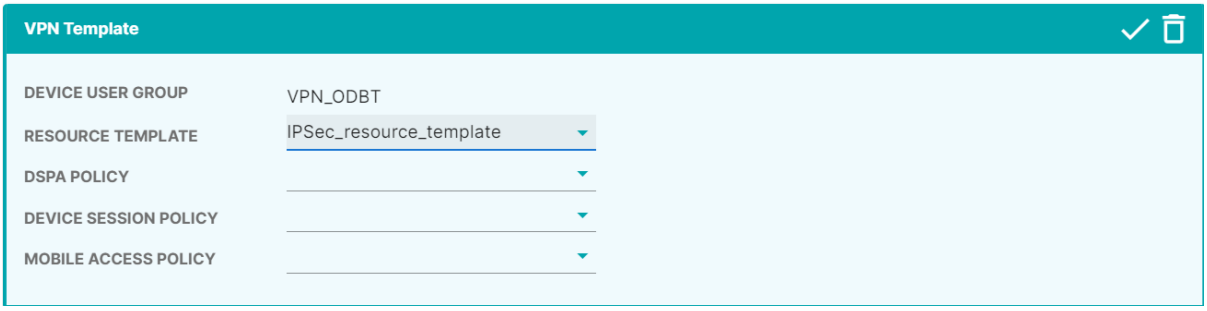
Step-3: Create a new resource-template with the set of applications (application-services and enterprise-services) that will be enabled to remote users.

Configure → Resources → Resource Templates



Step-4: Assign the resource-template to the appropriate device-user-groups.

Configure → Device User Groups → Device User Group Policies



Step-5: At this stage, customer must configure the Cloudbrink endpoints on the IPSec Gateways also. Customer needs to contact Cloudbrink Sales team to get the public IP information of the Cloudbrink IPSec endpoints.

IPSec requires configuration on both sides to create the IPSec tunnels.

With above configuration, remote users belong to “VPN_ODBT” device-user-group can access all subnets defined under “IPSec_resource_template” via the IPSec gateways defined under “IPSec_endpoint_DC1”.

8. Cloudbrink Network Firewall as-a-Service

Cloudbrink Network Firewall as-a-Service feature enables customers to implement network level (layer-3/4) firewalling rules for remote workers accessing datacenter apps (private apps) hosted inside a physical on-prem or cloud IaaS VPC network. Similar to a typical enterprise perimeter network firewall that allows only whitelisted traffic, Cloudbrink Network Firewall as-a-Service allows only whitelisted traffic from the remote users.

Cloudbrink Brink App acts like a deny-all firewall by default so, only sysadmin configured traffic is tunnelled through Cloudbrink into the datacenter. With the enhanced Network Firewall as-a-Service feature, sysadmin can configure policies that can define the whitelist apps at Domain-name, IP address, Port and Protocol level details.

Advantages of Cloudbrink Network Firewall as-a-Service

1. **Enforce firewall rules very close to the origin or source of the traffic**: Brink App is installed and running on the users’ endpoint. Brink App enforces the firewall rules defined by the sysadmin on the endpoint, which is the origin or source of the traffic. Enforcing firewall rules very close to the origin prevents the data to even come out of the endpoint and prevents other types of MITM or DDoS type of attacks.
2. **Edge-native service**: Cloudbrink Network Firewall as-a-Service is a cloud-based edge service that is configured and managed from a central cloud administration console.
3. **Consistent policy enforcement**: Since the firewall rules are defined at one place centrally, the policies are enforced consistently irrespective of any number of datacenters or apps that user might be accessing.
4. **User and App awareness**: The big difference between enterprise perimeter network firewall and Cloudbrink Network Firewall as-a-Service is the user and application awareness. In case of Cloudbrink, customer can define the network firewall rules with the context of user and application awareness. Traditional layer-3/4 network firewalls do not have the user and app awareness.

How Cloudbrink Firewall works?

Cloudbrink follows ‘principle of least privilege’ model. So, all destinations are denied by default for every device-user-group. Admin must explicitly whitelist the set of destinations (IP addresses and domain-names) that are allowed for specific device-user-groups.

When the admin configures an enterprise-service config entity for specific destination IP address or domain-name and assigns the enterprise-service to a specific device-user-group by using resource-template, users belong to this device-user-group can access only the specific IP address and domain-name. All other destinations are blocked by default.

IP address config can be a single IP address (/32 subnet) or a subnet of IP addresses (/24 or /16, etc.). Similarly, domain-name can be a specific FQDN or a top-level domain-name.

Port & Protocol based policies

With 13.4 release, admin can now specify more granular whitelist policies that include port(s) or port-range as well as protocol parameters. When the port and protocol parameters are specified, traffic that matches exactly the defined criteria is allowed. Rest of the traffic is blocked by Cloudbrink.

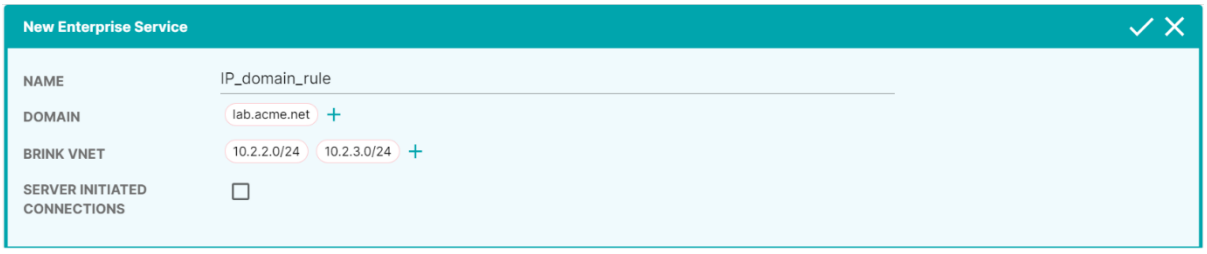
The port and protocol definitions can be done at the IP address level or at the domain-names level. This provides complete flexibility to handle any access control requirements for the user.

If port or protocol parameters are not specified, and only IP address(es) and domain-names are configured, it will be considered as ‘any port’ (wildcard port) and ‘any protocol’ (wildcard protocol).

Configuration

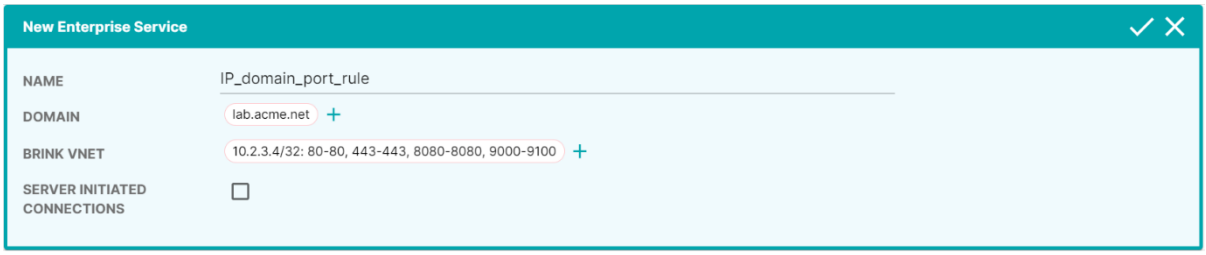
Below are some examples of configuring firewall rules.

i) IP-address and domain-named based rules



With above configuration, users can access all destination IP addresses and to any port and any protocol in the two subnets 10.2.2.0/24 and 10.2.3.0/24.

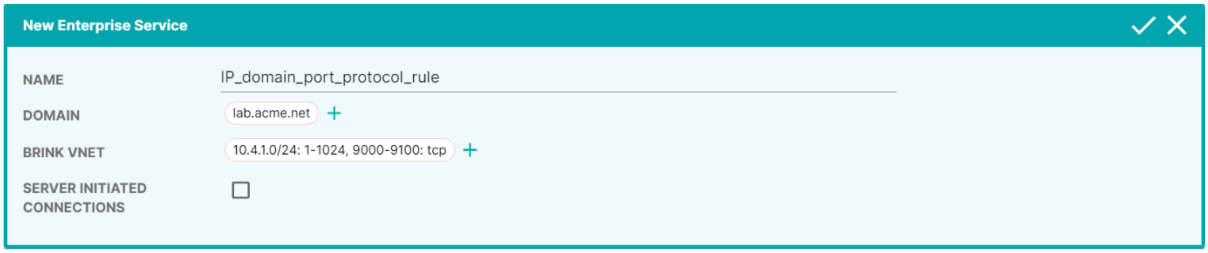
ii) IP, domain and port based rules



With above configuration, users can access only one IP address (10.2.3.4/32) and only specific ports 80,443,8080 and 9000-9100. Protocol can be any (TCP, UDP, etc.)

Note: Traffic to 10.2.3.4 IP but any other port (say port = 5000) will be blocked.

iii) IP, domain, port and protocol based rule



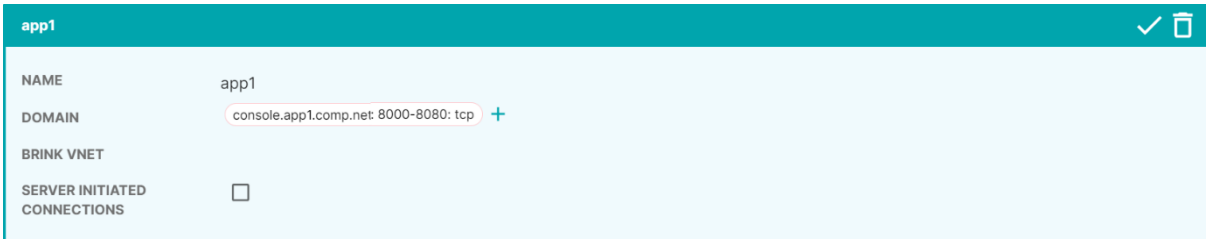
With above configuration, users can access any IP address in the subnet 10.4.1.0/24 but only on port ranges 1-1024 or 9000-9100 and only on TCP protocol.

Note: Any other port or other protocol (say UDP) will be blocked.

