



Citrix Secure Internet Access

Contents

Citrix Secure Internet Access	2
Release notes	5
What’s new	5
Fixed issues	8
Known issues	10
Getting started	10
Licensing	26
Dashboard	28
Configuration	31
Administration	44
Glossary	52

Citrix Secure Internet Access

December 28, 2021

What is Citrix Secure Internet Access?

Citrix Secure Internet Access (CSIA) is a cloud-delivered service that provides secure access to web and SaaS applications, globally. It provides a complete stack of security capabilities, such as Secure Web Gateway, Cloud Access Security Broker, Malware Protection with Sandboxing, Intrusion Prevention and Detection Systems, and Data Loss Prevention.

Along with SD-WAN and Secure Workspace Access, Citrix Secure Internet Access forms one of the pillars of the fully integrated Secure Access Service Edge (SASE) solution that Citrix provides.

Citrix Secure Internet Access offers secure access to web and SaaS apps inside and outside the Citrix Workspace, irrespective of user location. It adds an extra layer of protection for Citrix Workspace users and also integrates with Citrix SD-WAN for a fully converged Citrix network and security solution.

Features and benefits of Citrix Secure Internet Access

Citrix Secure Internet Access helps provide unified management of services made available through Citrix Cloud. The following list summarizes the key features and benefits of Citrix Secure Internet Access.

- **Unified management.**

- A holistic view and granular control over the comprehensive security capabilities. This is provided on a single platform, alongside analytics for identifying security incidents, unusual behavior, reported risks, productivity loss, and policy violations.
- Users with both SD-WAN and Citrix Secure Internet Access entitlements can manage these services from the same pane. As a result, all traffic and users are protected with a combination of network and security architectures in one platform.

- **Efficiency.**

- Simple and fast deployment, with automated configuration between Citrix SD-WAN and Citrix Secure Internet Access.
- High performance architecture that scales at cloud speed.
- Single pass architecture for optimal performance: traffic is decrypted once, and all security controls are applied before being re-encrypted.

- Reduced latency with SD-WAN: auto-selection of the closest Citrix Secure Internet Access gateway node.
- **Reliable performance.**
 - Automated updates for the latest protection against security threats.
 - Back up links for dual resiliency.
 - Faster troubleshooting for IT due to the single, unified view.
- **Privacy.** Each customer's data is processed through separate gateways and segregated by enterprise in the Citrix Secure Internet Access service.
- **Better remote working user experience.** Moving network security to the cloud, where the resources that users want to access already live, brings security closer to the users. Citrix Secure Internet Access service has more than 100 points of presence (PoP) across the globe.

For more information about the key features and benefits, see the [solution brief](#).

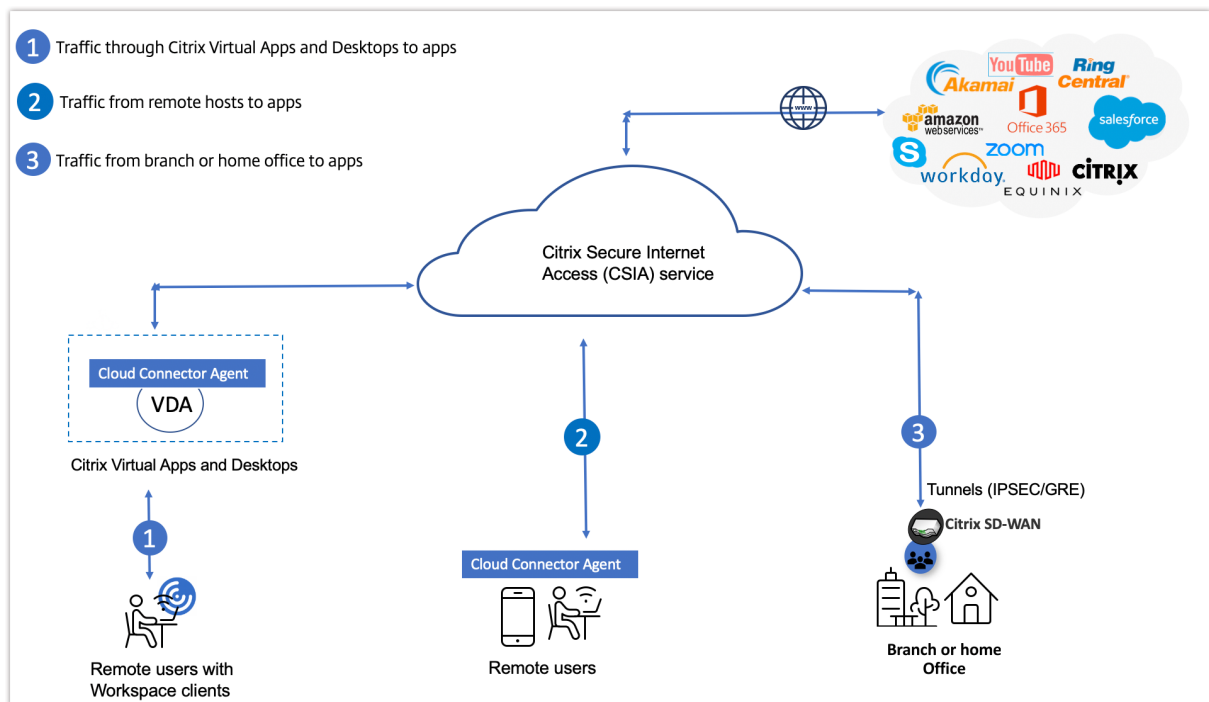
How Citrix Secure Internet Access works

Your users might access unsanctioned web and SaaS applications using one of the following methods:

- through virtual desktops using Citrix Workspace
- remotely from local host systems
- from a branch or home office

Whichever method of direct internet access that the user adopts, traffic is redirected through Citrix Secure Internet Access.

The following diagram is a visual depiction of the different use cases.



As shown in the preceding image, the following three key use cases describe how the process works.

- 1. Citrix Virtual Apps and Desktops.** Remote users with Workspace apps can securely access unsanctioned web and SaaS applications through Citrix Virtual Apps and Desktops. Install a CSIA Cloud Connector agent on the Virtual Delivery Agent (VDA) to redirect internet traffic to the Citrix Secure Internet Access service.
- 2. Native browsers on host systems.** Remote users can securely access unsanctioned apps using their local systems, such as laptops and mobile devices (managed or unmanaged). To secure traffic on these devices, install CSIA Cloud Connector agents to redirect all internet traffic to the Citrix Secure Internet Access service.

The Cloud Connector agent also authenticates the user and installs the appropriate certificates for SSL decryption. Cloud Connector agents are available for the following operating systems: iOS, macOS, Android, Windows, Linux.

- 3. Branch offices.** Onsite users can securely access web and SaaS apps through Citrix SD-WAN by redirecting the traffic to Citrix Secure Internet Access. This occurs through IPsec or GRE tunnels, without the need for a Cloud Connector agent.

Citrix SD-WAN automatically creates secure connectivity to the closest Citrix Secure Internet Access point of presence (PoP). Traffic is tunneled through IPsec or GRE tunnels. Redundancy is achieved both at the tunnel level and through multiple links to primary and secondary Citrix Secure Internet Access PoPs.

Where to go next

- Understand the licensing editions available. See [Licensing](#)
- Review the pre-requisites before you begin onboarding. See [Pre-requisites](#)
- Begin the onboarding process. See [Onboarding](#)
- Configure Cloud Connector agents. See [Configuration](#)

Release notes

April 29, 2021

The Citrix Secure Internet Access service release notes describe the new features, fixed issues, and known issues in a service release. The release notes include the following sections:

- [What's new](#): The new features and enhancements in the release.
- [Fixed issues](#): The issues that were fixed in the release.
- [Known issues](#): The issues that exist and their workaround, where applicable.

What's new

December 2, 2021

This article provides a list of the latest customer-facing features for the Citrix Secure Internet Access (CSIA) 2021-Q3 Release.

December 2, 2021

Azure Active Directory support for SSO

Azure Active Directory (AD) is also supported as an Identity Provider (IdP) for Single sign-on (SSO) with Citrix Secure Internet Access (CSIA) account. By default, the CSIA account is configured with Citrix IdP settings. If the Citrix tenant has Azure AD enabled, the CSIA account is configured with Azure AD IdP for SSO validation. Currently, a given CSIA account can be configured to have either Azure AD IdP or Citrix IdP settings.

Integration with Citrix Secure Browser Service

Citrix Secure Browser Service provides **Remote Browser Isolation** by isolating web browsing to protect the corporate network from browser-based attacks. With Citrix Secure Internet Access, you can create and apply web filtering rules to redirect web traffic to a Secure Browser instance.

October 28, 2021

Onboarding

The Citrix Secure Internet Access onboarding helps you configure your user account post you get the cloud access and done with the initial setup. You must perform some basic onboarding settings to access the other CSIA configuration. You cannot view the configuration policy portal without completing the onboarding process.

Account Settings

The **Account Settings** feature helps to change/override the user account name that appears for your account in the Citrix Secure Internet Access service portal.

October 14, 2021

Offline Cloud Backup

The **Offline Cloud Backup** settings provide the ability to store/save the backup settings and logs from reporting nodes based on the **Region**, **Location**, and **Time** that you select.

Citrix Secure Internet Access APIs with Swagger support

A set of configuration related APIs are now available in the [swagger](#) docs. The CSIA-Core Swagger API information is available under the [sia-core-controller](#) section.

September 15, 2021

Predefined roles

Customer: Read Only Access (Privacy mode) role is introduced as a new predefined role. You can add a user and assign this role from **Citrix Identity and Access Management**. A user that is assigned with the **Customer: Read Only Access (Privacy mode)** role has read-only access to view all the features of the service except for **Licensing** and **User Settings**.

Email settings

The **Email settings** page under **Configuration > Cloud Settings** is enhanced to include the following features:

- **Test Email Settings:** Verify your email settings.
- **Set Default Settings:** Populate the default email settings.
- **Email Recipients:** Add email recipients to receive User Alerts and URL Exception requests.

July 29, 2021

Cloud Settings in Citrix Secure Internet Access UI

The UI now supports Cloud configuration settings for NTP Server, Platform Maintenance, Update Release Settings, and Anonymized Logging. For more information, see [Configuration](#).

ECMP tunnel load balancing

Citrix Secure Internet Access now supports SD-WAN Orchestrator service ECMP load balancing. For more information, see [ECMP load balancing](#).

April 29, 2021

Internet breakout for Cloud Connector traffic

Traffic to Citrix Secure Internet Access cloud nodes is redirected through internet services instead of the IPsec and GRE tunnels deployed on the site. With this direct breakout, you avoid tunneling the traffic twice.

Notifications

To ensure that you don't miss important messages about iboss subscription and configuration changes, the Citrix Secure Internet Access service displays alerts as notifications within the Dashboard.

User reallocation

To minimize latency in particular locations, you can now reconfigure the location of your nodes within a geographical region. You can also edit the number of users assigned to these nodes.

Multi-links support with IPsec and GRE tunnels

Deliver network traffic over multiple tunnels in parallel by configuring tunnels from a single location with multiple ISP connections to the same Service Provider points of presence (PoPs).

Network map of PoPs under a node

View which points of presence (PoPs) are being used for a customer and the SD-WAN branches that connect to Citrix Secure Internet Access PoPs.

Role settings (Technical Preview)

Citrix is offering role-based access control (RBAC). RBAC gives you the ability to customize permission-based roles and to add these roles to different users.

Fixed issues

October 28, 2021

The following issues have been fixed.

October 28, 2021

SIAS-27: Data Loss Prevention (DLP) graphs are now labeled with names when using content analysis search patterns.

SIAS-290: The details section of the cloud status report is no longer being cut off.

SIAS-394: Alerts for advisories and incidents include affected data center information.

SIAS-451: Custom Cloud Access Security Broker (CASB) application controls were now rendering in the user interface.

September 15, 2021

SIAS-218: Provisioning trial SKUs for the middle eastern region is not getting completed successfully.

SIAS-302: Enabling reporting and sending alert email notifications required modifications to the email settings. The issue is now fixed by populating the **Configuration > Email Settings** fields with default values.

SIAS-306: The **Configuration > User Settings** page is shown (instead of getting hidden) to admins who do not have access to view the page. When tried to access, an error is displayed.

SIAS-307: Having user roles with read-only permissions can cache data from one tenant and present it as the data of another tenant.

SIAS-329: The format of cloud status email alerts and notifications is changed to include the following statuses of maintenance, incident, or advisory message:

- New
- Updated
- Rescheduled
- Complete
- Canceled

SIAS-395: The notifications for URL recategorization are enhanced to include status, old category, and new category for the requested URL.

July 29, 2021

SIAS-1: Users receive a block page for the write.com app

SIAS-161: Win7 32-bit client doesn't connect.

