Citrix Secure Private Access Hybrid Deployment

Contents

Citrix Secure Private Access hybrid deployment 3

What's new 4

System requirements and prerequisites 8

Cloud Connector for hybrid deployment 12

Setup and configure for hybrid deployment 16

Access the Secure Private Access admin console 17

Onboard and setup 17

StoreFront 21

Configure NetScaler Gateway 23

Update existing NetScaler Gateway configuration 26

NetScaler Gateway configuration for earlier versions 31

Contextual tags 35

Configure Web/SaaS applications 41

Configure TCP/UDP apps 44

Configure TCP/UDP - server to client apps 48

Configure access policies for the applications 51

Access restriction options 54

End user flow 72

Advanced features 75

Discover domains or IP addresses accessed by end users 76

Policy modeling tool 81

Unsanctioned websites 82

Upgrade 84

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Manage configurations **85**

Manage settings after installation **85**

Manage applications and policies **87**

Integration with DaaS monitor **89**

Basic troubleshooting **94**

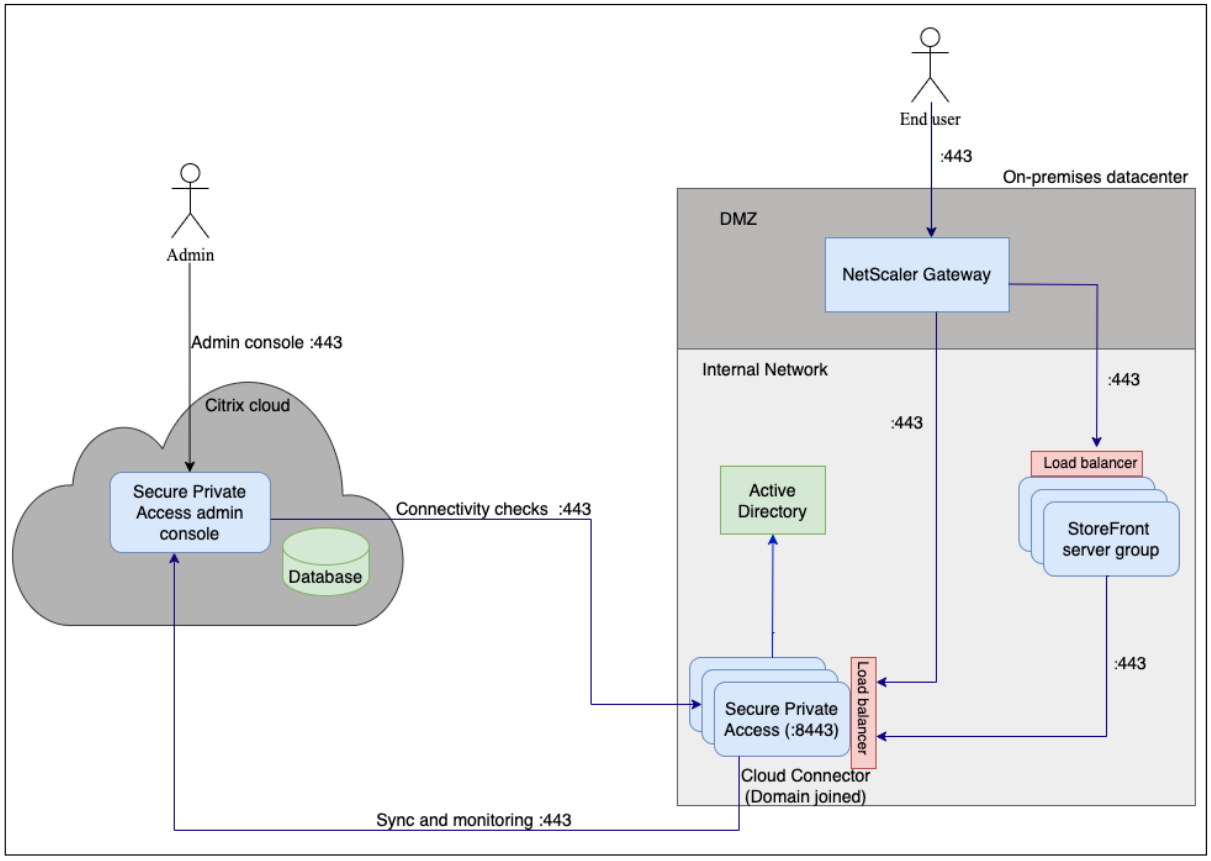
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Secure Private Access hybrid deployment