Note: Traffic to 10.4.1.100 IP, on port 5000 and protocol TCP will be blocked

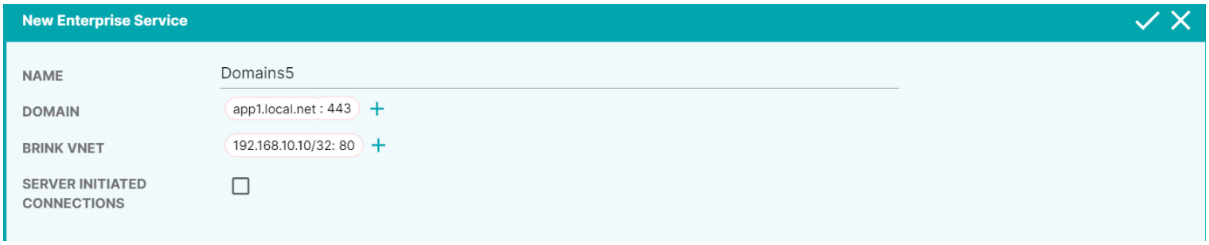
Note: Traffic to 10.4.1.100 IP on port 9000 and protocol UDP will be blocked

iv) Domain-level port protocol rules



With above config, users can access any IP that resolves for DNS name console.app1.comp.net and on TCP port 8000-to-8080

v) Different port/protocol for domain vs IP



With above config, user can access app1.local.net on port 443 (TCP or UDP). Also, user can access one IP address 192.168.10.10 on port 80 (TCP or UDP).
Note: if the domain-name app1.local.net resolves to 192.168.10.10, then user can access both the ports 443 and 80 on TCP or UDP because both the ports.

Best Practices & Guidelines

Customers need to be aware of the below behaviours before using the port and protocol-based policies.

a. Server-initiated connections feature will not consider the port or protocol parameters. The source-IP address of server that is initiating the connection must be within the IP range specified in the enterprise-service.
    1. If the Brink App initiated ping to the server, and if server immediately initiates ping to Brink App, it will fail due to the port based rule.
b. When conflicting policies are configured, below methods are used to resolve the conflict.
    1. If two policies have same IP subnet but port parameter in one policy and protocol parameter in another policy, then port-based policy is evaluated first and then the protocol based policy.
    2. If a port is falling under two ranges in two different policies, the policy with lesser range will be chosen.
    3. If two policies have same port but one policy specifies protocol also, then more granular matched policy (port as well as protocol) will be chosen.
c. To edit an existing port configuration, admin has to delete and re-add the vnet configuration. Editing only port parameter is not allowed.
d. For default route case (0.0.0.0/0), port and protocol parameters are not allowed.
e. DNS port 53 is not allowed to be configured in the port parameter.

9. Internet Security

Cloudbrink offers a high-performance Zero-Trust Security solution to enterprises to safeguard their users and applications from unauthorized access as well as external threats. Cloudbrink secures all types of applications (protocol agnostic) that are hosted anywhere – SaaS, private apps hosted inside physical on-premises or public/private cloud IaaS. While delivering a very strong security stack, Cloudbrink also improves the quality of experience for users over these enterprise applications by using a unique, innovative performance optimization stack. Enterprises benefit from both strong Zero-Trust Security access and improved application performance benefits.

In 14.1 release, Cloudbrink is introducing Internet Security, the world's first high-performance secure web gateway for enterprises and eliminate the trade-off between security vs performance or security vs user

experience. Enterprises can now extend the Cloudbrink security to all Internet applications and not just enterprise applications. With Internet Security feature, users will be able to browser only safe websites and with proper reputational scores.

There are several security attacks resulting from users browsing through an unknown malicious website posing as a legitimate website. Once a user or endpoint is infected, it can spread to the rest of the organizational resources easily. Enterprises can prevent such attacks at the source itself using Internet Security.

9.1 How does Internet Security work?

Administrator can define the Internet Security Profiles config where one can define the action and acceptable reputation level for each of the App-Categories. Cloudbrink provides couple of built-in Internet Security profiles for easy use by the customers. Cloudbrink can categorize the entire Internet domain-names and websites into specific app-category and apply the actions specified by the admin.

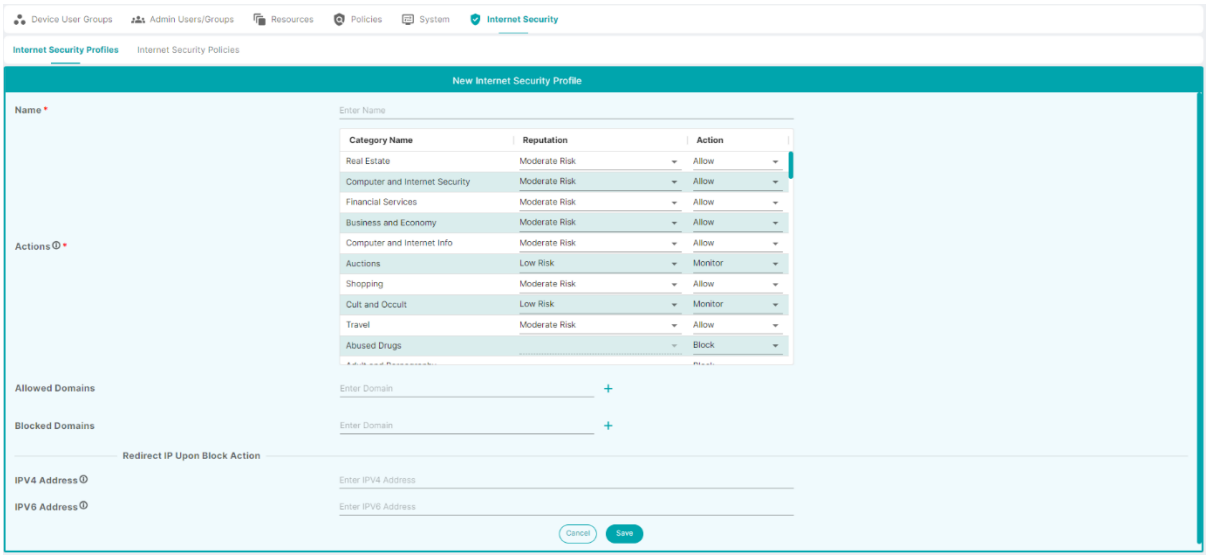
Notes:

a) If the reputation level of a specific website or domain-name is lower than the acceptable level specified by the admin, the website or domain-name will be blocked.
b) When a new profile is created, default action and reputation level for each App-Category will be specified. Admin can modify the action and reputation level as per their corporate infosec policies.
c) Admin can override the actions specified in the profile by configuring the domain-names in the Allowed or Blocked list in each profile.

Once the profiles are defined, admin can configure the Internet Security policies using the profiles already created. These Internet Security policies can be assigned to Device-User-Groups so that users belonging to these groups will be secured using the defined profile settings.
Admin can define the IP addresses (IPv4 and IPv6) to which the user will be redirected to in case of a domain-name or website being blocked due to the admin configured Internet Security policies.

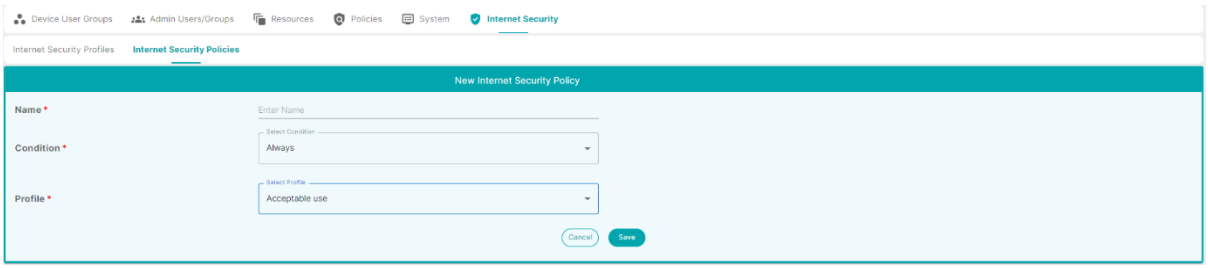
Configuration

Step-1: Configure Internet Security profile
Configure → Internet Security → Internet Security Profiles



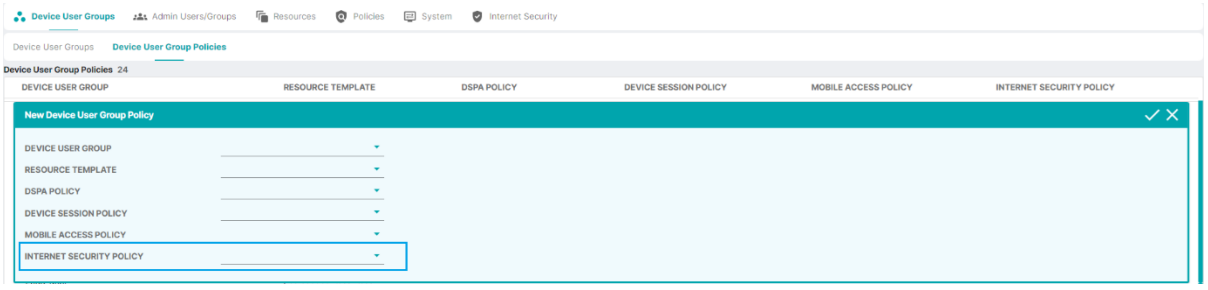
Step-2: Configure Internet Security policy

Configure → Internet Security → Internet Security Policies



Step-3: Assign the Internet Security policy to a Device-User-Group

Configure → Device User Groups → Device User Group Policies



9.2 Device Posture Assessment based Internet Security

Cloudbrink provides some advanced flexibility to customers while applying the Internet Security policies. The Internet Security policy to be applied can be decided based on the results of the Device Posture Assessment (DPA) feature. If the endpoint is in compliant status (DPA is successful), one Internet

Security policy could be applied. If the endpoint is out of compliance (DPA is failure), another Internet Security policy could be applied.

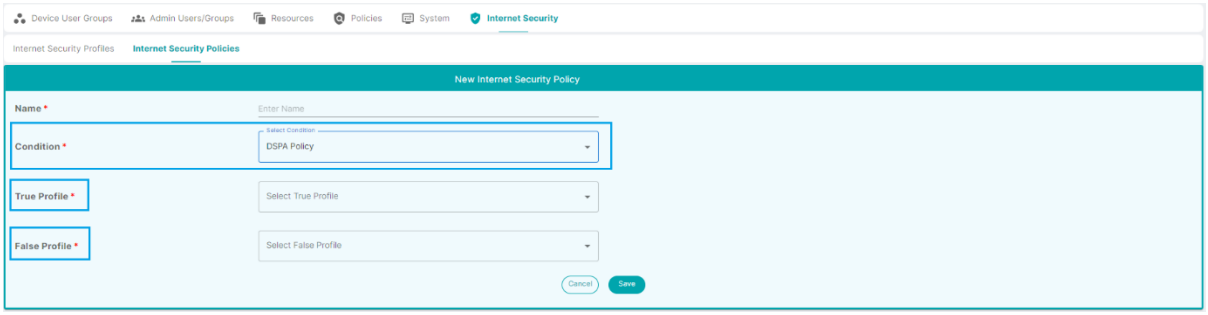
This flexibility gives customers better flexibility to apply appropriate level of strictness based on the endpoint status.

Configuration

When creating the Internet Security policy, admin can select the “Condition” as “DSPA Policy”. This would prompt the admin to select the “True Profile” which is the Internet Security profile that will be applied when DSPA check is successfully and “False Profile” which is the Internet Security profile when DSPA check is failure.