SDW-18408: Users with the same permissions for both Citrix Secure Internet Access and SD-WAN are shown in duplicate in **Change Role** settings.

NSSDW-32478: User roles for Customer scope are shown in duplicate for a given user for SIA + SD-WAN customer

April 29, 2021

NSSDW-33107: GRE tunnel connectivity from Citrix SD-WAN isn't supported.

NSSDW-33099: Frame breakout for Android Connector.

NSSDW-33530: Postgres queries aren't encrypted between gateway/reporting servers.

NSSDW-34575: **Proxy & Caching** isn't loading.

Known issues

September 15, 2021

Citrix Secure Internet Access service has the following known issues:

SIAS-13: Ultrasurf blocking requires additional configuration beyond evasive protocol settings.

SIAS-22: On the Configuration policy portal, some of the settings might not be applicable to Citrix Secure Internet Access deployments.

Getting started

October 28, 2021

This article describes how to get started with Citrix Secure Internet Access (CSIA) for the first time.

Before you begin the initial setup, review the [licensing](#) and [pre-requisites](#) information.

Pre-requisites

Ensure you have the following:

- **Citrix Cloud account.** To use Citrix Secure Internet Access, you must have a Citrix Cloud account. Go to <https://citrix.cloud.com> and verify that you can sign in with your existing Citrix Cloud account.

If you do not have a Citrix Cloud account, first create a Citrix Cloud account. You can also join an existing account created by someone else in your organization. For detailed processes and instructions on how to proceed, see [Sign up for Citrix Cloud](#).

- **Citrix Virtual Apps and Desktops deployment** accessible through Citrix Workspace.
- **Workspace app** on your host systems such as laptops and mobile devices.
- **SD-WAN deployments.** If you are working from a branch office, you must have the following deployments:
 - Citrix SD-WAN 11.1 and later
 - Subscription to Citrix SD-WAN Orchestrator service. Ensure that you have done the initial setup and configured sites on your SD-WAN Orchestrator.

Initial setup

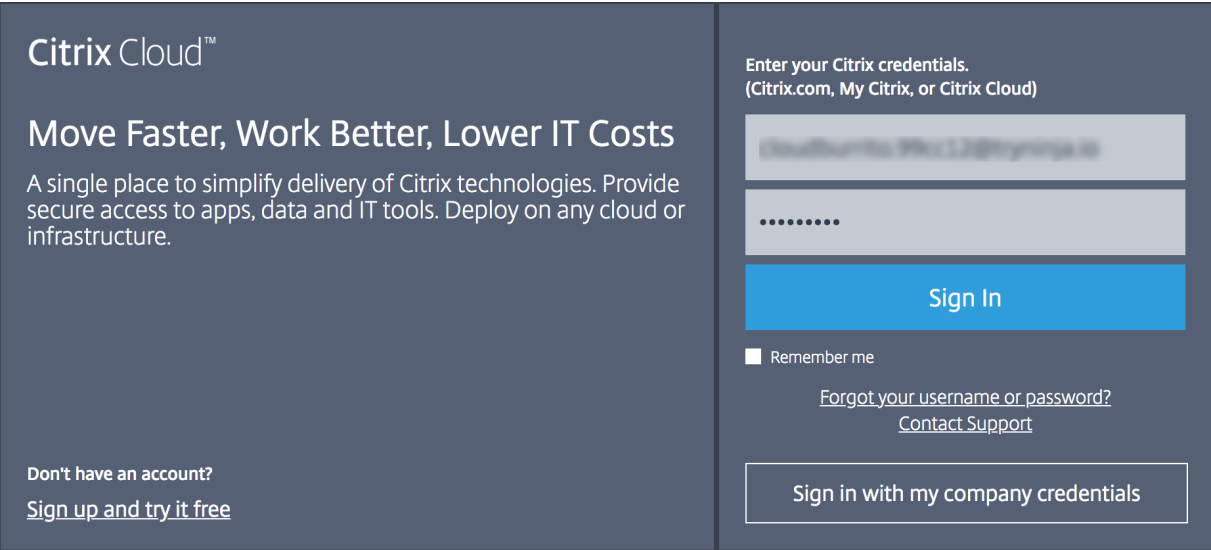
This section walks you through the required tasks for the Citrix Secure Internet Access initial setup.

Step 1: Request access to Citrix Secure Internet Access

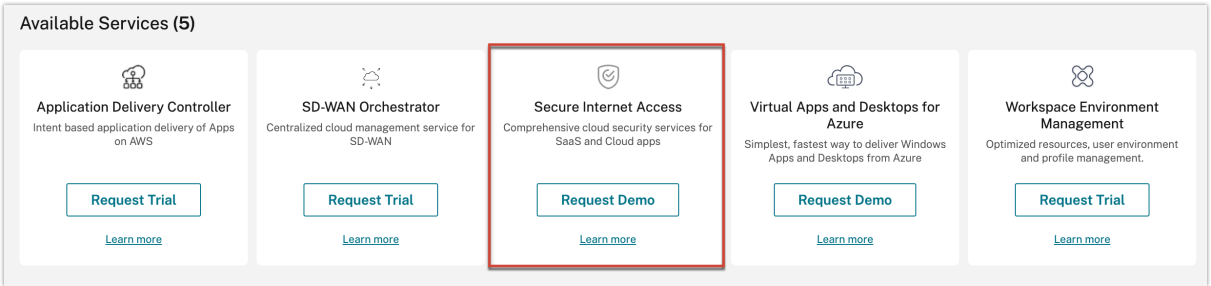
You can get access to Citrix Secure Internet Access by requesting for a Citrix Secure Internet Access trial. You can use the trial for a maximum 60 days period. For more information on service trials, see [Citrix Cloud Service Trials](#).

To request a trial,

Sign in to your Citrix Cloud account.



On the Citrix Cloud home page, in **Available Services**, on the **Secure Internet Access** tile, click **Request Demo**.



Note

Alternatively, you can also visit <https://www.citrix.com/products/citrix-secure-internet-access/form/inquiry/> and contact a Citrix expert who can help you.

Enter the required details and select **Submit**.



Speak to a Citrix Secure Internet Access expert

Secure access to your digital workspace with unified, cloud-delivered security.

Request a call to learn how Citrix Secure Internet Access:

- Enables efficiency with policy configuration, bandwidth control and real-time reporting from one, cloud-managed interface
- Protects users from threats while securing access to both sanctioned and unsanctioned apps
- Segregates your data based on customers and locations to ensure privacy without compromise

Our experts can:

- Show you a live demo
- Discuss implementation options
- Answer your technical questions
- Provide quotes and purchasing information

Tell us about yourself. Simply fill out the form and a Citrix Secure Internet Access expert will contact you shortly

Contact a Citrix representative for more information.

Citrix will process your data according to our [Privacy Policy](#)

When your trial is approved, Citrix initiates the trial process and creates your Customer Entitlement Package based on the license package selected. You also receive an email confirmation.

Step 2: View status of your account

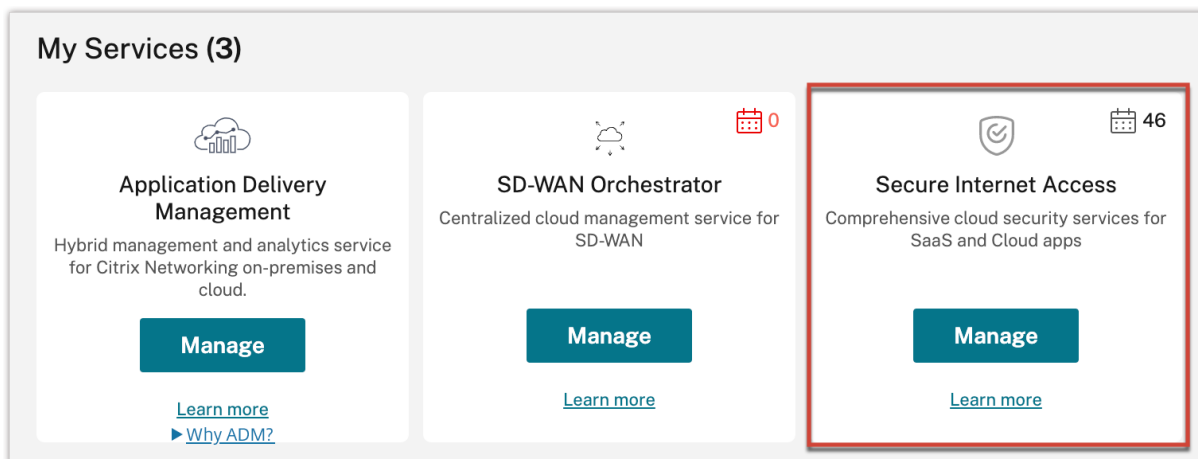
After your trial is approved and initiated, you will receive an email confirmation and you can also view your account status on Citrix Cloud.

To set up your account, Citrix provisions gateway nodes for you implicitly. These nodes are containerized nodes that scan data and traffic in the cloud. The nodes also perform security functions such as web filtering, malware prevention, and data loss prevention.

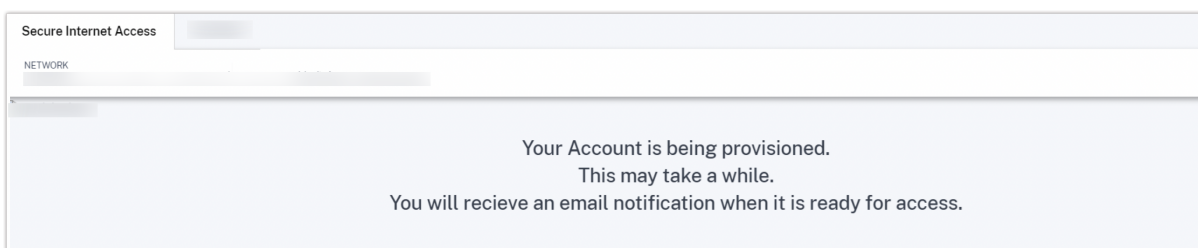
After the nodes are set up, you receive an email notification that your account is available. Provisioning of nodes can take a few days.

To view the status of your account

1. Sign in to your Citrix Cloud account.
2. On the **Citrix Cloud** home page, in **My Services**, on the **Secure Internet Access** tile, click **Manage**.



If your account provisioning is in progress, you see the following message:



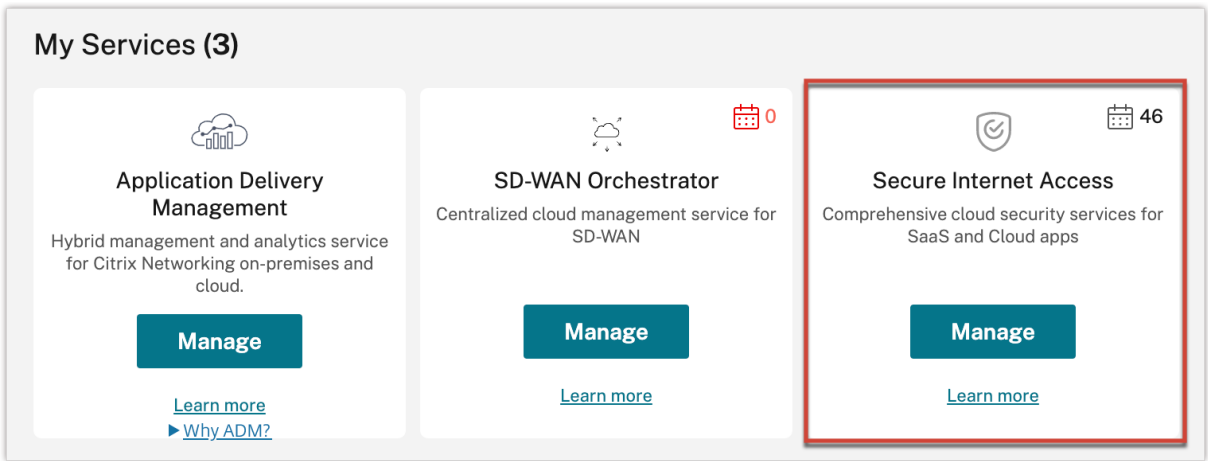
Step 3: Manage Citrix Secure Internet Access

After you receive the email confirmation about your account setup, sign in to Citrix Cloud and start configuring and managing your deployment.