October 28, 2024

Citrix Secure Private Access for hybrid deployment allows customers to implement a Zero Trust Network Access (ZTNA) solution using on-premises StoreFront and NetScaler Gateway components and use the Citrix Cloud for managing the configuration, administration, and monitoring functions. This means customers can leverage existing NetScaler Gateway on-premises to control user traffic routing while using Citrix Cloud hosted UI for management of configurations and policies. Also, use Citrix Monitor hosted in the Citrix Cloud for monitoring and troubleshooting functions.

The key components of the Secure Private Access hybrid deployment are:



Cloud Connector: Pulls and caches all the configuration data, which allows app launches and access even when Citrix Cloud is unavailable. No user traffic is sent to the cloud. Cloud Connector is installed on a Windows server within your on-premises network. The Secure Private Access provider is part of the Cloud Connector. For details, see Cloud Connector for hybrid deployment.

StoreFront: Handles the enumeration and delivery of applications and desktops to the end users. StoreFront remains on-premises and you can continue to use your existing StoreFront setup without migrating to the cloud. For details, see StoreFront.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NetScaler Gateway: Provides secure remote access to applications and desktops. NetScaler Gateway remains on-premises, ensuring that users can securely connect to their resources from outside the corporate network. For details, see Configure NetScaler Gateway.

Secure Private Access admin console: Provides access to administrative and management functions, such as onboarding new users, configuring applications, and setting up policies. Site management tasks are centralized and administration is streamlined without requiring on-premises infrastructure for these functions. For details, see Access the Secure Private Access admin console.

> **Note:**
>
> For details on the system requirements and supported product versions for Secure Private Access hybrid deployment, see System requirements and prerequisites.

What's new

October 28, 2024

October 2024

Initial release

Citrix Secure Private Access for hybrid deployment allows customers to implement a Zero Trust Network Access (ZTNA) solution using on-premises StoreFront and NetScaler Gateway components and use the Citrix Cloud for managing the configuration, administration, and monitoring functions.