Step-4: Configure Internet Security policy with DSPA condition

Configure → Internet Security → Internet Security Policies



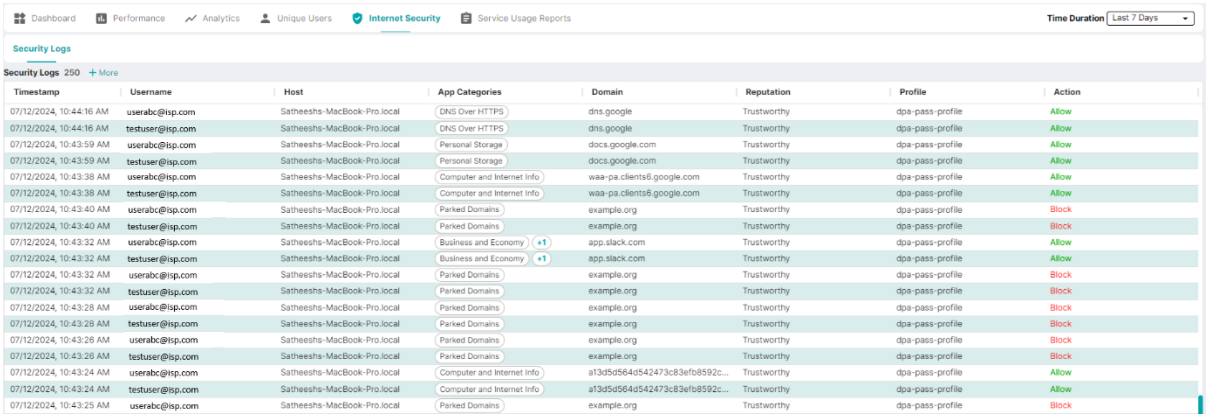
9.3 Visibility

For all configuration changes/updates related to Internet Security, Cloudbrink generates AUDIT type logs that are available under Troubleshoot → Logs section.

For all the actions applied by the Internet Security policies, the detailed actions taken on each domain-name or website and other information is available under Dashboard → Internet Security

Note: By default, a filter is applied on the logs for displaying only Block and Warning Action type of logs. Admin can clear the filter to see all the logs including Allow action type.

Dashboard → Internet Security



Timestamp	Username	Host	App Categories	Domain	Reputation	Profile	Action
07/12/2024, 10:44:16 AM	userabc@isp.com	Satheeshs-MacBook-Pro.local	DNS Over HTTPS	dns.google	Trustworthy	dpa-pass-profile	Allow
07/12/2024, 10:44:16 AM	testuser@isp.com	Satheeshs-MacBook-Pro.local	DNS Over HTTPS	dns.google	Trustworthy	dpa-pass-profile	Allow
07/12/2024, 10:43:59 AM	userabc@isp.com	Satheeshs-MacBook-Pro.local	Personal Storage	docs.google.com	Trustworthy	dpa-pass-profile	Allow
07/12/2024, 10:43:59 AM	testuser@isp.com	Satheeshs-MacBook-Pro.local	Personal Storage	docs.google.com	Trustworthy	dpa-pass-profile	Allow
07/12/2024, 10:43:38 AM	userabc@isp.com	Satheeshs-MacBook-Pro.local	Computer and Internet Info	waa-pa.clients6.google.com	Trustworthy	dpa-pass-profile	Allow
07/12/2024, 10:43:38 AM	testuser@isp.com	Satheeshs-MacBook-Pro.local	Computer and Internet Info	waa-pa.clients6.google.com	Trustworthy	dpa-pass-profile	Allow
07/12/2024, 10:43:40 AM	userabc@isp.com	Satheeshs-MacBook-Pro.local	Parked Domains	example.org	Trustworthy	dpa-pass-profile	Block
07/12/2024, 10:43:40 AM	testuser@isp.com	Satheeshs-MacBook-Pro.local	Parked Domains	example.org	Trustworthy	dpa-pass-profile	Block
07/12/2024, 10:43:32 AM	userabc@isp.com	Satheeshs-MacBook-Pro.local	Business and Economy +1	app.slack.com	Trustworthy	dpa-pass-profile	Allow
07/12/2024, 10:43:32 AM	testuser@isp.com	Satheeshs-MacBook-Pro.local	Business and Economy +1	app.slack.com	Trustworthy	dpa-pass-profile	Allow
07/12/2024, 10:43:32 AM	userabc@isp.com	Satheeshs-MacBook-Pro.local	Parked Domains	example.org	Trustworthy	dpa-pass-profile	Block
07/12/2024, 10:43:32 AM	testuser@isp.com	Satheeshs-MacBook-Pro.local	Parked Domains	example.org	Trustworthy	dpa-pass-profile	Block
07/12/2024, 10:43:28 AM	userabc@isp.com	Satheeshs-MacBook-Pro.local	Parked Domains	example.org	Trustworthy	dpa-pass-profile	Block
07/12/2024, 10:43:28 AM	testuser@isp.com	Satheeshs-MacBook-Pro.local	Parked Domains	example.org	Trustworthy	dpa-pass-profile	Block
07/12/2024, 10:43:26 AM	userabc@isp.com	Satheeshs-MacBook-Pro.local	Parked Domains	example.org	Trustworthy	dpa-pass-profile	Block
07/12/2024, 10:43:26 AM	testuser@isp.com	Satheeshs-MacBook-Pro.local	Parked Domains	example.org	Trustworthy	dpa-pass-profile	Block
07/12/2024, 10:43:24 AM	userabc@isp.com	Satheeshs-MacBook-Pro.local	Computer and Internet Info	a13d5d564d542473c83efb8592c...	Trustworthy	dpa-pass-profile	Allow
07/12/2024, 10:43:24 AM	testuser@isp.com	Satheeshs-MacBook-Pro.local	Computer and Internet Info	a13d5d564d542473c83efb8592c...	Trustworthy	dpa-pass-profile	Allow
07/12/2024, 10:43:25 AM	userabc@isp.com	Satheeshs-MacBook-Pro.local	Parked Domains	example.org	Trustworthy	dpa-pass-profile	Block

9.4 Additional Information

a) Internet Security is supported on all desktop platforms – Windows, Mac and Ubuntu.
b) When a website or domain-name is blocked, and if Redirect IP configuration is set, user will be redirected to the configured IP address.
c) Admin can specify action for “Undefined” app-categories and for those domain-names/websites whose app-category could not be determined.

10. Monitoring

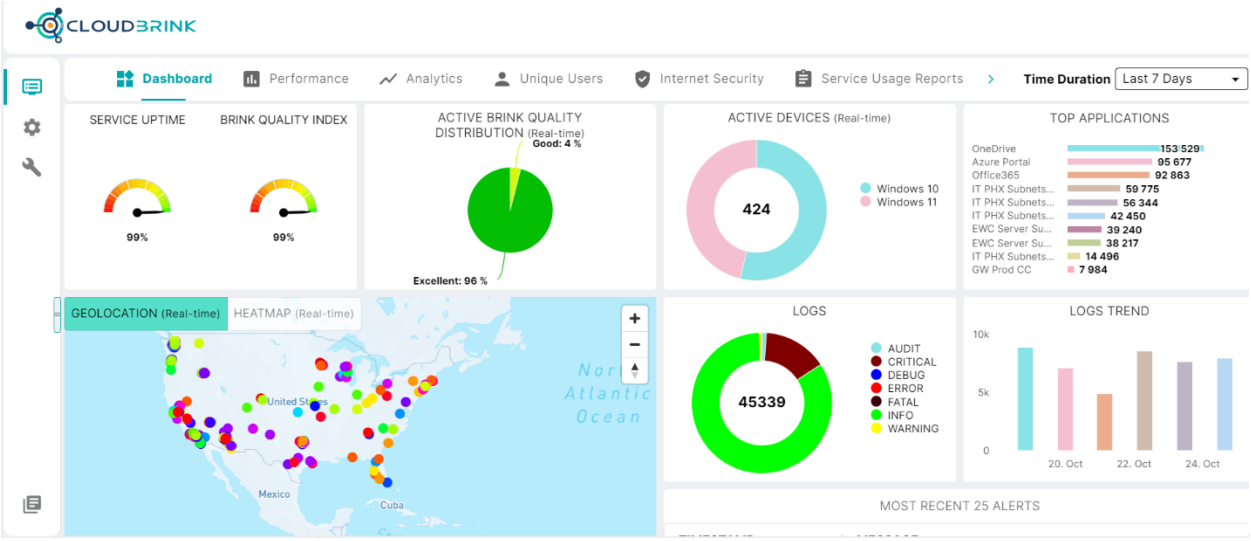
Cloudbrink management portal (https://admin.cloudbrink.com/) provides very rich data about the usage of Cloudbrink by their users for a customer admin. This section describes each element of the Dashboard page on the management portal.

On the management portal, admin can select the time period for which data must be shown on all Dashboard and Troubleshoot pages. Admin can use the simple drop-down at the right-top corner and select the time duration. The maximum duration is last 30-days of data that is available on the management portal.

10.1 Dashboard

Below is the snapshot of the main dashboard. Admin users will land on this page immediately after logging into the management portal.

Dashboard on the management portal



The individual elements on dashboard are explained below.

Service Uptime

Service uptime represents the Cloudbrink service status for the last 7-days period. A 100% service uptime means there was 0sec downtime in the last 7 days.

Cloudbrink provides enterprise-grade uptime SLA of 99.99% uptime (apart from planned maintenance activity) to customers.

Brink Quality Index (BQI)

Brink Quality Index is the quantitative measure of the quality-of-experience (QoX) that Cloudbrink provides to the end-users. Cloudbrink Agent has intelligence to monitor the network conditions for the endpoint. Agent will then determine what level of experience users would receive without Cloudbrink in place and compares it with the experience being delivered with Cloudbrink. Using this information, Brink Quality Index is determined, and represented with value that ranges from 0-to-100, 100 being the best possible QoX with the given endpoint network.

Active Brink Quality Distribution

Active Brink Quality Distribution represents the distribution of users with various levels of QoX being delivered currently. Active means, endpoints which are currently actively using Cloudbrink service.

Active Devices

Active devices are all the endpoints which are currently using Cloudbrink service. Admins can quickly check how many endpoints are actively connected, which endpoints are these, etc.

Top Applications

Top applications section provides the information about the most used applications in the organization by all users put together. This gives valuable information to the admins about which apps are highly used, how they are performing. Admins can use this information to evaluate the application capacity, plan maintenance activities, etc.

Geolocation

Geolocation shows where the endpoints are connecting from. The dashboard uses a geographic map and overlays the endpoint location on the top of it to make is easy and intuitive to check the location.