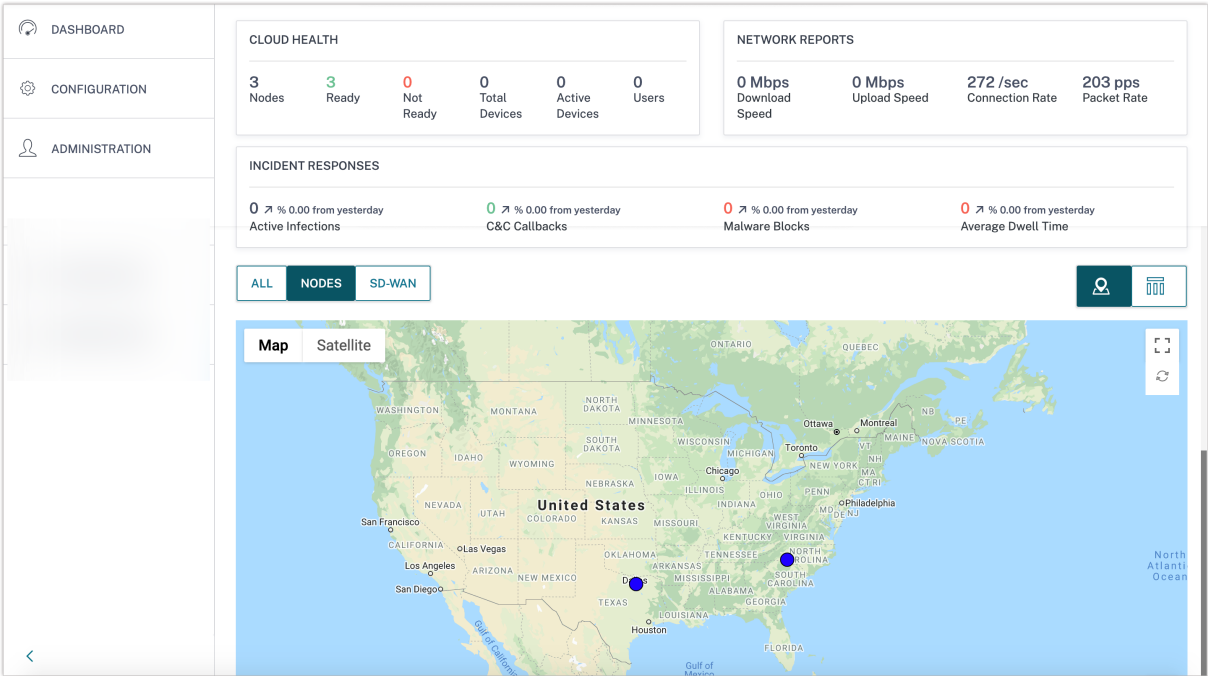
On the **Citrix Cloud** home page, in **My Services**, on the **Secure Internet Access** tile, click **Manage**.

Note

If you have a Citrix SD-WAN Orchestrator subscription, you can also click **Manage** on the **SD-WAN Orchestrator** tile to view the Citrix Secure Internet Access dashboard.



On the **Dashboard** menu, you can view the status and a graphical representation of your nodes.



The initial setup is now complete.

Onboarding

The Citrix Secure Internet Access Onboarding lets you configure your user account after your account is provisioned. You must perform some basic onboarding settings to access the other CSIA configuration.

The **Open Citrix SIA Configuration** option is available in the **Network Configuration Home** page. You cannot view the configuration policy portal without completing the onboarding process.

Once your account is provisioned, you land on the Citrix Secure Internet Access Onboarding page by

default. Click **Get Started** to proceed with the onboarding process or click **Skip Onboarding** to skip this step and perform the onboarding later. When you click **Skip Onboarding**, you will land on the Citrix Secure Internet Access dashboard page.

Getting Started with Secure Internet Access!

Citrix Secure Internet Access (CSIA) is a cloud native internet and web security service. SIA provides end to end web security with integrated SSL inspection, Intrusion prevention system (IPS), malware detection, sandboxing, URL filtering, Data Loss Prevention (DLP) and Cloud Access Security Brokering (CASB).

Unmatched security

Inspect all traffic from and to your users, devices and servers. We leverage Citrix as well as other industry leading malware engines.

Global Presence

Over 100 Points of Presence(PoP) across the globe to provide lightning fast experience regardless of where the user is.

Privacy and Control

We offer dedicated nodes with dedicated gateways to our customers. Use Static IPs for greater access control to sanctioned SaaS apps. Control your own maintenance windows and more.

Seamless Integration

Seamless and simple integration with Citrix ZTNA, RBI (Secure Browser) and SD-WAN to provide a complete SASE solution.

[Get Started](#)

[Learn More](#)

[Skip Onboarding](#)

1. Configure Proxy Settings

Select the user authentication method from the drop-down list. The default value is set to **Local User Credentials + Cloud Connections**.

The screenshot shows the 'Secure Internet Access Onboarding' page. At the top, there's a back arrow and the title 'Secure Internet Access Onboarding'. Below that, a description states: 'Secure Internet Access (SIA) is a cloud native internet and web security service.' A red message says: 'The following changes will be saved and applied.' The main section is 'Step 1: Proxy Settings'. It contains three items: 1. 'Enable Proxy Settings' with a checked checkbox and an information icon. 2. 'User Authentication Method' with a dropdown menu showing 'Local User Credentials + Cloud Connections' and an information icon. 3. 'Enable Proxy SSL Decryption' with a checked checkbox and an information icon.

The following are the four authentication methods:

- **Local User Credentials + Cloud Connections:** Login with local secure internet access account. This method also supports agent mode which enables secure internet access agents/endpoints to automatically register with the gateway by injecting proxy authentication into requests.
- **Local User Credentials:** Login with local secure internet access account.

- **Cloud Connectors Only:** Uses agent mode which enables secure internet access agents/endpoints to automatically register with the gateway by injecting proxy authentication into requests.
- **Browser Based SMAL:** Authentication in the browser and ideal for branch office users who would be sourced from the same public IP.

Enable Proxy Settings and **Enable Proxy SSL Decryption** settings are enabled by default and non-editable check boxes.

In the proxy auto configuration settings, under the **PAC Settings: Bypass Domains** section, select the following check box as required:

- **Bypass WebSockets:** Bypass domains for WebSockets traffic and WebSockets traffic over the Secure Sockets Layer (SSL)/ Transport Layer Security (TLS). The **Bypass WebSockets** check box is enabled by default.
- **Bypass Cloud security for Citrix Cloud infrastructure domains:** Bypass the Citrix sites requests. It is enabled by default. The **Citrix Cloud Domain List** is a non-editable list of Citrix Cloud infrastructure domains that must be bypassed from any inspection.

The screenshot displays the 'Step 1: Proxy Settings' configuration window. Under 'PAC Settings: Bypass Domains', the 'Bypass Cloud security for Citrix Cloud infrastructure domains' checkbox is checked and highlighted with a red box. To its right, a link labeled 'Citrix cloud Domain List' is visible. Below this, there are two more options: 'Bypass cloud security for all domains used by Microsoft Office 365 (Recommended By Microsoft)' (checked) and 'Bypass cloud security for this subset of domains' (unchecked, with a link to 'Custom cloud Domain List'). On the right side of the window, a list titled 'Citrix cloud Domain List' contains various domains including cloud.com, citrixdata.com, citrixworkspaceapi.net, citrixnetworkapi.net, nssvc.net, xendesktop.net, cloudapp.net, and netscalergateway.net. At the bottom of the configuration window are 'Back' and 'Next' buttons. The domain list on the right has an 'Ok' button at the bottom.

- **Bypass Cloud security for all domains used by Microsoft Office 365 (Recommended by Microsoft):** Bypass the domains that is used for the Microsoft Office 365. The **Bypass Cloud security for all domains used by Microsoft Office 365 (Recommended by Microsoft)** check box is enabled by default.
- **Bypass Cloud security for this subset of domains:** Bypass any custom domains. You can

create your own domains using the **Custom Cloud Domain List** option.

Step 1: Proxy Settings

☒ Enable Proxy Settings ⓘ

User Authentication Method

Local User Credentials + Cloud Connections ⓘ

☒ Enable Proxy SSL Decryption ⓘ

PAC Settings: Bypass Domains

☒ Bypass WebSockets ⓘ

☒ Bypass Cloud security for Citrix Cloud infrastructure domains [Citrix cloud Domain List](#)

☒ Bypass cloud security for all domains used by Microsoft Office 365 (Recommended By Microsoft)

☐ Bypass cloud security for this subset of domains [Custom cloud Domain List](#)

Back

Next

Custom cloud Domain List

Enter Custom Domain List

Add each domain on new line

Ok

Click **Next**.

PAC Settings: Bypass Domains

☒ Bypass WebSockets ⓘ

☒ Bypass Cloud security for Citrix Cloud infrastructure domains [Citrix cloud Domain List](#)

☒ Bypass cloud security for all domains used by Microsoft Office 365 (Recommended By Microsoft)

☐ Bypass cloud security for this subset of domains [Custom cloud Domain List](#)

Back

Next

2. Configure Cloud Connector Settings

The Cloud Connector is a downloadable agent that is available for various OS such as Windows, Linux, macOS, and so on. These settings will configure the behavior of the installed Cloud Connector on your devices.

← Secure Internet Access Onboarding

Secure Internet Access (SIA) is a cloud native internet and web security service.

The following changes will be saved and applied.

Step 2: Cloud Connector Settings

<input checked="" type="checkbox"/>	Use HTTPS PAC	i
<input checked="" type="checkbox"/>	Register Over SSL	i
<input checked="" type="checkbox"/>	Configure Auto Login	i

Agent Policy (Default Group)

<input checked="" type="checkbox"/>	Redirect All Ports	i
<input checked="" type="checkbox"/>	Bypass Private Subnets	i

<input type="checkbox"/>	Enable Multi-User Mode	i
<input type="checkbox"/>	Enable Windows Desktop App	i

[Back](#) [Next](#)

Use **HTTPS PAC**, **Register Over SSL**, **Configure Auto Login**, **Redirect All Ports**, and **Bypass Private Subnets** settings are enabled by default and cannot be edited.

- **Enable Multi-User mode:** Check/Uncheck the **Enable Multi user mode** as needed. You can select **Enable Multi-User mode** to support multiple user sessions when running a virtual desktop or terminal server.
- **Enable Windows Desktop App:** Check/Uncheck the **Enable Windows Desktop App** as

needed. The **Enable Windows Desktop Application** installs an interactive desktop application on Windows devices.

Click **Next**.

3. Configure Security Settings

In Security Settings page configure Web Security, Cloud Access Security Broker, Malware Defense and Intrusion Prevention settings (available in Advanced and Premium SKUs), and Data Loss Prevention (available in Premium SKUs).

- **Web Security**

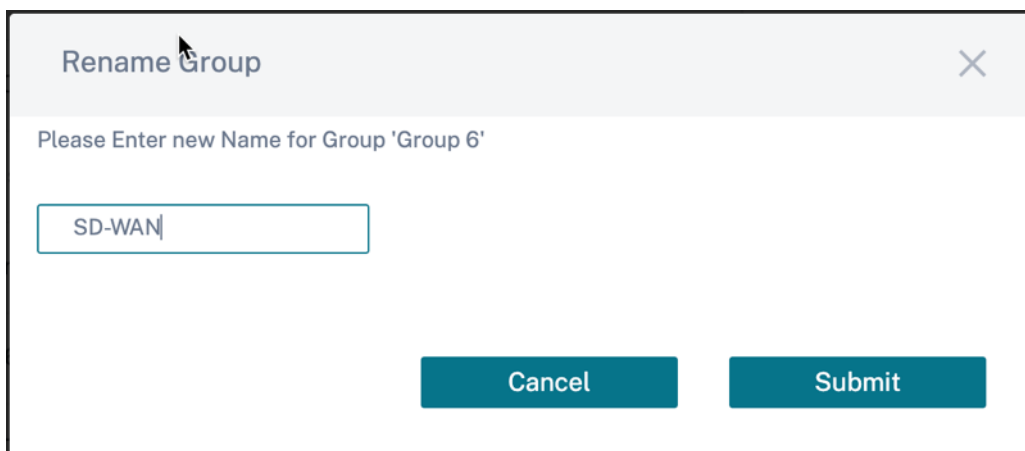
- **Show Groups:** View the first 20 groups list.

Web Security



Show Groups

You can edit the names of the group, for example department/domain/product and so on. Click the edit option next to the group name > enter the group name > click **Submit**.



Rename Group

Please Enter new Name for Group 'Group 6'

SD-WAN

Cancel Submit

Upon selection of a group, the pre-defined group policy is applied on the user. The **Default** group is a non-editable group.

Web Security

Hide Groups

Select	Group Names	Actions
<input checked="" type="checkbox"/>	Default	
<input checked="" type="checkbox"/>	Demo Citrix User	...
<input checked="" type="checkbox"/>	Demo Citrix Guest	...
<input checked="" type="checkbox"/>	Administrators	...
<input checked="" type="checkbox"/>	New Group 5	...
<input checked="" type="checkbox"/>	Group 6	...
<input checked="" type="checkbox"/>	Group-7	...
<input checked="" type="checkbox"/>	Group 8	...