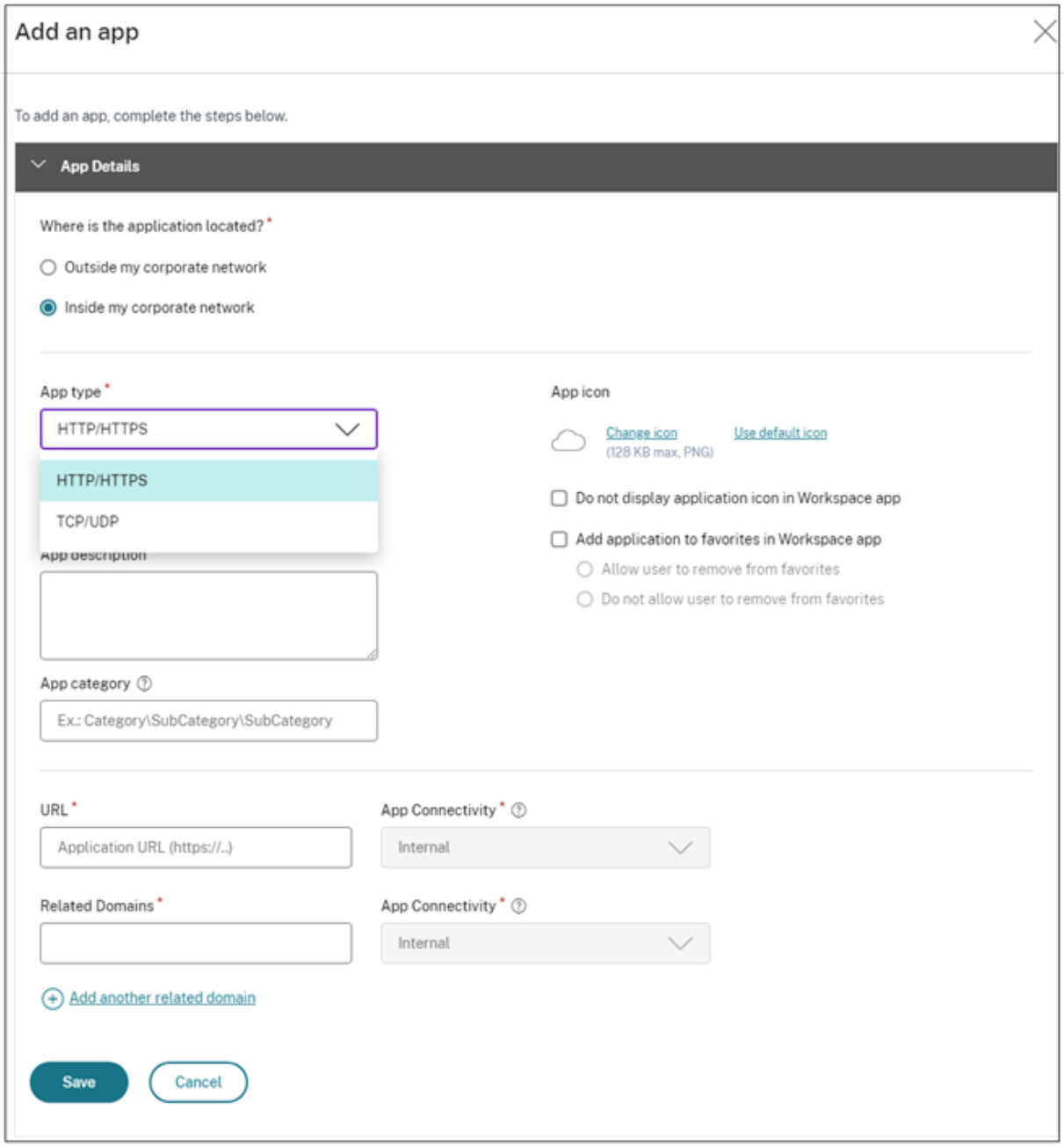
The following are some of the key features of the Citrix Secure Private Access for hybrid deployment.

- **Web/SaaS and TCP/UDP support:**

  Citrix Secure Private Access for hybrid deployment supports Web/SaaS and TCP/UDP apps. For details, see the following topics:

  - System requirements and prerequisites.
  - Configure Web/SaaS applications
  - Configure TCP/UDP apps