Logs

Logs section shows how many logs of each level (INFORMATION, ERROR, CRITICAL, AUDIT, etc.) are generated in a simple pie-chart format. Admins can quickly get an understanding of how many issues are being seen on the Cloudbrink service.

Logs Trend

Logs trend shows many logs are being generated in 4-hour intervals for the last 6 times (total of last 24-hour period). This information helps admins to check if there is any spike of events in the last 24-hours, and deep-dive in case such an issue happened.

Most Recent 25 Alerts

Alerts means log messages of level CRITICAL or ERROR. Most recent 25 alerts gives admins a quick view into the last 25-issues of CRITICAL/ERROR level so that they can quickly look into the issue before users complain.

10.2 Performance

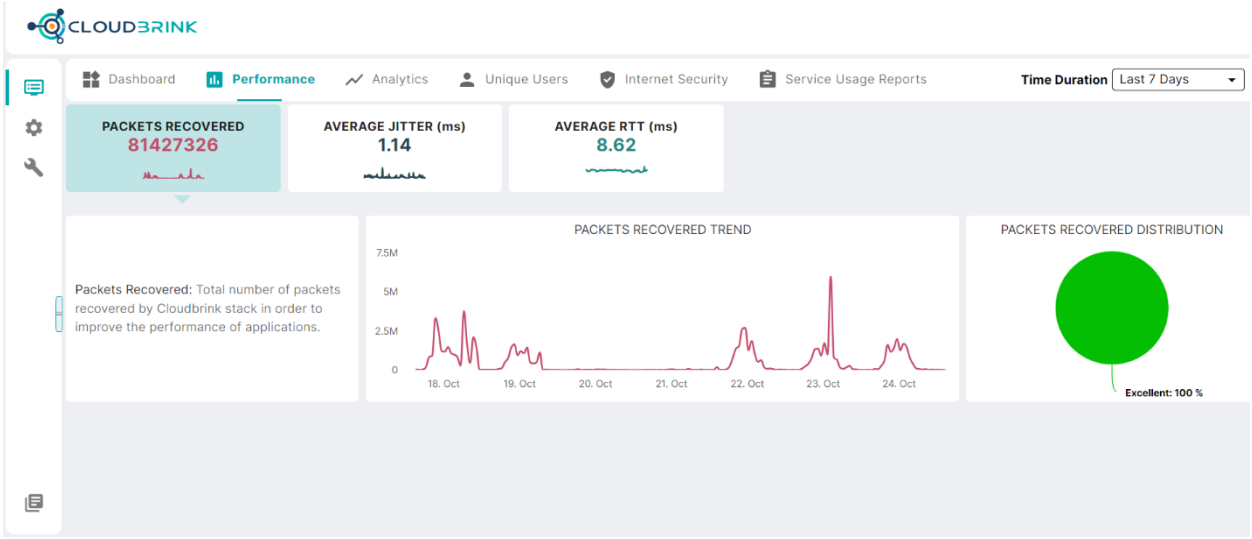
Performance tab provides granular details about how the Cloudbrink is able to provide the QoX. Cloudbrink addresses several network impairments such as packet loss. In the Performance tab, the portal displays how much of packet drops were recovered, average jitter for UCaaS apps, etc.

Packets Recovered

Cloudbrink QOX algorithm is capable of detecting packet loss due to network behavior on the endpoint, and then take mitigation steps so that packet loss is recovered and applications function at their best possible performance. If packet loss is not mitigated, applications using TCP/IP protocol slow down significantly and performance deteriorates making the application unusable by the users.

Packets recovered represents how many packets across all users that would be dropped if Cloudbrink were not used. All this would have resulted in applications being very slow or unusable.

Packets recovered graph



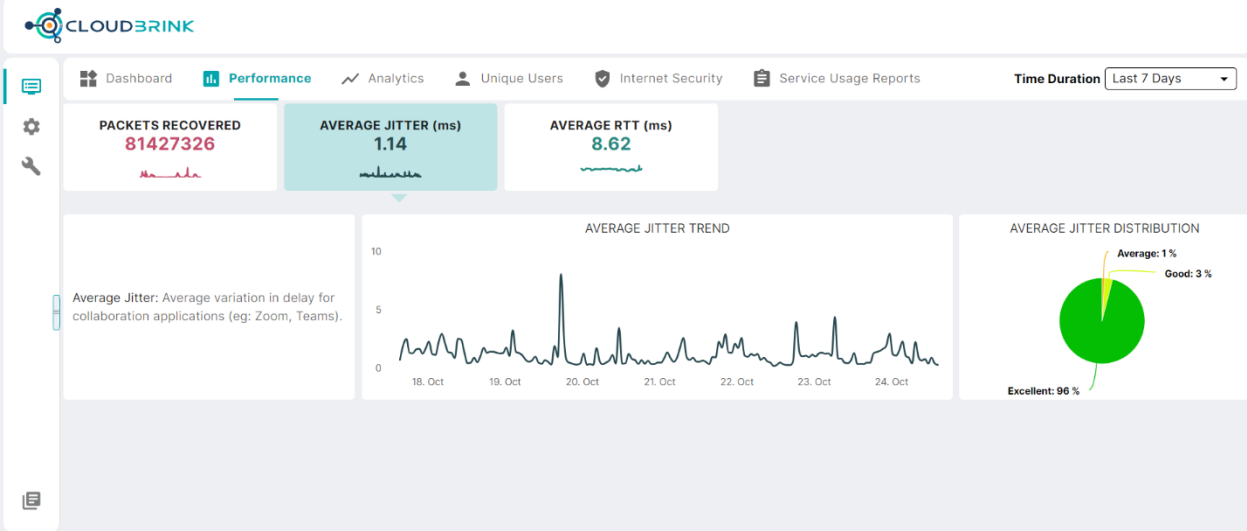
Average Jitter

UCaaS applications such as Zoom, Teams, Webex, Google-Meet, etc. which are heavily used by users today after hybrid-work have become mainstay, are very sensitive to jitter. If the jitter is very high, the audio and video call on the UCaaS apps will become unproductive.

Cloudbrink has the ability to smoothen the jitter and make the UCaaS apps very productive. Audio will not be gibberish or staggered, and video will never blank out.

Average jitter represents the jitter across all users the Cloudbrink is able to deliver. A very low average means all users are receiving very good experience on the UCaaS applications.

Average jitter graph

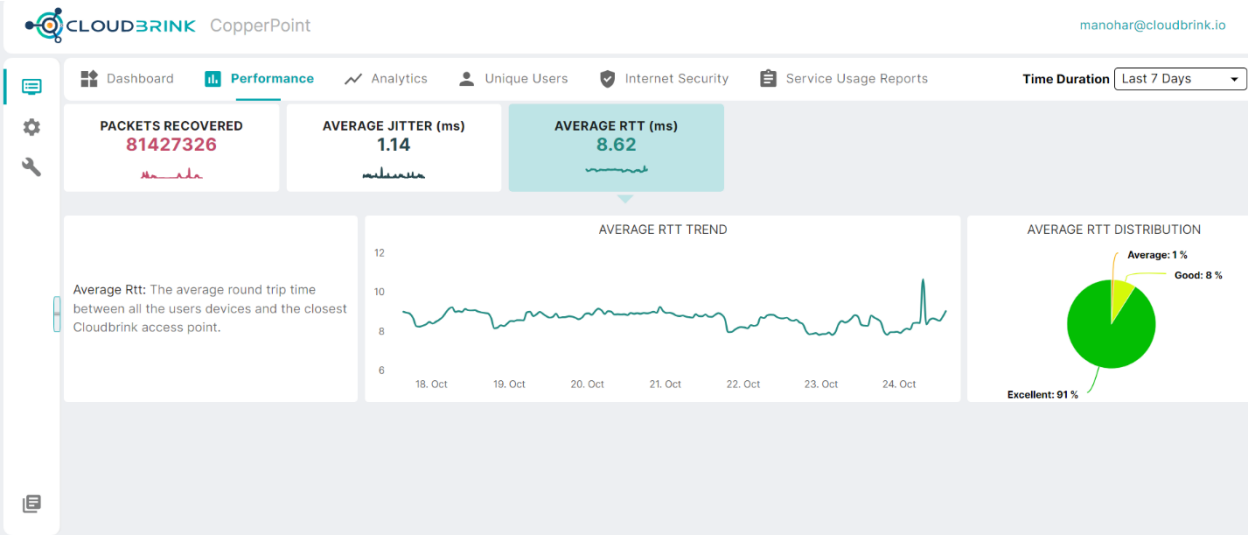


Average RTT

All applications, especially TCP/IP based applications are very sensitive to end-to-end latency. Cloudbrink with its unique Elastic Edge technology provides enterprise access points very close (< 20msec) to all users for the organization. This helps is maintaining high application performance and improve the user QoX.

Average RTT represents the average round-trip time of all Cloudbrink users from their respective Cloudbrink Edge infrastructure. The lower the average RTT, the better the user QoX will be on all their apps.

Average RTT graph



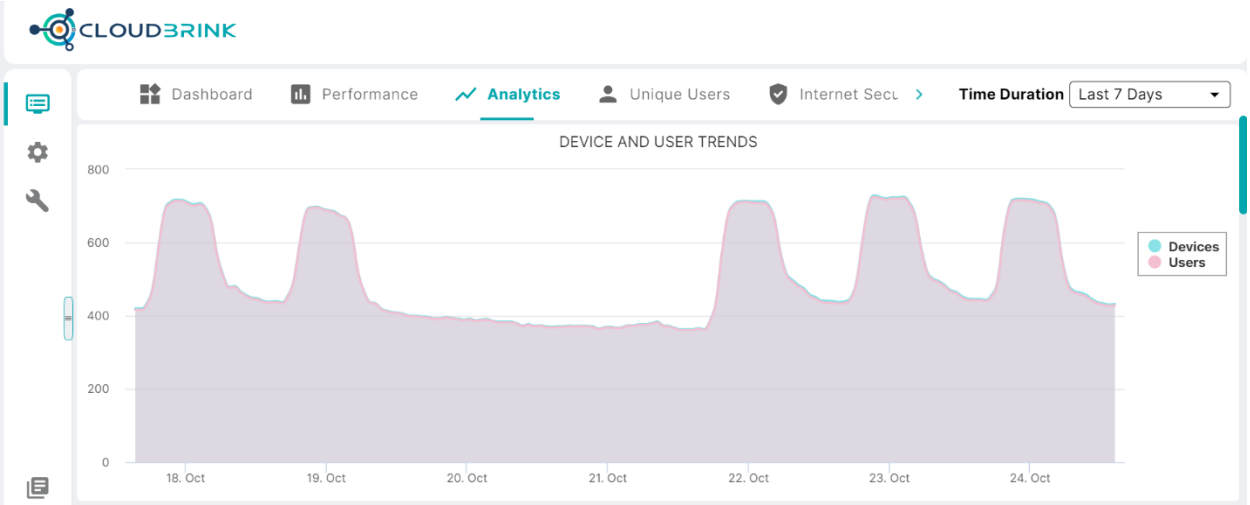
10.3 Analytics

Analytics tab provides granular information about the users and applications being served using Cloudbrink service. Below are the details provided in this tab.