All these 20 groups are checked by default. You can check/uncheck the groups as required. The changes you make to the security settings are applied to the selected group.

- **Block Default Keywords:** Select the **Adult** and **High Risk** check boxes to block the defined keywords. The **Edit** option helps you to configure the set of keywords that you want to block.

Click **Edit** > Select **Adult Words/Select High Risk Words** > select the available keywords and move them to selected section and click **Save**.

The search bar helps to quickly find the keyword you are looking for.

Search

Available (176 Adult Words)

☐ Name

☐ affiliates

☐ amateur

☐ anal

☐ anime

☐ ass

☐ asses

☐ asshole

☐ babe

☐ babes

☐ bbw

☐ bdsm

☐ bikini

→

←

Selected (2 Adult Words)

☐ Name

☐ adult

☐ adult-dating

Save

Cancel

- **Web Filtering Level:** Select the **Web Filtering Level** to **Allow All, Lenient, Moderate,** or **Strict** profile. These filtering levels are defined based on some pre-set categories as described in the below table:

Category	Lenient	Moderate	Strict
Adult	Blocked	Blocked	Blocked
Computing and Internet	Some blocked	Some blocked	Blocked
Gambling	Blocked	Blocked	Blocked
Illegal and harmful content	Blocked	Blocked	Blocked
Malware and Spam	Blocked	Blocked	Blocked
Business and Industry, Finance	Allowed	Blocked	Blocked
Email, Messaging, Chat, Telephony	Allowed	Blocked	Blocked
News, Entertainment, and Society	Allowed	Some blocked	Blocked
Social Networking	Allowed	Blocked	Blocked

Web Security

Show Groups

Block Default Key Words: ?

☒

Adult [Edit](#)

☒

High Risk [Edit](#)

Web Filtering Level ☐ Allow All ☒ Lenient ☐ Moderate ☐ Strict [More Info](#)

Click **More Info** link to view the web filtering level information.

- **Cloud Access Security Broker:** Provides the ability to block file uploads to various services, enforce safe search through various search engines such as Google/Yahoo/Bing and so on.

If the **Microsoft Azure and Office 365 Tenant Restriction** check box is selected, specify the allowed domain names and multitenant context to apply the security settings.

Select the location (All/Dropbox/Box/OneDrive/Google Drive/Generic File Uploads/None) from the **Prevent File Uploads** drop-down list to prevent uploading the files. By default **All** is selected.

Cloud Access Security Broker

Show Groups

☒ Microsoft Azure and Office 365 Tenant Restrictions

Allowed Microsoft Domains (comma separated) ?

Allowed Multi-tenant context ?

☒ Google, Yahoo, Bing, YouTube Safe search enforcement ?

Prevent File Uploads

All X

Back

Next

In Citrix Secure Internet Access, there are three different SKUs available –Standard, Advanced, and Premium.

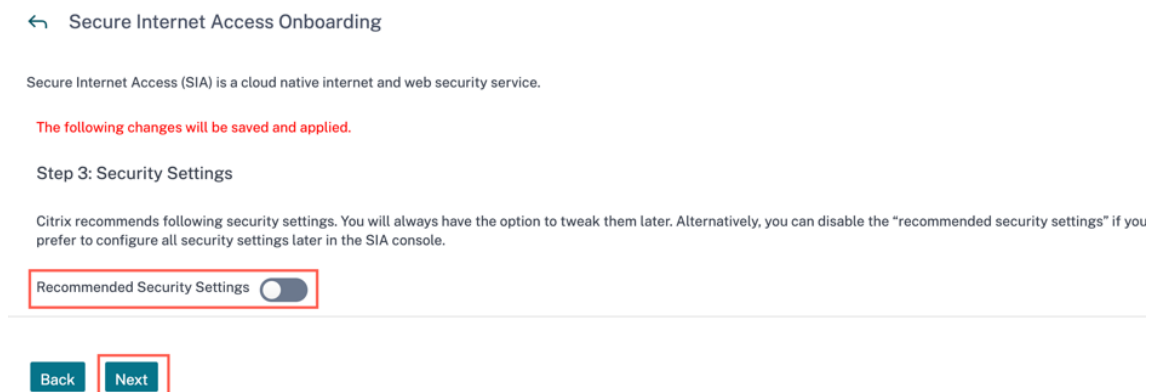
In Citrix Secure Internet Access GUI:

- The **Malware Defense and Intrusion Prevention settings** option is only available for the customers who have Advanced and Premium SKUs.
- The **Data Loss Prevention (DLP)** option is only available for the customers who have Premium SKUs.

For Standard plan, the **Malware Defense and Intrusion Prevention settings** and **Data Loss Prevention (DLP)** options are not available in Citrix Secure Internet Access UI.

By default all the options are pre-checked for both **Malware Defense and Intrusion Prevention settings** and **Data Loss Prevention (DLP)**. You can reset the settings or select the options as needed. Click **Next**.

Alternatively, if you want to skip the **Security Settings** configuration, you can disable the **Recommended Security Settings** button. You can configure the settings later in CSIA console.



In this scenario, click **Next** and review the settings that you made and click **Finish** to save the changes.

4. You can view the summary page with all your settings that you set to complete the onboarding process.

←

Secure Internet Access Onboarding

Secure Internet Access (SIA) is a cloud native internet and web security service.

Step 4: Summary View

Following changes have been applied. Please review if you would like to make any change.

You may click on Back button to navigate through these steps and make changes as needed.

Proxy Settings

Enable Proxy Settings :	Enabled
User Authentication Method :	Local User Credentials + Cloud Connections
Enable Proxy SSL Decryption :	Enabled
Bypass WebSockets :	Yes
Bypass Citrix (and Iboss) domains :	Default List
Bypass Microsoft domains :	Yes
Bypass custom domains :	0

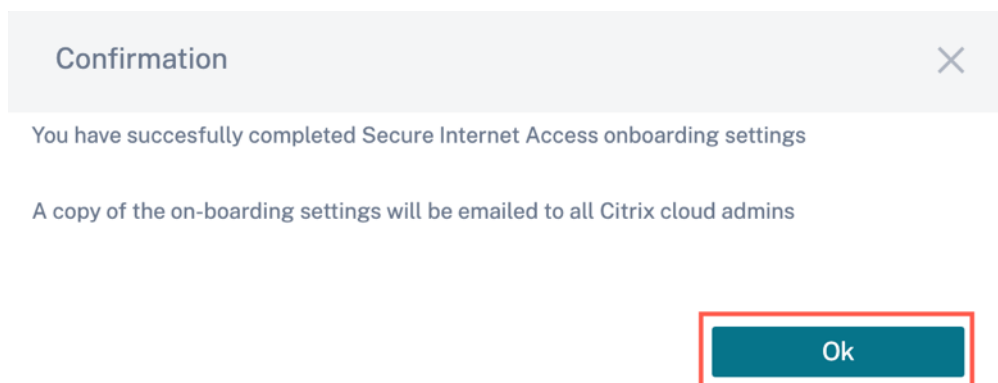
Cloud Connector Settings

Use HTTPS PAC :	Yes
Register over SSL :	Yes
Configure auto login :	All
Redirect all ports :	Yes
Bypass private subnets :	Yes
Multi user mode :	Disabled
Windows desktop app :	Disabled

Back

Finish

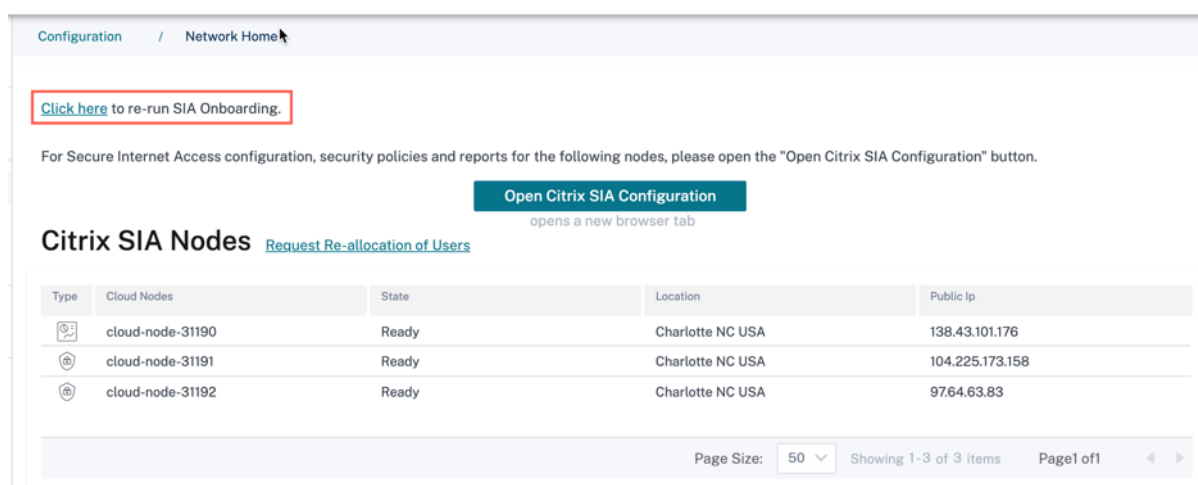
Click **Finish**, a popup is shown to confirm that you have successfully completed the onboarding settings. Click **OK**.



Also, an email is sent to all Citrix Cloud administrators who have been added under this customer account for Citrix Internet Secure Access service.

Once the onboarding is completed, navigate to **Configuration > Network Configuration Home > Open Citrix SIA Configuration** > select **Connect Device to Cloud**. In this page, you can follow the instruction to download/install Cloud Connector matching to the end-device OS.

You can rerun the onboarding process from **Configuration > Network Configuration Home** page. If you missed out any settings, you can always go back and rerun the onboarding process to restore default/recommended settings.



What's next?

- View the status of the nodes in your network. See [Dashboard](#).
- View details about your subscribed license entitlements. See [View licensing details](#).
- Configure CSIA Cloud Connector agents on Virtual Delivery Agents (VDA) and local host systems. See [Configure Citrix Secure Internet Access Cloud Connector agents](#).
- Configure tunnels for your branch office if you also have a Citrix SD-WAN deployment. See [Configure tunnels for branch office](#).

- Use the Citrix Secure Internet Access configuration policy portal to configure cloud connectors and security features and to monitor reports and logs. See [Configuration](#).

Licensing

February 3, 2021

Citrix Secure Internet Access (CSIA) is available in three editions.

- **Standard:** Cloud-based security solution that provides centralized management and administration in the cloud. It includes core security features such as web and internet content filtering, SSL traffic management, and CASB.
- **Advanced:** Complete security solution with added security offerings such as malware prevention and breach detection, command and control callback detection, and incident response.
- **Premium:** Comprehensive security solution that includes advanced sensitive content detection and advanced content analysis engine.

For a complete list of the features available in an edition, see the feature matrix on <https://www.citrix.com/>.

Each of these editions includes the following:

- 500 GB of storage space
- One IPSEC or GRE tunnel for every 10 users in an account

You can purchase more storage space or tunnels.

After your [onboarding](#) process is complete, you can get insight into your subscribed license and usage details.

View licensing details

View details about your subscribed license entitlements by navigating to **Administration > Licensing**.

You can view the following information on the **Secure Internet Access Entitlements** tab:

- Subscription type and the list of features enabled for your subscription.
- Storage capacity included in your subscription package. By default, each subscription includes 500 GB of storage space.
- Number of tunnels included with your subscription package. By default, each subscription includes one tunnel for every 10 users in an account.

- License term and its expiration date
- Number of users added to this subscription
- Status of your entitlement

SD-WAN Entitlements

Secure Internet Access Entitlements

Secure Internet Access Entitlements

Subscription Type : DLP Package

Storage Included : 500.00 GB

Term : 1 Years

Number of Users : 0

Tunnels Included : 1

Expiration Date : Mon Mar 08 2021

Status : Active

Status	Type	Name
Enabled	Feature	Advanced Malware Defense
Enabled	Feature	Intrusion Prevention
Enabled	Feature	Bandwidth Optimization
Enabled	Feature	Dataloss Prevention
Enabled	Feature	CASB
Enabled	Platform	Web Gateway Nodes
Enabled	Platform	Reporting Nodes
Enabled	Platform	Premium Enabled

You can also view details about any additional storage space or tunnels that you have purchased.