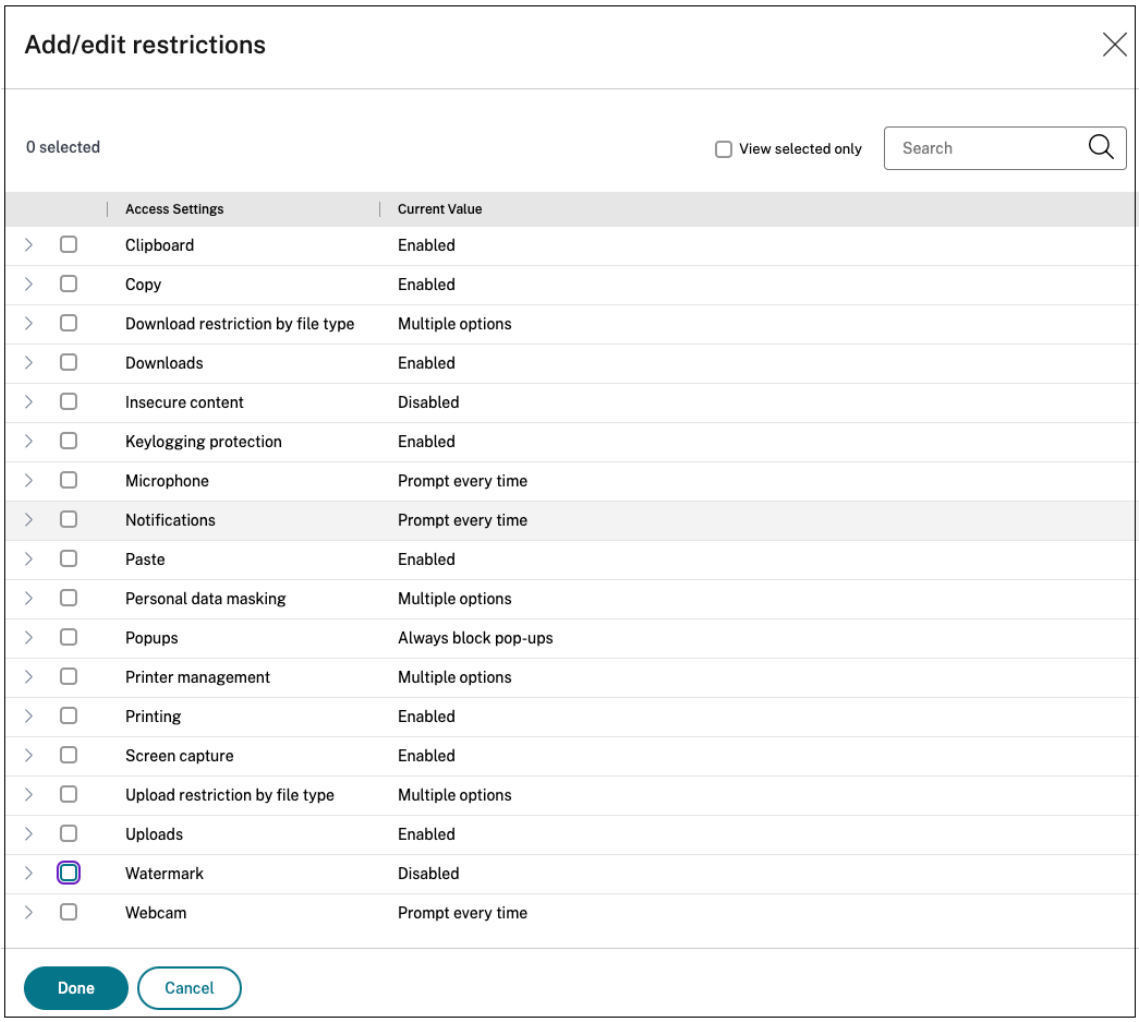
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Enhanced access restriction options:**

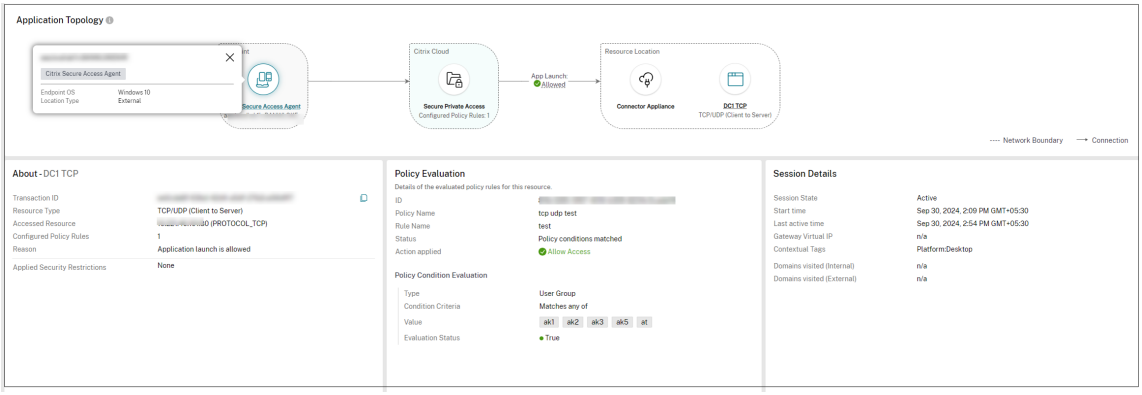
  While creating access policies for applications, you can select access restrictions that must be enforced on the applications. These security restrictions are predefined in the system. Admins cannot modify or add other combinations. For details, see Access restriction options.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