Devices and Users Trends

Trends chart provides the total number of active users and devices/endpoints that were using Cloudbrink service over the period of last 7-days. This helps admins to monitor the usage of their subscription and plan the license capacity accordingly.

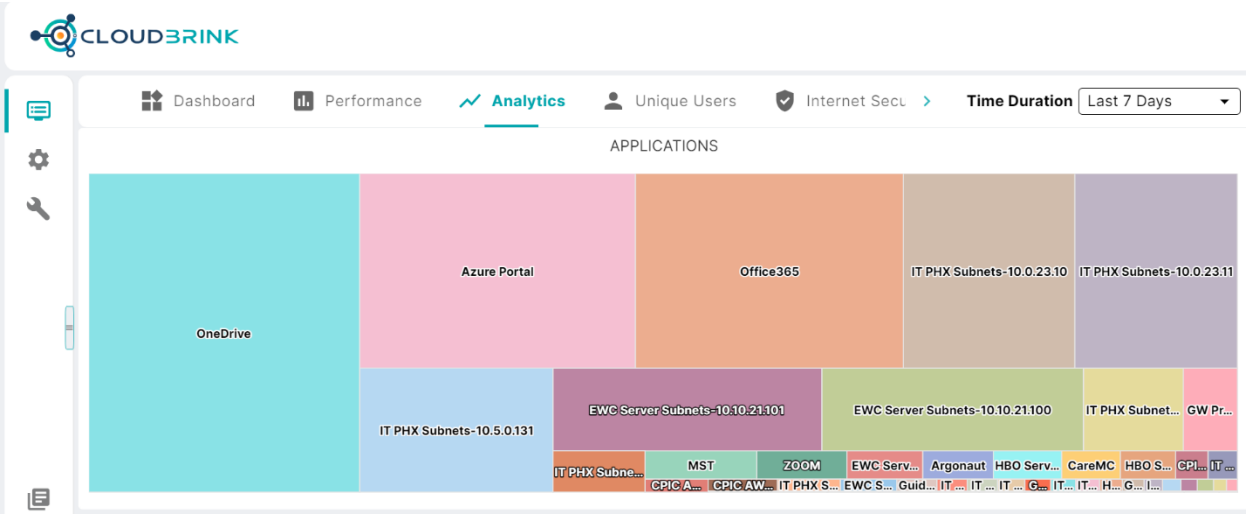
Devices and Users trend graph



Applications

Applications section shows all applications that their users have ever used over Cloudbrink service. This includes top used applications as well as very rarely used application details. This is helpful for admins to quickly understand how many total number of apps are being used by their users.

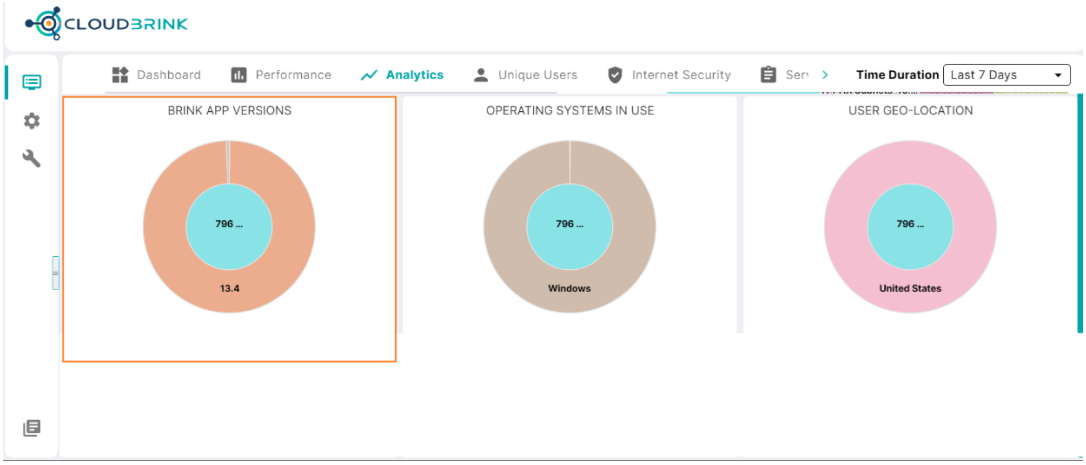
Applications block diagram



Brink App Versions

Customers always prefer to know if all their users are using the latest version of the software. BrinkApp version pie-chart shows all the versions being used by their users. Admins can find out which users are using older version of BrinkApp and ask them to upgrade.

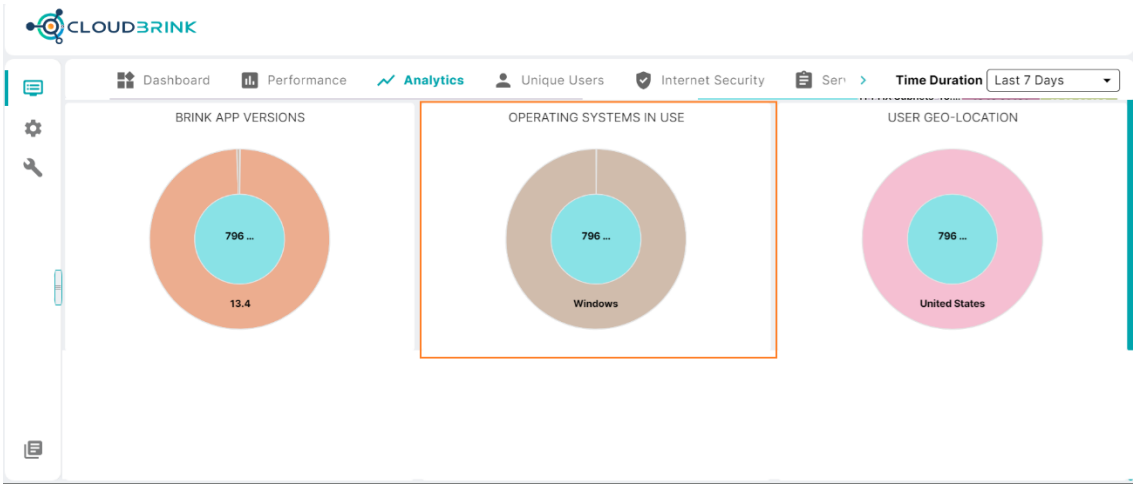
BrinkAgent versions distribution



Operating Systems in Use

Admins can find out the endpoint OSes that their users are using. For each OS category (Windows, Linux, etc.), Cloudbrink provides details of the sub-versions as well when admin clicks on the OS type.

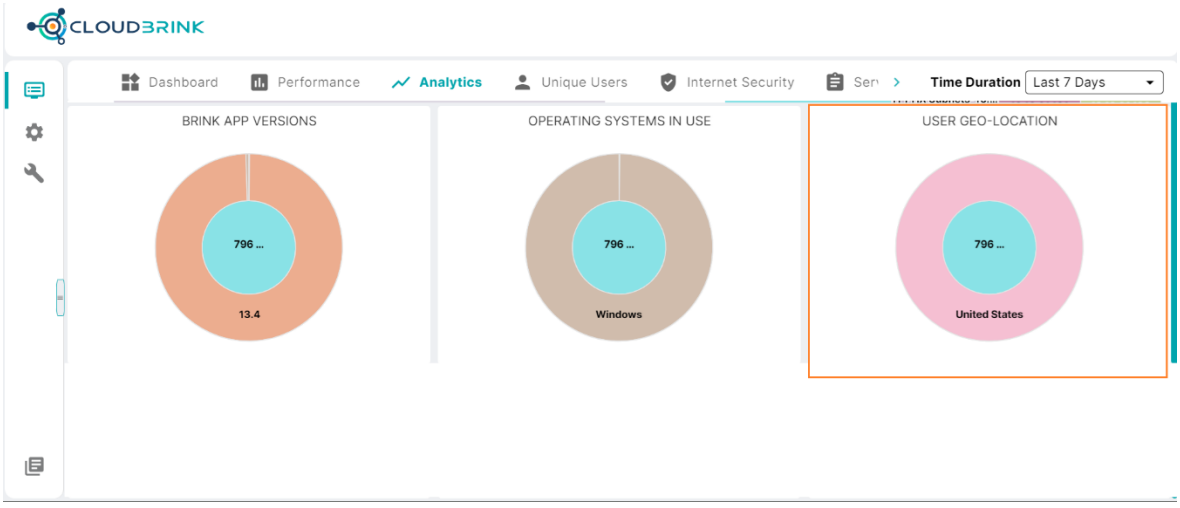
OS on endpoints distribution



User Geolocation

Admins can look into the locations from which users are connecting to Cloudbrink service. Admin can click on each portion of the pie chart and deep dive.

User location distribution

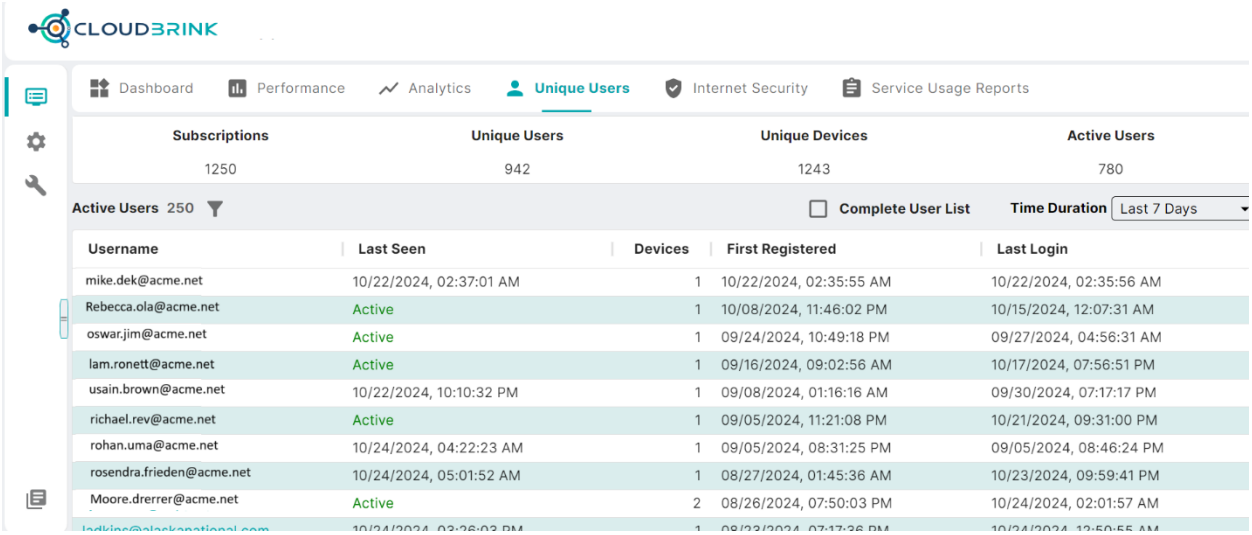


10.4 Unique Users

Unique users tab provides information about all the users that have used Cloudbrink service at least once after the customer has been onboarded. Along with the users, the number of devices that each user is using, when was the first time the user accessed Cloudbrink and when was the last-seen activity from the user will also be provided.