Secure Internet Access Add-On - IPSec Tunnels			
IPsec tunnels	5	Term	2 years
Status	Active	Expiration date	1 Jan, 2023
Secure Internet Access Add-On - Storage Capacity			
Type	3 TB	Term	2 years
Status	Active	Expiration date	1 Jan, 2023

Note

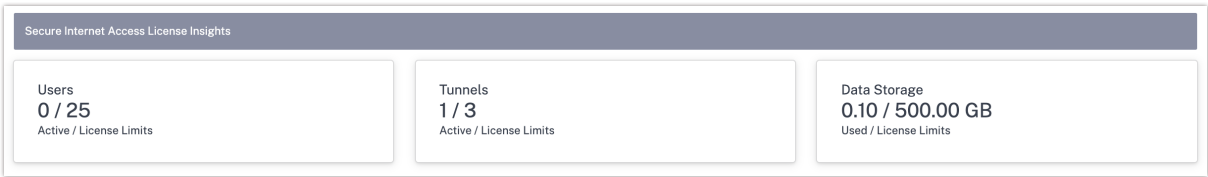
If you also have a Citrix SD-WAN entitlement, you can view the SD-WAN license details on the SD-WAN tab. For information about SD-WAN licensing, see SD-WAN Orchestrator [Licensing](#).

License usage insights

You can get insights into license usage by navigating to **Administration > License Usage Insights**.

View the total number of user licenses you have and the number of active user licenses. You can also view the number of total and active licenses for data storage and tunnels.

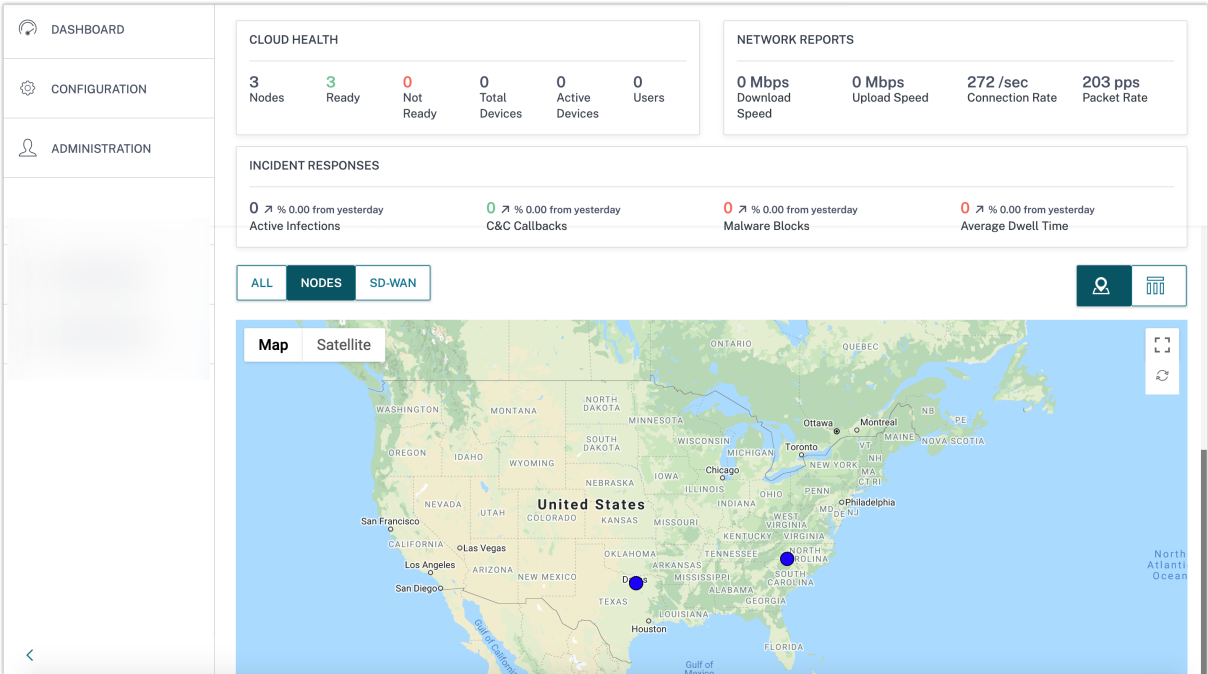
These insights help you decide whether you need more user licenses, storage capacity, or tunnels.



Dashboard

September 15, 2021

The Dashboard, as shown in the following image, provides a high-level view of the performance of your Citrix Secure Internet Access (CSIA) network.



The **Dashboard** includes four main sections: **cloud health**, **network reports**, **incident responses**, and a **map view** of the network.

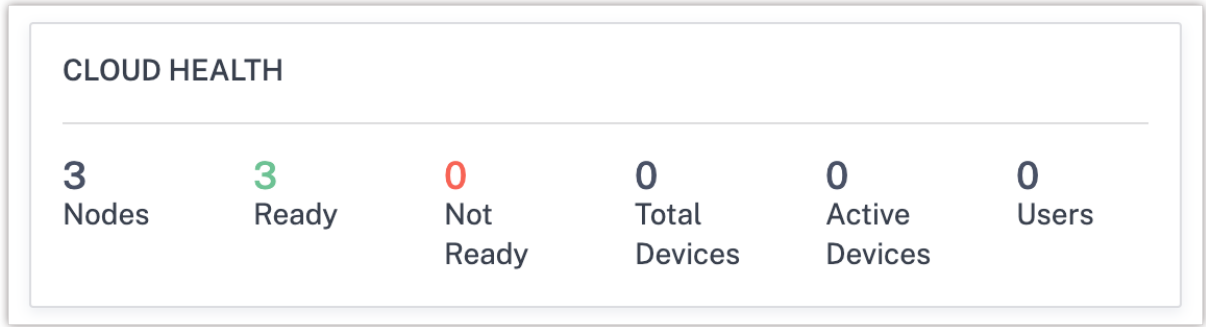
You can access more detailed reports on the **Reports & Analytics** page. To do so, navigate to **Configuration > Open Citrix SIA Configuration**.

Cloud health

This section gives you the status of the nodes in your network. View the total number of nodes that were configured for you. Also, view how many of those nodes are ready and how many are not ready.

A node that is **Not Ready** is not working or not provisioned, indicating a problem that you need to investigate or report so it can be fixed.

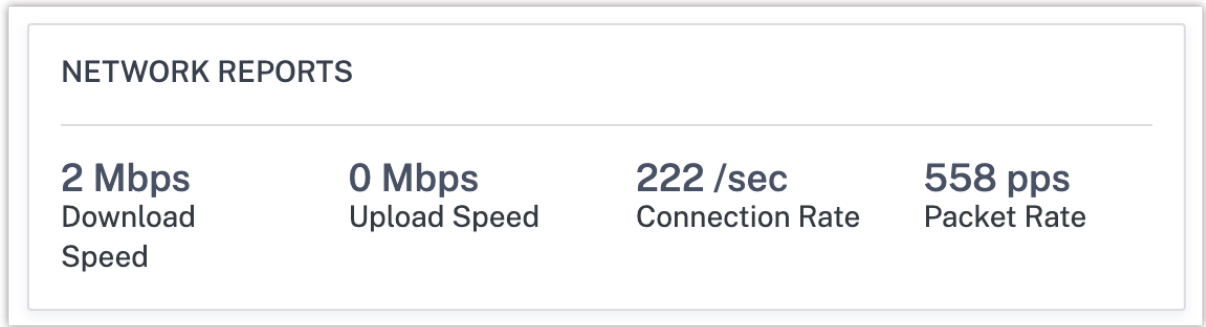
The **cloud health** section also provides insights into the total number of devices that are connected to the nodes and the number of active devices. It also allows you to track the number of users that are connected to the network.



Network reports

This section provides an overview of the real-time activity on your network. It lists the bandwidth usage such as download speed and upload speed for all connected devices. This section also provides insight into the rate of connections and packets used across the network.

Together, this information can tell you whether there might be a network issue that needs to be dealt with.



Incident responses

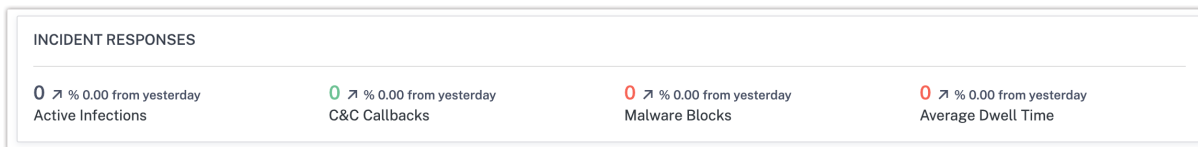
This section provides a high-level view of the infected devices in your network and that you need to investigate or report.

This section lists the following security data:

- the number of currently active infections in the network
- the number of Command and Control (C&C) callbacks

- the total number of malware that has been blocked from entering the network
- the average dwell-time of infections across the network.

This section also shows the percentage by which each of these incidents have increased since the previous day.



Notifications

Important updates relevant to your subscription to the Citrix Secure Internet Access service are sent to you as notifications in the Dashboard. Notifications include, but are not limited to:

- Information about license expiration
- Release notes of new builds
- URL review requests
- Alerts and advisories

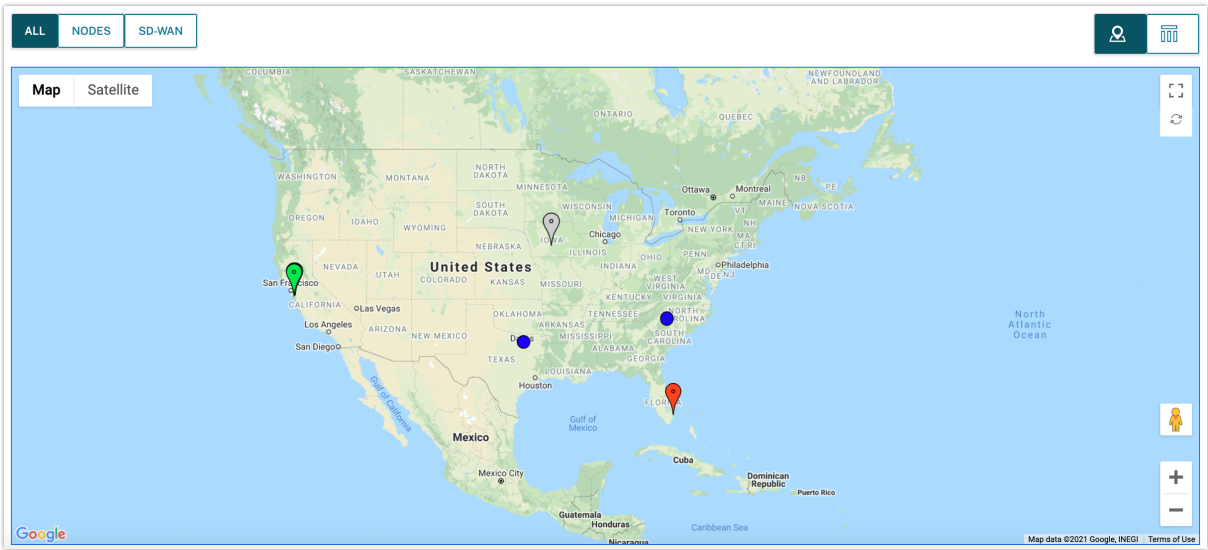
Citrix informs you that you have notifications with a number on the bell icon. You can find the bell icon in the top right of the Dashboard. You can expand the notification view by selecting the bell icon. These notifications are displayed only in the bell icon and not sent by email.

Map view

The map view shows the geographical locations of the cloud and gateway nodes of your Citrix Secure Internet Access deployment. The blue dots represent nodes on the map.

If you have an SD-WAN entitlement, you can see the geo locations of your SD-WAN sites. The sites are indicated in green, red, or gray on the map.

You can limit this view to Citrix Secure Internet Access nodes by selecting the **Nodes** tab or to SD-WAN sites by selecting the **SD-WAN** tab.



To view this information in a tabular format, select the table view icon to the far right, directly above the map. To switch back to the map view, select the map view icon located to the left of the table view icon.

Type	Cloud Nodes	State	Location	Public Ip
	cloud-node-31190	Ready	Charlotte NC USA	
	cloud-node-31191	Ready	Allen TX USA	
	cloud-node-31192	Ready	Charlotte NC USA	

Configuration

December 2, 2021

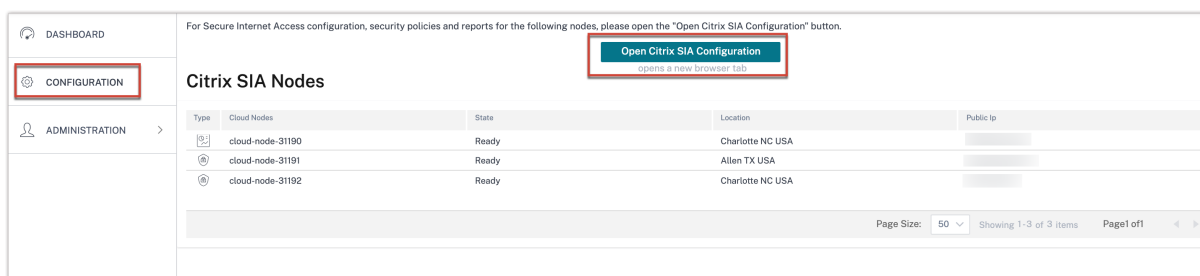
Use the Citrix Secure Internet Access (CSIA) configuration policy portal to configure cloud connectors and security policies, and to monitor reports and logs.