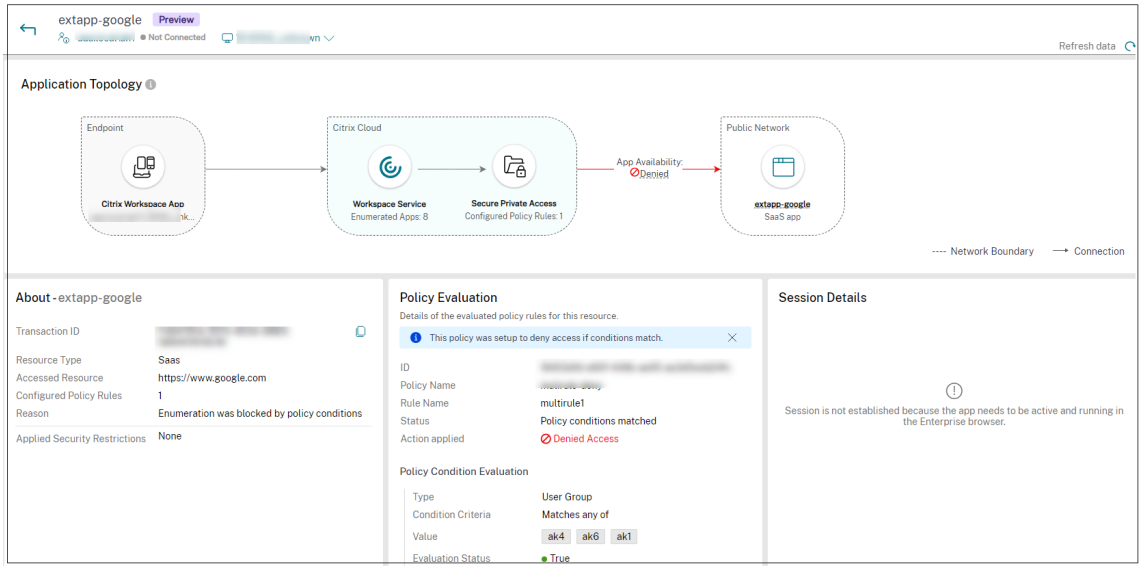


- **Secure Private Access integration with DaaS Monitor:**

  Secure Private Access is integrated with Monitor, the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can monitor and troubleshoot Web/SaaS and TCP/UDP app sessions and events from the DaaS Monitor. For details, see Secure Private Access integration with DaaS monitor.