Customers can use this page to determine how many licenses have been consumed. Cloudbrink supports Named-User licensing model where each user, up to 5 devices, consumes only one license.

Unique users details



- **Subscriptions** → Total number of licenses that customer has subscribed for Cloudbrink service
- **Unique Users** → Total number of unique users that have used Cloudbrink service at least once from the start of the contract
- **Unique Devices** → Total number of unique devices where Brink App was installed and connected to Cloudbrink service at least once during the selected time period (From <-> To timestamp)
- **Active Users** → Users who have used Cloudbrink service at least once during the selected time period (From <-> To timestamp)
- **Complete User List** → If this checkbox is enabled, it will show Unique Devices from the start of the contract (Time duration in From & To fields is not considered)
    - In this case, Active Users will those users who are currently active at the present time

10.5 Service Usage Reports

Customers can generate or schedule reports of Cloudbrink service usage for a specific period. The service usage reports can be generated for a specific user or at the complete ORG level.

The service report contains information about the data below.

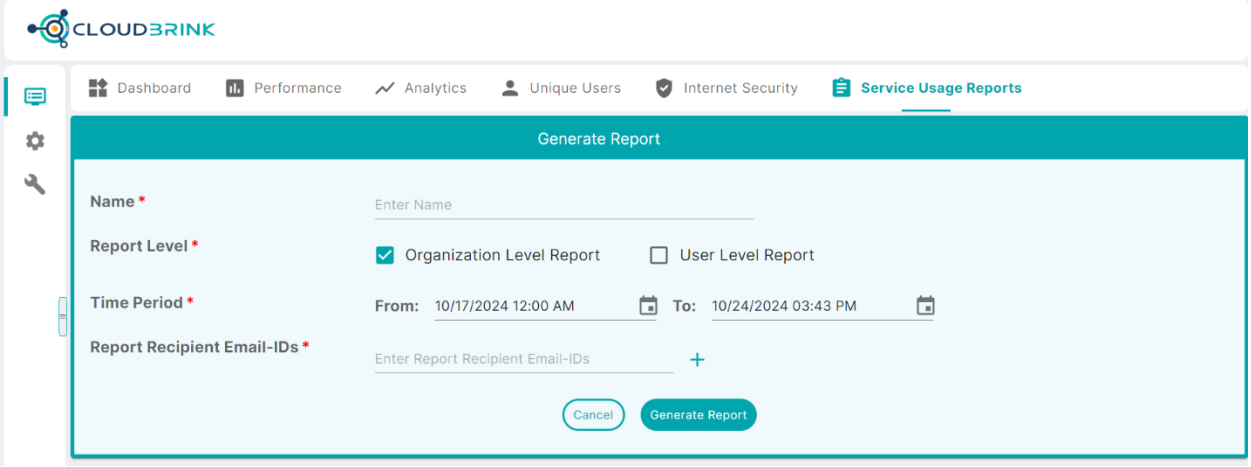
- Users using Cloudbrink service in that period
- Devices being used by each user
- Apps accessed by these users
- Total data transferred over Cloudbrink tunnel
- And other data points

10.5.1 Organization level report

Admin can generate or schedule the service usage report for complete organization for specific period by configuring a required parameter. The report will be generated in a few minutes (roughly 30min) and will be sent to the email IDs specified in the configuration.

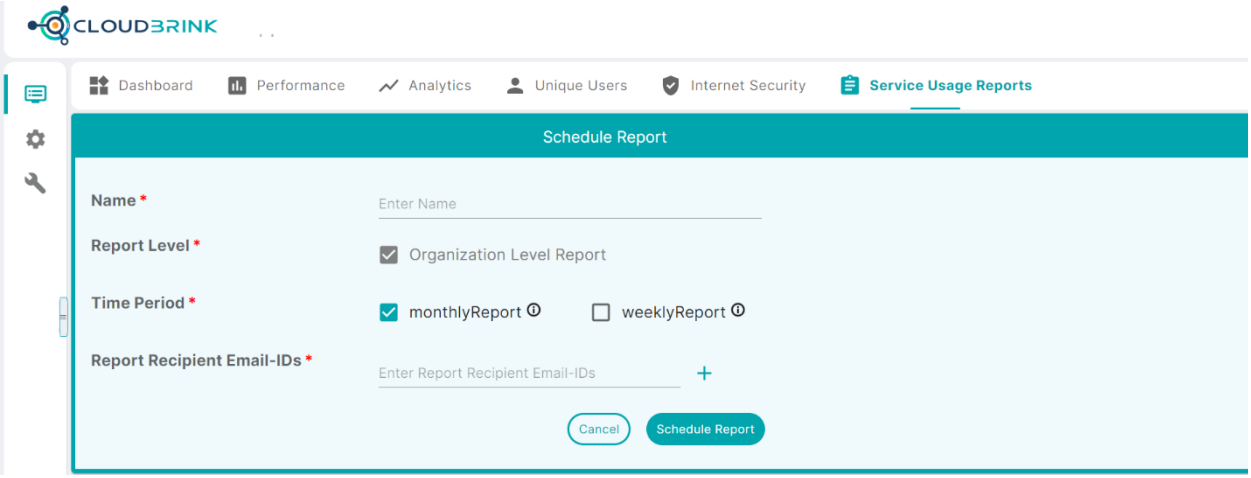
Generate Organization-level report for one-time:

Monitor → Service Usage Reports → Generate



Schedule Organization-level report on Monthly or Weekly basis in recurring manner:

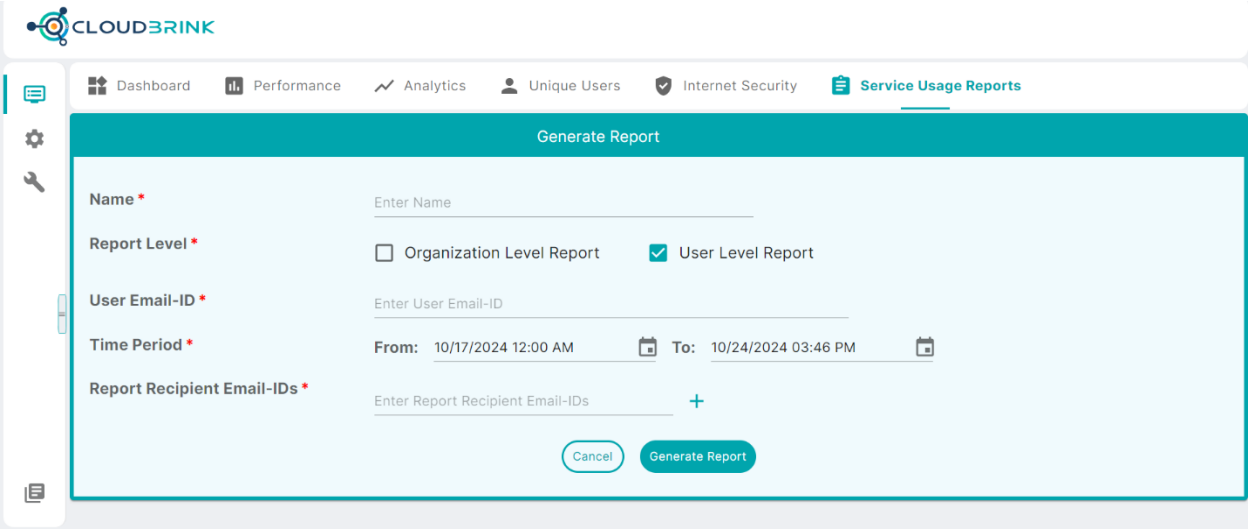
Monitor → Service Usage Reports → Schedule



10.5.2 User level reports

Admin can generate service usage report for a specific user and for a specific period. Admin has to provide the user email ID for whom the report needs to be generated apart from the time period and recipient email ID details.

Monitor → Service Usage Reports → Generate



10.6 App-Level QOE Analytics

NOTE (Internal): This feature is available only if the feature flag "App-Level QOE Visibility" is set to ENABLED for the tenant from the Ops-portal or MSP-portal.

Cloudbrink provides best user experience (Quality of Experience – QOE) when accessing enterprise applications from anywhere over a highly secured zero-trust platform. Customers can improve their user's productivity while providing flexibility to work from anywhere options without compromising on the application performance or user experience.

It is very critical for IT administrators to have a deep visibility into the quality of experience that users are getting. These insights help administrators to monitor, plan and deliver the right set of applications and user experience to their users. Administrators can use the deeper visibility into user experience in two different ways.

Use Cases:

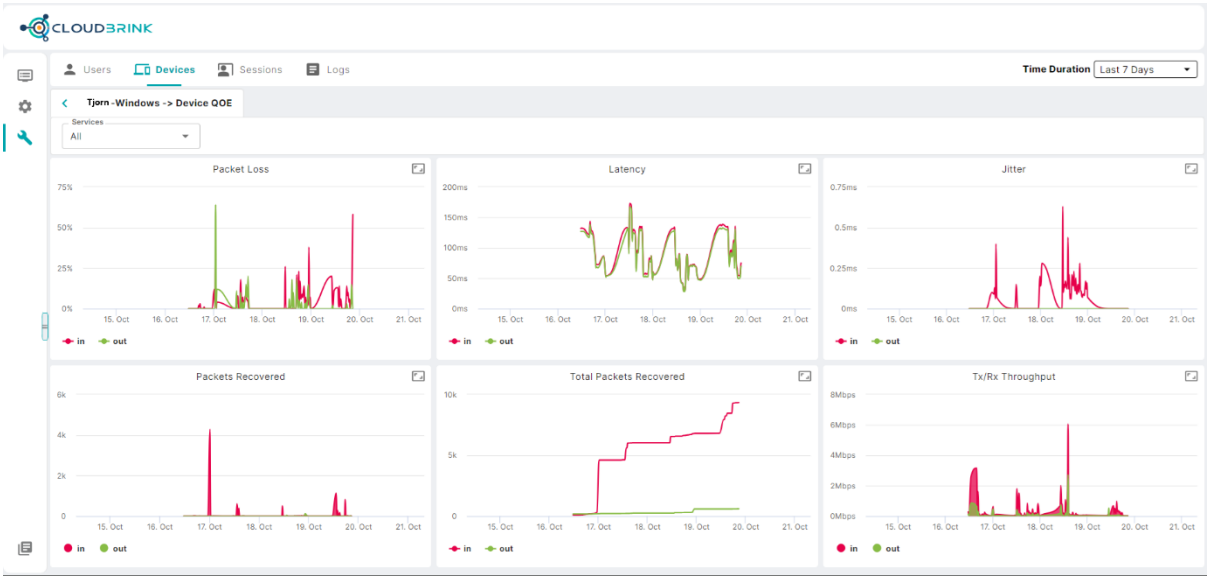
1) **Cloudbrink Value**: Administrators can quickly see the benefits of Cloudbrink platform in terms of how the network impairements have been overcome and the throughput that their users are able to get.
2) **Troubleshoot**: When users raise IT tickets related to application performance or experience, administrators can quickly triage the issue using the Cloudbrink QOE analytics info and narrowing down the root cause of the problem.