To access the configuration policy portal:

1. Sign in to Citrix Cloud
2. On the **Secure Internet Access** tile, select **Manage**
3. In the navigation pane, select **Configuration**

The Configuration page also lists the details about the cloud nodes that have been configured for you. All the configurations that you perform are connected to these nodes.

4. Select **Open Citrix SIA Configuration** to view the configuration policy portal and start configuring the features and security policies



How to get help on configuration

For instructions on configuration or help with any configuration page, you can do one of the following:

- **Access help documentation.** On the top right corner of the configuration policy portal, click the menu (where your name appears) and select **HelpDocs**. You can view the complete help documentation.

Note

The help documentation includes references to iboss terminology, iboss user interface elements, iboss features not supported by Citrix, and iboss Support information.

Review the following article before using the help documentation: [Citrix Secure Internet Access and iboss integration](#). You can access this article only after signing in to Citrix Secure Internet Access.

- **Access contextual help.** At the top right corner of each configuration page, select the **help icon (?)** to view the help documentation pertaining to that page.
- **Contact Citrix Support.** Sign in with your Citrix account and open a support case, start a live chat, or explore other options available for receiving help.

Configure Citrix Secure Internet Access Cloud Connector agents

The CSIA Cloud Connector agents are software agents that redirect Internet traffic through Citrix Secure Internet Access.

After your onboarding process is complete, do the following:

- **Install CSIA Cloud Connector agent on Virtual Delivery Agent (VDA):** To securely access unsanctioned web and SaaS applications from virtual desktops on Citrix Workspace, configure CSIA Cloud Connector agents to redirect traffic through Citrix Secure Internet Access.

For detailed configuration steps, see [Citrix Secure Internet Access with Citrix Virtual Apps and Desktops](#).

- **Install CSIA Cloud Connector agent on your host device:** To securely access direct Internet traffic from your host systems such as laptop and mobile devices, install Cloud Connector agents on each device.

Configure tunnels for branch office

If you have a Citrix SD-WAN deployment in your branch office, you must configure IPSEC or GRE tunnels. This redirects branch traffic to unsanctioned web and SaaS applications through Citrix Secure Internet Access. You use Citrix SD-WAN Orchestrator to configure tunnels.

On Citrix SD-WAN Orchestrator, the Citrix Secure Internet Access service is available in **Configuration > Delivery Services > Service and Bandwidth**.

Note

The service link is only visible if you are an SD-WAN Orchestrator customer and have Citrix Secure Internet Access entitlement.

Delivery Services		Global Service Bandwidth Defaults for each Link type		
		Internet Links	MPLS Links	Private Intranet Links
Virtual Path		30 %	100 %	100 %
Internet		25 %	0 %	0 %
Secure Internet Access Service		35 %	0 %	0 %
Cloud Direct Service		0 %	0 %	0 %
Intranet + Service		10 %	0 %	0 %
1. Zscaler		10 %	0 %	0 %
2. Azure Virtual WAN		0 %	0 %	0 %
3. AWS Gateway Service		0 %	0 %	0 %
4. Non_SDWAN_Sites		0 %	0 %	0 %

[Save](#)

The configuration includes the following high-level steps:

1. Create a Citrix Secure Internet Access service by specifying the bandwidth percentage and provisioning percentage for the Internet Links.
2. Add and map SD-WAN sites to the Citrix Secure Internet Access service and select the appropriate tunnel (IPSEC or GRE). Then, activate the configuration to enable tunnel establishment between Citrix SD-WAN and the Citrix Secure Internet Access PoP.

3. Create application routes to steer traffic through the tunnels.

For detailed instructions, see [Delivery services - Citrix Secure Internet Access service](#).

User reallocation

You can minimize latency for users in particular locations by redistributing cloud nodes within a geographical region.

You can make a request to redistribute both reporting nodes that collect usage data and gateway nodes that perform security functions. Citrix aims to deliver nodes closest to users based on node availability.

Important

Reallocation of nodes causes a brief disruption in the service. The operation is typically performed immediately after account activation, before client connectors are configured and distributed. Citrix recommends that you request reallocation of nodes at the beginning of the deployment to realign the nodes closest to users, and to reallocate nodes infrequently.

You can also move users between nodes or add them to a node if they aren't already allocated to a node.

Request Re-allocation of Users

Licensed User Count

Region	Licensed User Count *
NAWE	25

Existing Regions & Locations

Reporting Node

Reporting Node	Location
cloud-node-31190	Charlotte NC USA
Nearest Preferred Location	<div>San Jose, CA, USA</div>

Gateway Nodes

Please provide us with the number of users you currently support for each region below.

Region	Location	# of Users *
North America + Western Europe	Allen TX USA	<div></div>
North America + Western Europe	Charlotte NC USA	<div></div>

Region *

City *

State

Country *

of Users *

X

NAWE

San Jose

CA

USA

25

[Add Another Location](#)

Submit Request

Cancel

To view, redistribute, and maintain nodes, navigate to the **Configuration** tab in the left side menu and select **Request re-allocation of users** above the table.

Note

You can only redistribute nodes within the same geographical region.

Cloud Settings

To configure settings for your Network Time Protocol (NTP) server, platform maintenance, and update releases, navigate to the **Configuration** tab and select **Cloud Settings**.

Account Settings

The **Account Settings** feature helps to change/override the user account name that appears for your account in the Citrix Secure Internet Access service portal.

To override account name, navigate to **Configuration > Cloud Settings > Account Settings**.

You can view the Citrix Secure Internet Access Account number.

Account Settings:

Account Number : 139898



Override Account Name

Account Name *

Save

Note

The initially configured account name is still present in the CSIA portal if you have not created any name or the **Override Account Name** is disabled.

1. Enable the **Override Account Name** and provide a name. By default the **Override Account Name** is disabled.

Account Settings:

Account Number : 139898

☒ Override Account Name

Account Name *

Save

Wait for some time to view the updated account name on the portal. You might have to relogin once the account name is changed.

2. Click **Save**.

NTP Server

To synchronize the date and time, navigate to **NTP Server** under **Cloud Settings**. Enter the time zone, the date format, the address of the NTP server, and daylight savings information.

Time Zone defines the regional standard time used for timestamps. After changing the time zone, the timestamps for events in reports will shift to align with the new time zone and maintain continuity. Timestamps are relative to the new time zone.

Date Format defines the structure of the date in numerical form. This parameter can be set to either **mm/dd/yyyy** or **dd/mm/yyyy**.

NTP Server defines the address of the NTP server.

Daylight Savings defines whether time zone adheres to daylight saving. This parameter can be set to either **United States** or **United Kingdom** depending on the time zone region.

Platform Maintenance

This functionality allows you to schedule the days and times that maintenance occurs to help ensure that your network is available during peak times.

To schedule automatic maintenance performed on your behalf, navigate to **Platform Maintenance** under **Cloud Settings**, and enable **Preferred Maintenance Window**. Then select your preferred dates and times for automatic maintenance.

Update Release Settings

To choose the types of updates that are installed on your behalf, navigate to **Update Release Settings** under **Cloud Settings**, and select one of the following release levels:

- **Mandatory**, for critical platform updates and security fixes, including new features, feature updates, bug fixes, and performance enhancements.
- **Optional**, for releases that are recommended but don't include critical fixes.
- **Early Access**, for early access to new features, updates, bug fixes, and performance enhancements.

Email Settings

You can configure email server settings to relay emails containing alerts, scheduled reports, and other notifications. To allow web gateways and reporting nodes to send out email notifications, complete the form in **Email Settings** under **Cloud Settings**. This process involves configuring the SMTP Server Address so that you can receive email notifications.

You can verify the email settings using the **Test Email Settings** option. You can also populate the default email settings using the **Set Default Settings** button.

Configure email addresses to receive User Alerts and URL Exception requests.

- **Alert Email**: The destination address for alerts that are triggered by high-risk keywords.
- **URL Exception Email**: The destination address for URL exception requests sent from block pages.

Note

Additional email alerts are available from the **Real-Time Alerts** page.

Email Settings:

Set Default Settings

Email Server Settings

From Address

CitrixSIA_DefaultReply@phantom.com

SMTP Server Address

mail.iphantom.com

Port

25

Authentication Type

Plain Text

Username

Password

Test Email

Test Email Settings

Save

Recipient Settings

Alert Email

Dhegn.Singh@citrix.com

URL Exception Email

Dhegn.Singh@citrix.com

Save

Note:

Typically, SMTP servers are configured with IP-based allow lists to prevent spam. You must therefore add the IP addresses of all nodes to the SMTP server’s allow list.

Also to reduce spam, SMTP servers sometimes use other mechanisms, such as DKIM. It might be necessary to exempt web gateways and reporting nodes from these restrictions on the SMTP server.

If you don’t have your own internal SMTP server, you can use one of Google’s SMTP services. You must have a valid Gmail account for this.

Google SMTP servers use ports 25, 465, 587, or a combination of these. The most popular is **smtp.gmail.com**, which uses ports 465 (with SSL) or 587 (with TLS).

Note:

SMTP servers commonly listen on TCP ports 25, 465, or 587, but can listen to any port that they're configured to operate on. SMTP over SSL uses port 465 and SMTP over TLS uses port 587. Both ports 465 and 587 require authentication services. Port 25 is unencrypted and requires no authentication.

When working with local web gateways or reporting nodes, ensure that the required ports aren't restricted.

The configurations for each of the three Google SMTP servers are as follows:

Fully qualified domain name	Configuration requirements	Authentication requirements
smtp-relay.gmail.com	Port 25, 465, or 587, with either Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols, and one or more static IP addresses.	IP address.
smtp.gmail.com	Port 465 with SSL or port 587 with TLS. Dynamic IPs are allowed.	Your full Gmail or G Suite email address.
aspmx.l.google.com	Mail can only be sent to Gmail or G Suite users. Dynamic IPs are allowed.	None.

smtp-relay.gmail.com is used to send mail from your organization by authenticating with the associated IP addresses. You can send messages to anyone inside or outside of your domain using port 25, 465, or 587.

smtp.gmail.com is used to send mail to anyone inside or outside of your domain. It requires you to authenticate with your Gmail or G Suite account and password. You can use SMTP over SSL (port 465) or TLS (port 587).

aspmx.l.google.com is used to send messages to Gmail or G Suite users only. This option doesn't require authentication. You can't use SSL or TLS with this SMTP server, and so the traffic is in Plain Text, which isn't recommended.

Anonymized Logging

For regulatory compliance and confidentiality, **Anonymized Logging** under **Cloud Settings** encrypts the personal user information that delegated administrators use to monitor network usage.

You must create an encryption key before you enable **Anonymized Logging** by selecting the **Add Key** button under the **Enable Anonymized Logging** toggle. Enter a 64-character value for the encryption key into the **Encryption Key** field. You can enter your own encryption key or use the **Auto Generate Key** option.

Important:

Citrix highly recommends that you record the encryption key in a separate location before continuing. You need the encryption key to decrypt the data associated with it for as long as it is active on the platform.

You can configure a key to encrypt the identifiable data of a particular category by enabling the following toggles under **Encrypt Categories**:

- **Personal Information.** Enables and disables the encryption of all personally identifiable information, including the user name, full name, and machine name of reported user activity.
- **Data Source.** Enables and disables the encryption of all information relating to the data source of reported user activity.
- **Group Names.** Enables and disables the encryption of the group names that are associated with reported user activity.

You can also configure encryption keys to apply only to a particular set of groups in the **Group Association** tab. When the **Select All** toggle is enabled, the currently configured encryption key applies to all security groups. When the **Select All** toggle is disabled, you can select which security groups to encrypt with the encryption key.

After configuring an encryption key, enable **Anonymized Logging** to monitor network usage based on the anonymized logs of user online activity.

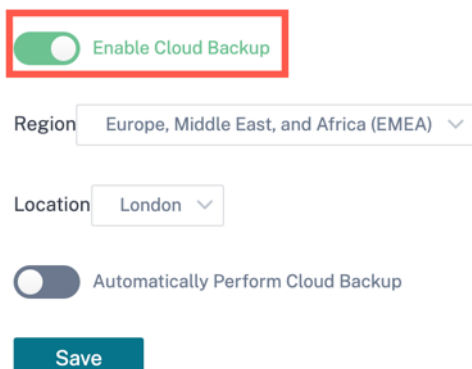
To delete a previously defined encryption key, select the ellipses next to the corresponding encryption key in the table, and select **Delete**.