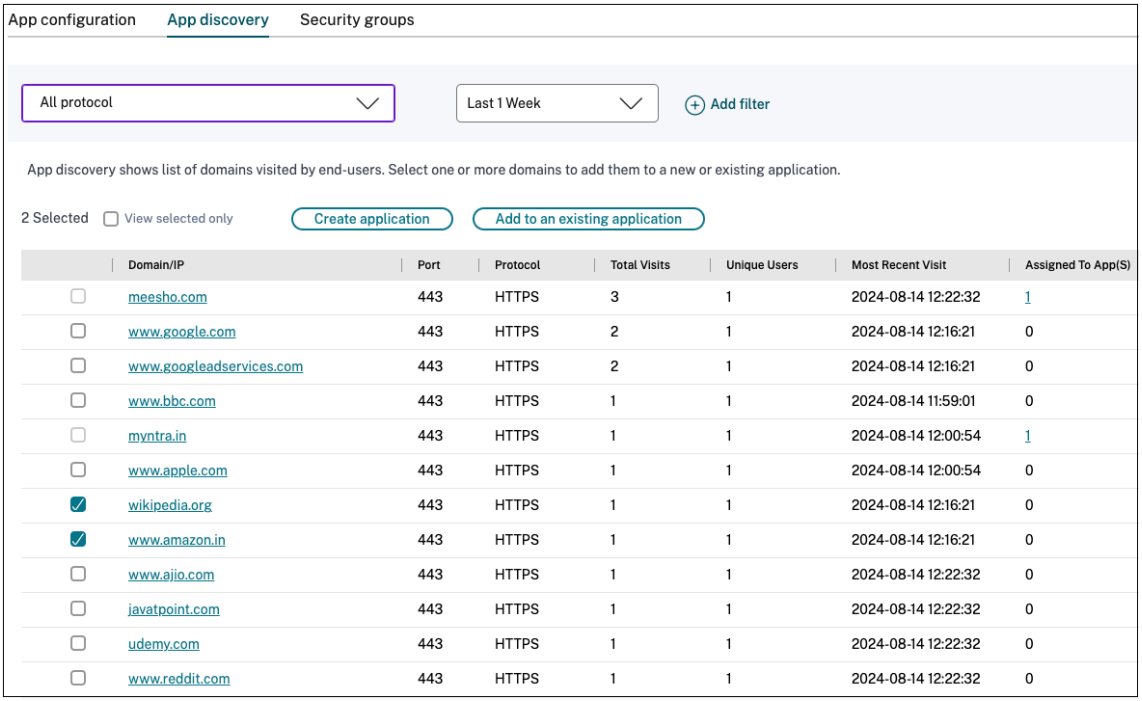


© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Application Discovery:**

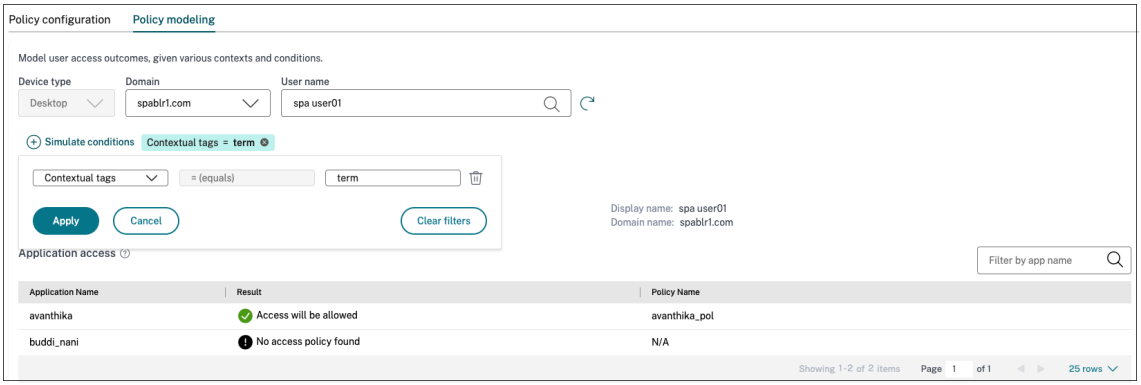
  The Application Discovery feature helps an admin get visibility into the external and internal applications (HTTP/HTTPS and TCP/UDP apps) that are being accessed in an organization. This feature discovers and lists all the domains/IPs addresses, published or unpublished. Thus, admins can see what domains/IP addresses are getting accessed, by whom, and decide if they want to publish them as applications, providing access to those users. For details, see Discover domains or IP addresses accessed by end users.