QOE Analytics Functionality

QOE Analytics feature provides deeper insights into the network characteristics and traffic information for each endpoint/device of a user at the device-level and at the individual application level.

Administrators can navigate to the QOE Analytics section from the Admin Portal (aka Enterprise Portal) in the following path

Admin Portal → Troubleshoot → Devices → QOE column → Click on the value of the QOE



i) Packet Loss

Packet loss graph shows the total percentage of the packets lost at the endpoint. This packet loss percentage is before the Cloudbrink recovered the packets. This information provides insight into the quality of the user's ISP network and any potential issues in the last-mile.

ii) Packets Recovered

Packets recovered is the no.of packets that Cloudbrink was able to recover from the network after detecting that there is packet loss at the endpoint. Administrators can corelate this information with the Packet Loss graph to see that when there is packet loss detected on the last-mile network, Cloudbrink will start the recovery process and hence, ensures applications perform at optimal levels.

iii) Latency

Latency is the end-to-end between BrinkAgent (endpoint) to the application service/server that user is accessing over Cloudbrink tunnel. The lower the latency, the higher the application performance can be maintained.

iv) Total Packets Recovered

Total packets recovered in the cumulative number of total packets that Cloudbrink was able to recover in the selected time duration.

v) Jitter

Jitter value is applicable only for "collaboration" (UCaaS) type of applications such as Zoom, Teams, Webex, etc. Maintaining a low and consistent jitter is important for having a productive

virtual meeting. Administrators can see the jitter that Cloudbrink is able to manage for UCaaS applications in order to deliver best quality of experience.

vi) Tx/Rx Throughput

The Tx/Rx throughput is the throughput over Cloudbrink tunnel that the user was able to achieve. The graph provides both Tx (transmission) and Rx (receive) side of the throughput so that administrators have clear insight into the network performance of the endpoint.

vii) Services dropdown:

The "Services" dropdown at the top of the graphs can be used to select a specific application for which administrators want to get deeper insights. When "Services" dropdown is selected as "All", the data in the graphs is at the device-level. If a specific app is selected, then the data in the graphs is at the individual application-level.

viii) Time Duration:

Time duration is a common field in all the sections of the Cloudbrink Admin Portal. The data shown in the graphs will be limited to the selected time duration. Administrators can see data for the last 30days by setting the time duration accordingly.

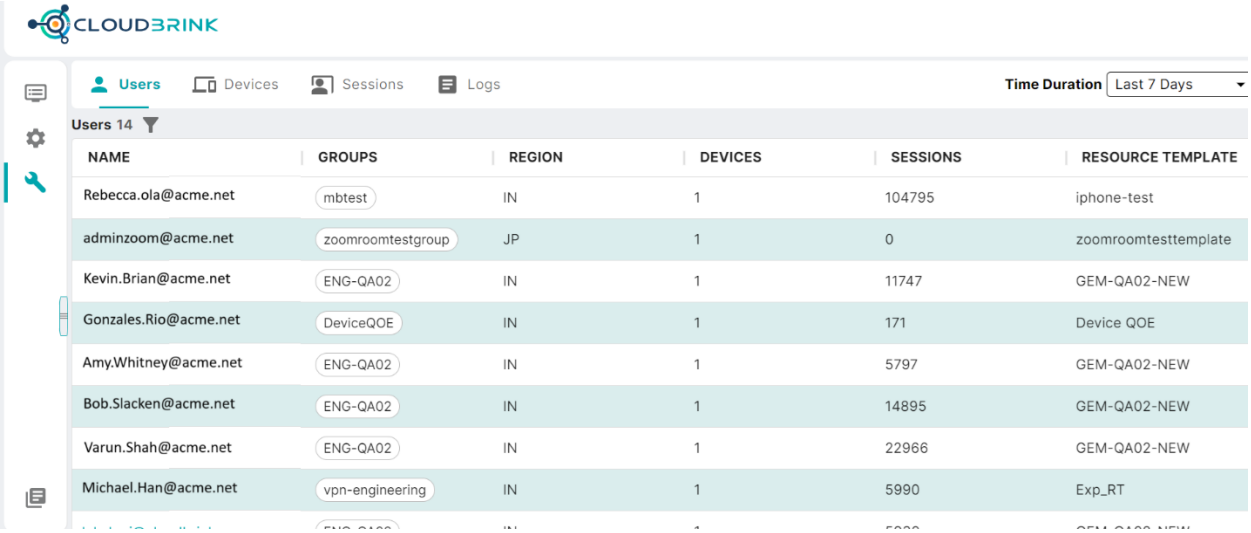
11. Troubleshoot

Customers can use Troubleshoot section on the management portal for analyzing any issues that users might be reporting. Cloudbrink collects rich data related to user activity (both control plane and data plane) and displays the data to admins. Cloudbrink provides multiple views into the data, so that admins can deep dive from any view. Cloudbrink provides users-based view, applications-based view, devices/endpoints-based view in addition to raw log messages.

11.1 Users

Users section provides information about all the users using Cloudbrink service in the last 7-days, along with information related to user devices, location, group, etc. Admin can deep dive into specific user to get details about their devices, application sessions and logs as well.

Users table

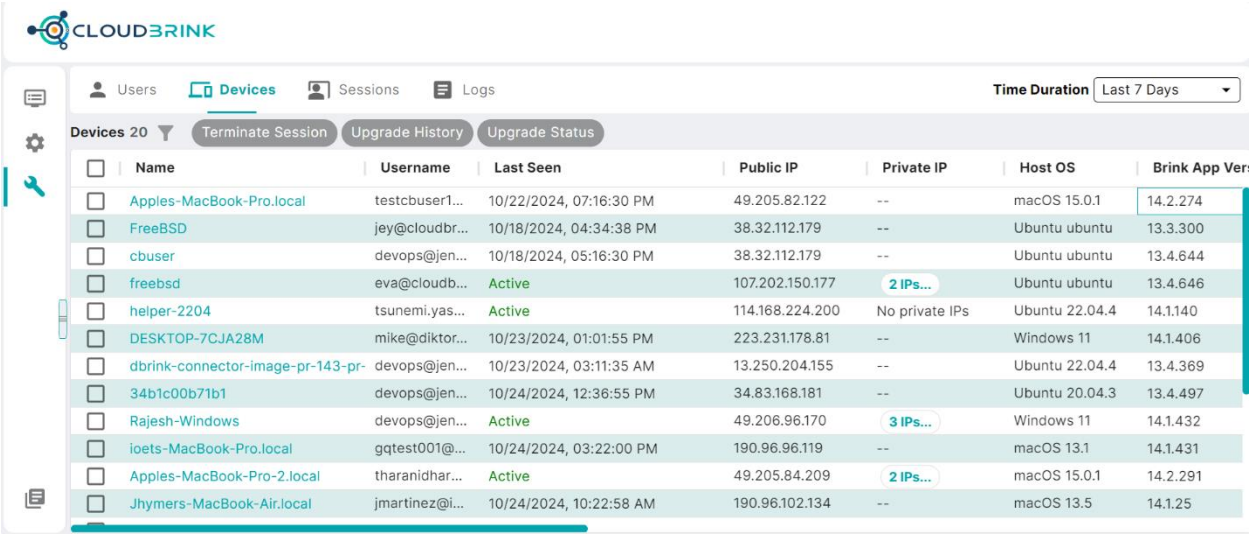


NAME	GROUPS	REGION	DEVICES	SESSIONS	RESOURCE TEMPLATE
Rebecca.ola@acme.net	mbtest	IN	1	104795	iphone-test
adminzoom@acme.net	zoomroomtestgroup	JP	1	0	zoomroomtesttemplate
Kevin.Brian@acme.net	ENG-QA02	IN	1	11747	GEM-QA02-NEW
Gonzales.Rio@acme.net	DeviceQOE	IN	1	171	Device QOE
Amy.Whitney@acme.net	ENG-QA02	IN	1	5797	GEM-QA02-NEW
Bob.Slacken@acme.net	ENG-QA02	IN	1	14895	GEM-QA02-NEW
Varun.Shah@acme.net	ENG-QA02	IN	1	22966	GEM-QA02-NEW
Michael.Han@acme.net	vpn-engineering	IN	1	5990	Exp_RT

11.2 Devices

Devices section provides granular details of each device/endpoint that users have been using. Admins can use this information to find out total number of devices on which Cloudbrink service is running, and several other details of each device.