Cloud Backup

The **Offline Cloud Backup** settings provide the ability to store/save the backup settings and logs from reporting nodes based on the **Region**, **Location**, and **Time** that you select. With the **Offline Cloud Backup** option, you can save the cloud backups through CSIA interface.

To enable the cloud backup settings, navigate to **Configuration > expand Cloud Settings > select Cloud Backup**.

1. Enable the **Enable Cloud Backup** toggle button and select the **Region** and **Location** from the drop-down list.

Offline Cloud Backup:

☒ Enable Cloud Backup

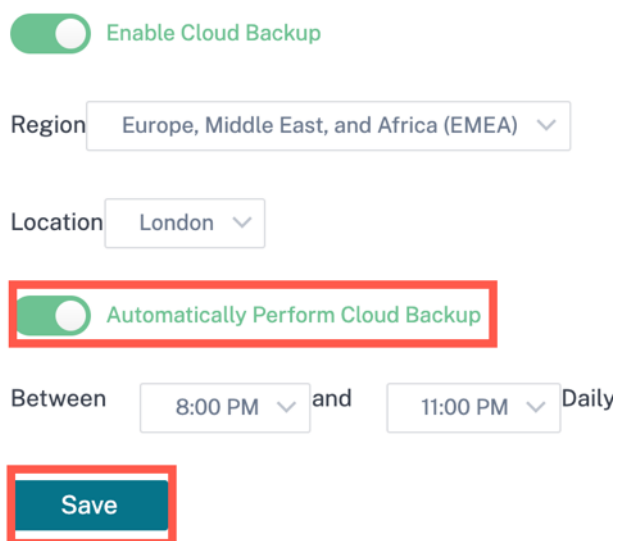
Region Europe, Middle East, and Africa (EMEA) ▾

Location London ▾

☐ Automatically Perform Cloud Backup

Save

2. You can also enable the **Automatically Perform Cloud Backup** toggle button and set the time interval to run and create the daily backup. Click **Save**.

Offline Cloud Backup:

☒ Enable Cloud Backup

Region Europe, Middle East, and Africa (EMEA) ▾

Location London ▾

☒ Automatically Perform Cloud Backup

Between 8:00 PM ▾ and 11:00 PM ▾ Daily

Save

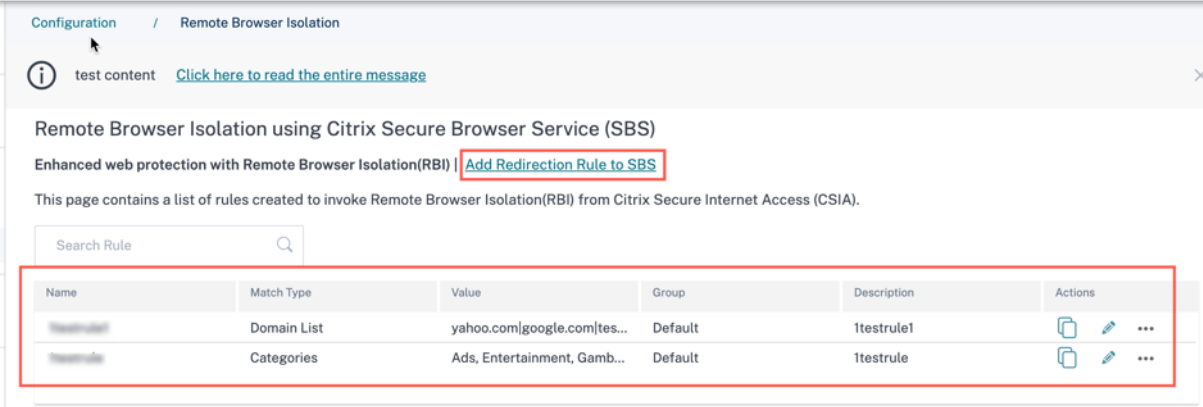
Remote Browser Isolation

Remote browser isolation is an advanced web protection feature that provides security from any malware/malicious threats. With the Remote browser isolation, Citrix Secure Internet Access Web filtering functionality can be used along with the Secure Browser Service (SBS) to protect the corporate network from browser-based attacks. For more information, see [Secure Browser service](#).

With the remote browser isolation feature, you can set rules for some targeted websites that are not trusted to be isolated and launched only through the remote cloud-based secure browser service. You

can create and apply the rule to a combination of user groups and type of traffic that you want to isolate.

You can view the list of rules created to invoke remote browser isolation.



To set the redirection rules for the traffic that needs to be invoked, navigate to **Configuration > Remote Browser Isolation > Click Add Redirection Rule to SBS.**

Add RBI Rule

Rule name

Rule description

Match type

Select match type

Value

Select group

Select group type

Cancel

Save

- **Rule name:** Provide a rule name.
- **Rule description:** Provide a rule description.
- **Match type:** Select a match type such as Domain Regex, Domain List, IP Address, URL, or Categories from the drop-down list.
- **Value:** Enter match value type.
- **Select group:** Select a group from the drop-down list.

With the **Add Redirection Rule to SBS** option, you can create the web filtering rules on the secure internet access portal to redirect the traffic to the browser service. For every remote browser isolation rule, there is a secure browser URL associated. That means, when the URLs launched through the secure internet access service, if the URL matches one of the defined remote browser isolation matching rules, the request is then redirected to the associated secure browser service.

Administration

September 9, 2021

An administrator's role defines the permissions to view features and perform various activities in the Citrix Secure Internet Access (CSIA) service.

The following features are included as part of the Citrix Secure Internet Access service:

- **Dashboard.** Access to top level reports.
- **Web Gateway.** Access to the Secure Web Gateway Service.
- **Reporting & Analytics.** Access to more detailed reports.
- **Locations & Geo Mapping.** Access to the geographical locations of cloud and gateway nodes.
- **Node Collection Management.** Access to the Node Collection Management feature.
- **Licensing.** Ability to fetch licensing details for the service.
- **User Management.** Ability to create custom roles and to assign custom roles to other administrators.

Role-based access control

As with Citrix SD-WAN Orchestrator, access to Citrix Secure Internet Access service resources is managed based on the roles assigned to individual administrators. There are four levels of access that can be assigned to an administrator user of the Citrix Secure Internet Access service: Customer-Master-Admin, Customer-Master-ReadOnly-Admin, Customer-No-Access, and Customer-Master-ReadOnly-Admin-Privacy-Mode.

- The **Customer-Master-Admin** level is a full access role that allows the administrator to do the following:
 - Manage all features of the Citrix Secure Internet Access service.
 - Add administrators to the service.
 - Delete administrators from the service.
 - Assign, edit, and delete roles within the customer network.
 - Create custom roles.

- The **Customer-Master-ReadOnly-Admin** level is a read-only role that allows the administrator only to view Citrix Secure Internet Access service features.
- The **Customer-No-Access** level denies access to all Citrix Secure Internet Access service features.
- The **Customer-Master-ReadOnly-Admin-Privacy-Mode** level grants read-only access to all Citrix Secure Internet Access service features except for **Licensing** and **User Settings**. Users with this role cannot view the list of other admin users in their account, assigned roles, or licensing related information.

Note:

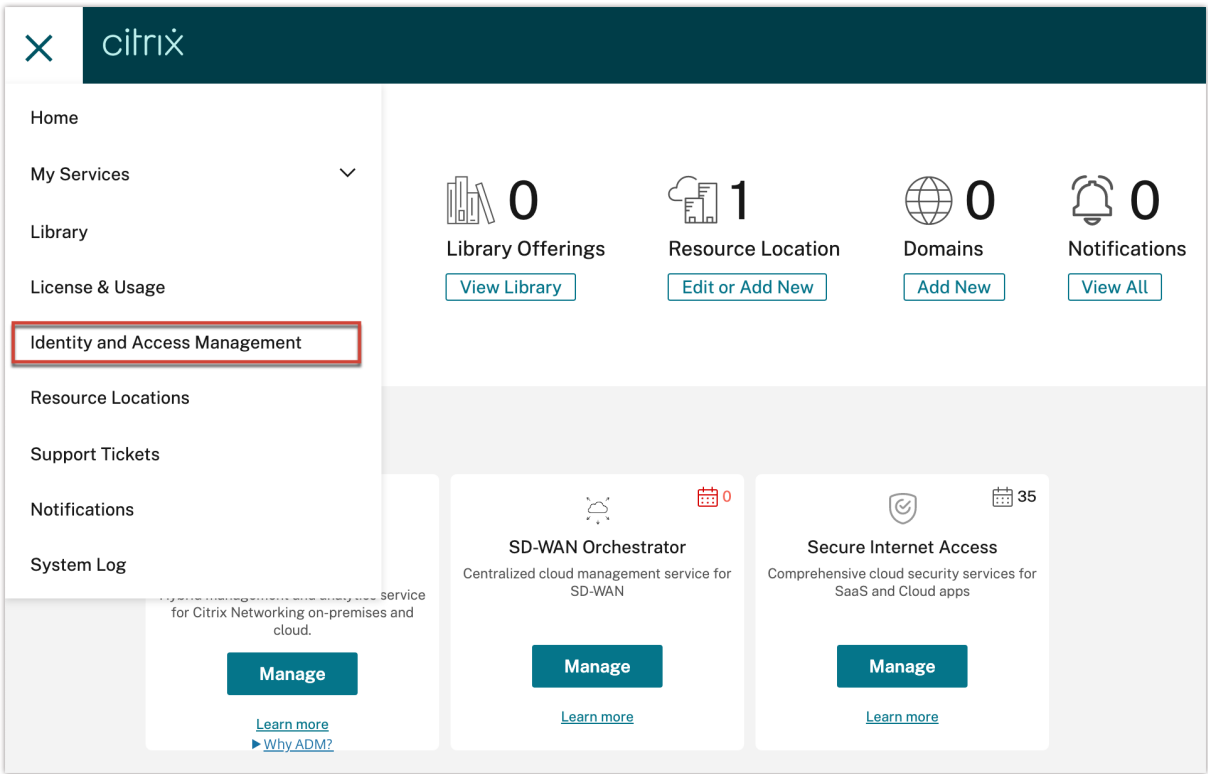
For the Citrix Secure Internet Access service, roles are assigned at the **Customer** level. For the Citrix SD-WAN Orchestrator service, roles are assigned at both the **Customer** level and at the **Provider** level. As a result, the Citrix SD-WAN Orchestrator service has both the **Customer-Master-Admin** role and the **Provider-Master-Admin-All** role available.

To apply RBAC, you first need to add users as administrators to Citrix Cloud services.

Add new users to Citrix Cloud services

You can add administrators to the Citrix Secure Internet Access service using the **Identity and Access Management** feature in Citrix Cloud. New administrators can use their existing Citrix account credentials or set up a new account if needed.

To add new administrators, select **Identity and Access Management** from the menu on the Citrix Cloud home page, and follow the prompts on the user interface. For more information, see [Manage Citrix Cloud administrators](#).

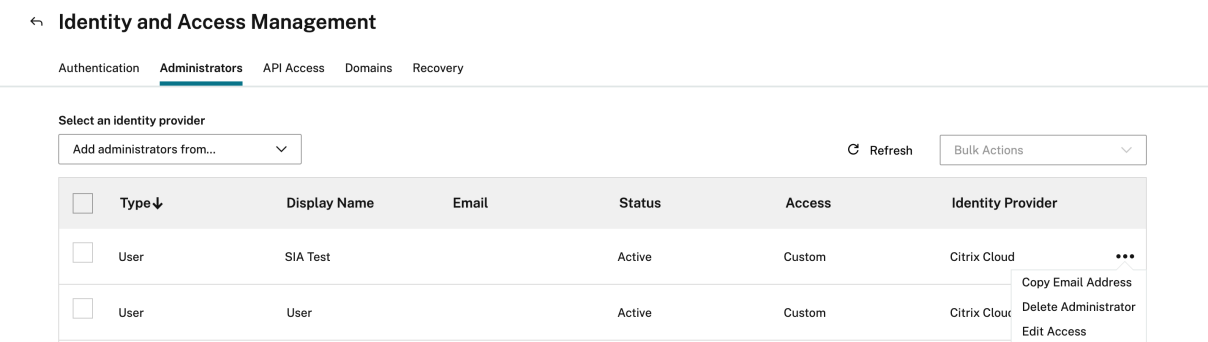


Any new administrator you add is automatically assigned full access to Citrix Cloud services. You can edit which parts of Citrix Cloud an administrator can view and manage on a more granular level.

Edit access for new users

Once you’ve added a new administrator through Citrix **Identity and Access Management**, you can set the role.

Select **Edit Access** from the list of actions against the account you created and choose either “Full access”(to Citrix Cloud services) or “Custom access”.



To grant full access to the Citrix Secure Internet Access service, with no customized selection of sub-features (under **Custom Access > General Management**), select the high-level **Full access** option.

Select **Custom access** if either or both of the following apply:

- You want to regulate access to subfeatures listed under **General Management**.
- You want to regulate the level of access to the Citrix Secure Internet Access service, specifically.

If you choose **Custom access**, you need to specify the level of access for **Secure Internet Access** separately from **General Management**. This access can be: full access, read-only access, read-only access (Privacy mode), or no access.

A user that is assigned **Customer Admin: Full Access** has the same access to the Citrix Secure Internet Access service as granted by the high-level **Full access** option (located above **Custom access**). Choose **Customer Admin: Full Access** to grant full access to Citrix Secure Internet Access service features while also choosing different levels of access to the subfeatures under **General Management**.

IMPORTANT

Choose **one** or **none** of the boxes under **Secure Internet Access**. If both boxes are selected, the highest level of permission is granted to the administrator, which poses a security risk.

A user that is assigned **Customer: Read Only Access** can only *view* the features of the service. A user that is assigned with **Customer: Read Only Access (Privacy mode)** has read-only access to view all the features of the service except for **Licensing** and **User Settings**.

If you select neither option, the user has no access to Citrix Secure Internet Access features.

Note

You can't edit an administrator's role in the Citrix Secure Internet Access service if they're denied access in **Identity and Access Management**. To view and edit an administrator in the Citrix Secure Internet Access service, you must grant them full or read-only access when you first add them.

SaveCancel

Full access

Full access allows administrators management control of Citrix Cloud and its services, as well as adding or removing other administrators.

Custom access

Switching to custom access will remove management access to certain services.

Custom access allows you to determine exactly which part of Citrix Cloud your administrators can manage.

[Select all](#) | [Deselect All](#)

General

No roles selected

>

SD-WAN

No roles selected

>

Secure Internet Access

1 of 3 roles selected

✓

Customer Admin: Full Access

Customer: Read Only Access

Customer: Read Only Access (Privacy mode)

IMPORTANT

All later changes to a user’s access must occur in the Citrix Secure Internet Access service user settings. Existing permissions for an administrator that are edited in **Identity and Access Management** aren’t sent to the Citrix Secure Internet Access service. In some cases, you might need to delete and reinvite the administrator.

Setting user roles

This section describes how you can further define and manage administrator access to features of the Citrix Secure Internet Access service.

Note:

Customers that have both a Citrix Secure Internet Access service subscription and a Citrix SD-WAN Orchestrator service subscription share **Administration > User Settings**.

To edit an existing user’s role as an administrator for the Citrix Secure Internet Access service, navigate to **Administration > User Settings**. You can assign roles from a list of predefined roles and a list of custom roles. Choose the appropriate role-based access from one of the menus, and then save your selection.

CUSTOMER
AMSHome102

Change Role

← Edit User

Network Administration: User

User settings are meant to enable the

Email
satest20@citrix.com
satest1@citrix.com

Email ID

☒ Predefined roles

Citrix SIA Access Level *

Customer-Master-Admin

☐ Custom role

Save Cancel

Predefined roles

There are four pre-defined roles at the **Customer** level that are available for the Citrix Secure Internet Access service:

- The **Customer-Master-Admin** role (default) allows the administrator to view and edit Citrix Secure Internet Access information.
- The **Customer-Master-ReadOnly-Admin** role allows the administrator to view Citrix Secure Internet Access information, with no editing permissions.
- The **Customer-No-Access** role denies the administrator access to Citrix Secure Internet Access service features.
- The **Customer-Master-ReadOnly-Admin-Privacy-Mode** level grants read-only access to all Citrix Secure Internet Access service features except for **Licensing** and **User Settings**. Users with this role cannot view the list of other admin users in their account, assigned roles, or licensing related information

← Edit User

Email ID

☒ Predefined roles

Citrix SIA Access Level ^{*}

Customer-Master-Admin

Customer-Master-Admin

Customer-Master-ReadOnly-Admin

Customer-No-Access

Customer-Master-ReadOnly-Admin-Privacy-Mode

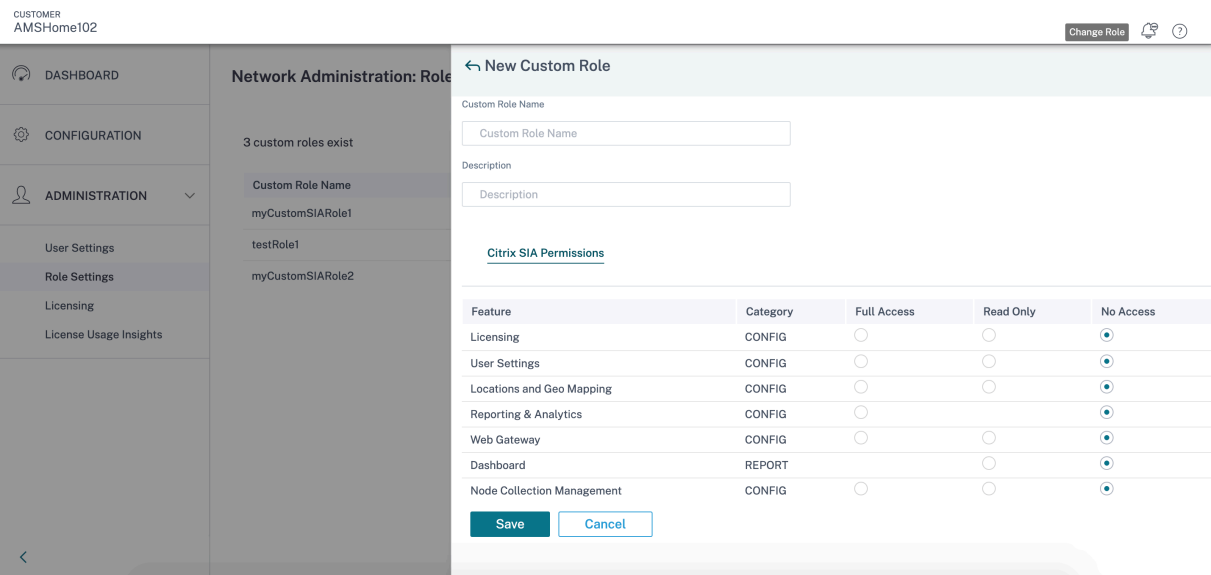
☐ Custom roles

Save

Cancel

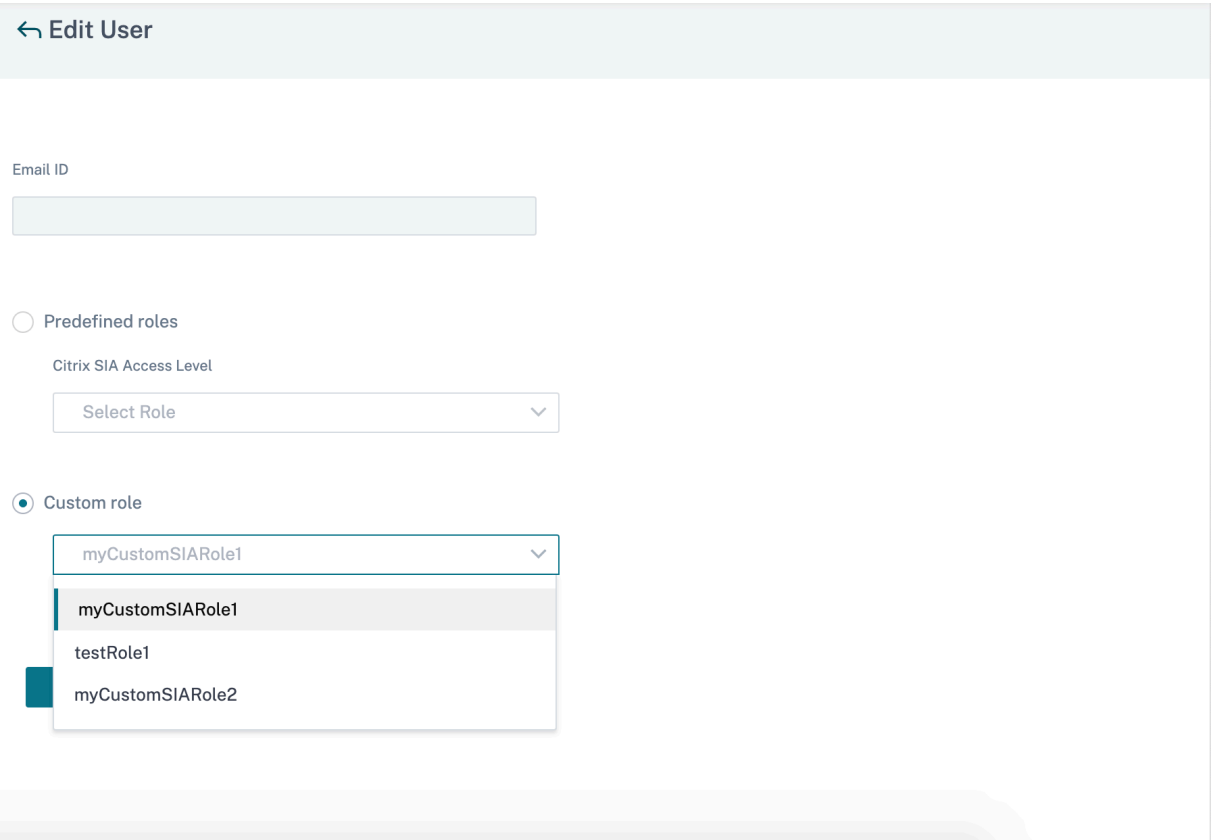
Custom roles

You can create custom roles based on varying permissions for individual features of the Citrix Secure Internet Access service.



To create a custom administrator role that can then be assigned to administrators, navigate to **Administration > Role Settings**. The **New Custom Role** form allows you to select different levels of access for individual features of the Citrix Secure Internet Access service.

Once you’ve created a custom role, it appears in the list of custom roles in **User Settings**.



Multiple roles

If a user is an administrator for more than one customer, they’re assigned multiple roles in the Citrix Secure Internet Access service and can switch between accounts. In such scenarios, the user can have a different role based each account.

To switch between roles, select **Change Role** at the top right of the screen, next to the bell icon.

View administrator details

You can view the roles and email addresses of all the administrators. To view administrator details navigate to **Administration > Administrators**.

Email	Role	Expiration date	
	Customer-Master-Admin	NA	—
	Customer-Master-Admin	NA	—
	Customer-Master-Admin	NA	—

Delete an administrator

To delete an administrator from the Citrix Secure Internet Access service, navigate to **Administration > Administrators**. Select the delete button against the account you want to delete, and then select **Save**.

	Customer-Master-Admin	NA	—
	Customer-Master-Admin	NA	—
	Customer-Master-Admin	NA	—
	Customer-Master-Admin	NA	—
	Customer-Master-Admin	NA	—

Save

Glossary

February 2, 2021

Citrix Cloud: Citrix Cloud is a platform that hosts and administers Citrix services. It connects to your resources through **connectors** on any cloud or infrastructure you choose (on-premises, public cloud, private cloud, or hybrid cloud). It allows you to create, manage, and deploy workspaces with apps and data to your end users from a single console.

Citrix SD-WAN: Citrix SD-WAN simplifies branch networking with a reliable and high-performance workspace experience that helps accessing SaaS applications, virtual desktops, or traditional data centers.

Citrix Secure Workspace Access: The Citrix Secure Workspace Access service enables the administrators to provide a cohesive experience integrating single sign-on, remote access, and content inspection into a single solution for end-to-end access control. With the Citrix Secure Workspace Access service, administrators can also protect the organization's network and end user devices from malware and data leaks by filtering access to specific websites and website categories.

Citrix Workspace: Citrix Workspace is a complete digital workspace solution that allows you to deliver secure access to the information, apps, and other content that are relevant to a person's role in your organization. Users subscribe to the services you make available and can access them from anywhere, on any device. Citrix Workspace helps you organize and automate the most important details your users need to collaborate, make better decisions, and focus fully on their work.

Citrix Workspace app: Citrix Workspace app gives users instant access to all their SaaS and web apps, their files and mobile apps, and their virtual apps and desktops from an easy-to-use, all-in-one interface. Citrix Workspace app is a single point of entry to all workspace services for users. Users get seamless and secure access to all the apps they need to stay productive, including features such as embedded browsing and single sign-on.

Virtual Delivery Agent (VDA): The VDA is a key component of Citrix Virtual Apps and Desktops. The VDA is installed on each physical or virtual machine in your site that you make available to users. The VDA enables the machine to register with the Controller, which in turn allows the machine and the resources it is hosting to be made available to users. VDAs establish and manage the connection between the machine and the user device. VDAs also verify that a Citrix license is available for the user or session, and apply policies that are configured for the session.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).