Devices/endpoints details table



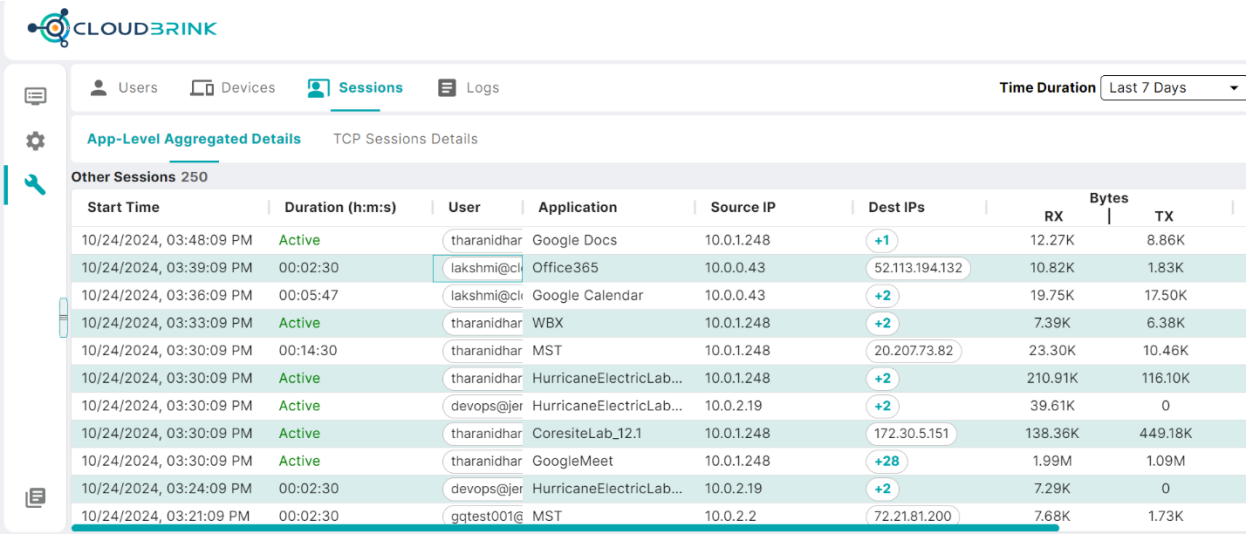
Name	Username	Last Seen	Public IP	Private IP	Host OS	Brink App Ver
Apples-MacBook-Pro.local	testcbuser1...	10/22/2024, 07:16:30 PM	49.205.82.122	--	macOS 15.0.1	14.2.274
FreeBSD	jey@cloudbr...	10/18/2024, 04:34:38 PM	38.32.112.179	--	Ubuntu ubuntu	13.3.300
cbuser	devops@jen...	10/18/2024, 05:16:30 PM	38.32.112.179	--	Ubuntu ubuntu	13.4.644
freebsd	eva@cloudb...	Active	107.202.150.177	2 IPs...	Ubuntu ubuntu	13.4.646
helper-2204	tsunemi.yas...	Active	114.168.224.200	No private IPs	Ubuntu 22.04.4	14.1.140
DESKTOP-7CJA28M	mike@diktor...	10/23/2024, 01:01:55 PM	223.231.178.81	--	Windows 11	14.1.406
dbrink-connector-image-pr-143-pr-	devops@jen...	10/23/2024, 03:11:35 AM	13.250.204.155	--	Ubuntu 22.04.4	13.4.369
34b1c00b71b1	devops@jen...	10/24/2024, 12:36:55 PM	34.83.168.181	--	Ubuntu 20.04.3	13.4.497
Rajesh-Windows	devops@jen...	Active	49.206.96.170	3 IPs...	Windows 11	14.1.432
ioets-MacBook-Pro.local	gqtest001@...	10/24/2024, 03:22:00 PM	190.96.96.119	--	macOS 13.1	14.1.431
Apples-MacBook-Pro-2.local	tharanidhar...	Active	49.205.84.209	2 IPs...	macOS 15.0.1	14.2.291
Jhymers-MacBook-Air.local	jmartinez@i...	10/24/2024, 10:22:58 AM	190.96.102.134	--	macOS 13.5	14.1.25

11.3 Sessions

Sessions section provides information about applications that are being served by Cloudbrink service. The details are provided at TCP/UDP and L3 layer networking details for admins to troubleshoot issues specific to applications.

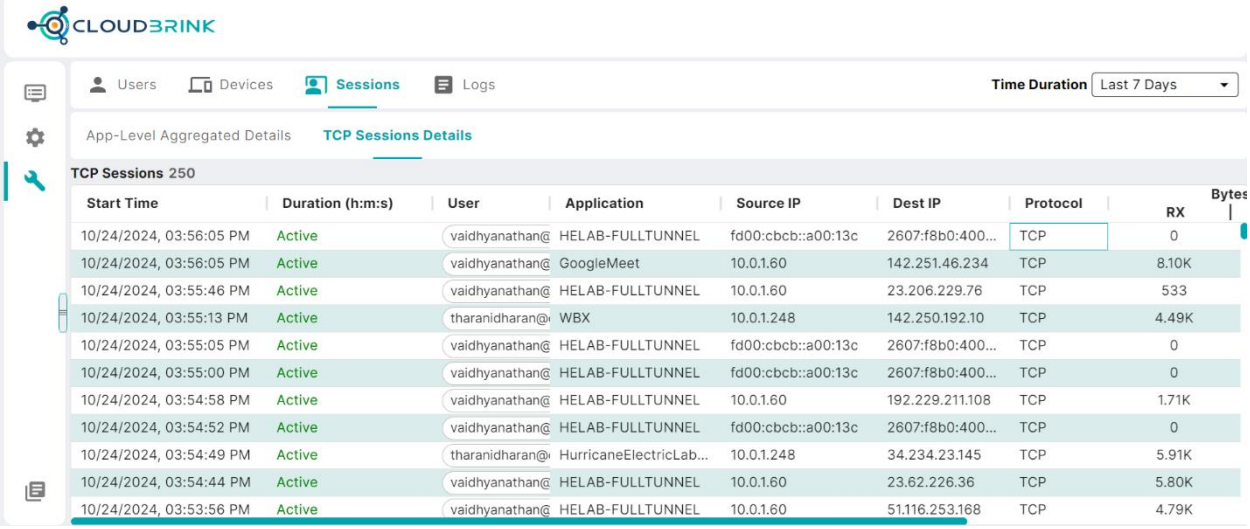
Application-level Aggregated details

This section provides information about the app-level view for all sessions of all types of protocols. Each row in this table represents the aggregated traffic info for a particular app used by the user. Each row represents the aggregated value of multiple network level connections (TCP / UDP) that are used by the application.



TCP Session Details

This section provides network level details for only TCP type connections. UDP connection level details will be provided in next releases.

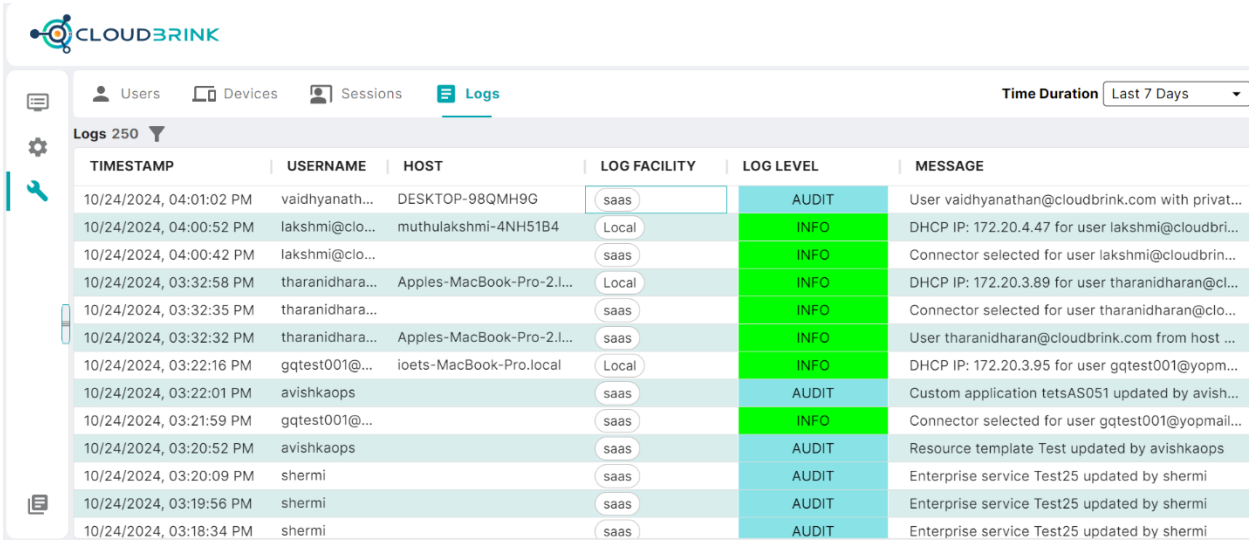


11.4 Logs

Logs section provides all details about user activity (eg: login, app launch, private IP being assigned, etc.) as well as admin activity (eg: config changes). Each event will have a log message that is displayed in the Logs section.

Log messages that are applicable for user activity will have username field also in the logs table. This username field can be helpful in troubleshooting user-specific issues or track user activity by filtering based on username.

Log messages for all user/admin activity



TIMESTAMP	USERNAME	HOST	LOG FACILITY	LOG LEVEL	MESSAGE
10/24/2024, 04:01:02 PM	vaidhyanath...	DESKTOP-98QMH9G	saas	AUDIT	User vaidhyanathan@cloudbrink.com with privat...
10/24/2024, 04:00:52 PM	lakshmi@clo...	muthulakshmi-4NH51B4	Local	INFO	DHCP IP: 172.20.4.47 for user lakshmi@cloudbri...
10/24/2024, 04:00:42 PM	lakshmi@clo...		saas	INFO	Connector selected for user lakshmi@cloudbrin...
10/24/2024, 03:32:58 PM	tharanidhara...	Apples-MacBook-Pro-2.l...	Local	INFO	DHCP IP: 172.20.3.89 for user tharanidharan@cl...
10/24/2024, 03:32:35 PM	tharanidhara...		saas	INFO	Connector selected for user tharanidharan@clo...
10/24/2024, 03:32:32 PM	tharanidhara...	Apples-MacBook-Pro-2.l...	saas	INFO	User tharanidharan@cloudbrink.com from host ...
10/24/2024, 03:22:16 PM	gqtest001@...	ioets-MacBook-Pro.local	Local	INFO	DHCP IP: 172.20.3.95 for user gqtest001@yopm...
10/24/2024, 03:22:01 PM	avishkaops		saas	AUDIT	Custom application tetsAS051 updated by avish...
10/24/2024, 03:21:59 PM	gqtest001@...		saas	INFO	Connector selected for user gqtest001@yopmail...
10/24/2024, 03:20:52 PM	avishkaops		saas	AUDIT	Resource template Test updated by avishkaops
10/24/2024, 03:20:09 PM	shermi		saas	AUDIT	Enterprise service Test25 updated by shermi
10/24/2024, 03:19:56 PM	shermi		saas	AUDIT	Enterprise service Test25 updated by shermi
10/24/2024, 03:18:34 PM	shermi		saas	AUDIT	Enterprise service Test25 updated by shermi

About Cloudbrink

Cloudbrink is a cloud-delivered IT Networking & Security services company that provides in-office like quality of experience (QoX) to users connecting from anywhere to their enterprise apps, along with zero-trust secure access (ZTNA).

Enterprises are adopting the new Hybrid-Work and Multi-Cloud IT infrastructure way of running their business operations. To be competitive and agile, enterprises need IT services that support Hybrid-Work and Multi-Cloud technologies by rearchitecting the solutions that meet the new IT needs rather than force-fitting legacy appliance-based, datacenter products.

Cloudbrink is redefining the Future of Work for global enterprises. The platform leverages principles of Zero-Trust Access with that of the recent market trends of Edge Computing to create a highly robust and scalable cloud-native SaaS service. Cloudbrink has built a software-only platform ground-up with performance and security as core benefits. Global enterprises that have massive user-base and operations are trusting on Cloudbrink to deliver networking and security services to their user base wherever they are working from, and with the highest level of security.