- **Policy modeling tool:**

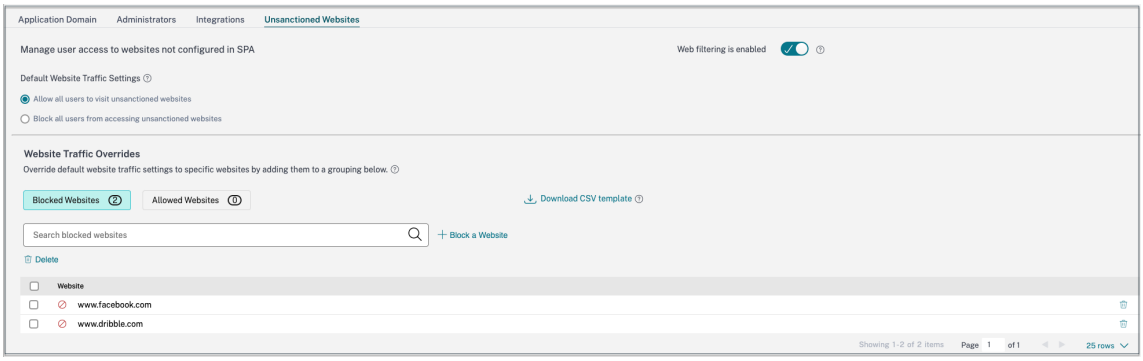
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

The policy modeling tool **(Access policies > Policy modeling**) provides the administrators full visibility into the expected application access result (allowed/allowed with restriction/denied). Admins can check the access results for specific users and add a user condition for contextual tags. For details, see Policy modeling tool.



- **Support for Unsanctioned websites:**

  Applications (intranet or internet) that are not configured within Secure Private Access are regarded as "Unsanctioned Websites". By default, Secure Private Access denies access to all intranet web applications if there are no applications and access policies configured for those applications. For all other internet URLs or SaaS applications that do not have an app configured, admins can use the **Settings > Unsanctioned Websites** tab from the admin console to allow or deny access via Citrix Enterprise Browser. For details, see Unsanctioned websites.



System requirements and prerequisites

October 28, 2024

Ensure that your product meets the minimal version requirements.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Product	Minimum version
Citrix Workspace app	Windows –2403 and later macOS –2402 and later
StoreFront	2402, 2407 and later
NetScaler	13.1, 14.1, and later. It is recommended to use the latest builds of the NetScaler Gateway version 13.1 or 14.1 for optimized performance. **Note:** The NetScaler Gateway minimum version required for Web/SaaS apps is 13.1. The TCP/UDP apps in hybrid deployments are supported from NetScaler Gateway version 14.1–34.42 and later.
Citrix Secure Access client	Windows client - 24.6.1.17 and later macOS client - 24.06.2 and later For details, see Citrix Secure Access client. Also, see Features and platforms supported by Citrix Secure Access client.
Citrix Cloud Connector	See Cloud Connector for hybrid deployment.
Communication ports	Ensure that you have opened the required ports for the Secure Private Access provider. For details, see Communication ports.

Though support for TCP/UDP apps along with Web/SaaS apps is available starting from NetScaler Gateway version 14.1–25.56, the 14.1–34.42 version significantly streamlines the configuration process.

Prerequisites

- **For the Secure Private Access admin console access, ensure that the following requirements are met:**
  - Citrix Cloud account. For details, see Create a Citrix Cloud account.
  - Secure Private Access service entitlement.
- **Ensure to get the Secure Private Access service in Cloud Connector enabled.**

  Once the Cloud Connector is updated, the Secure Private Access service is disabled. To enable

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

the feature, customers must contact Citrix Support. Once enabled, the service status changes to **Running** and the Secure Private Access service automatically starts on the connector machine.

- **For creating or updating an existing NetScaler Gateway, ensure that you have the following details:**
  - StoreFront store URLs to enter during the setup.
  - Store on StoreFront must have been configured and the Store service URL must be available. The format of the Store service URL is `https://store.domain.com/Citrix/StoreSecureAccess`.
  - NetScaler Gateway virtual IP address, FQDN, and NetScaler Gateway callback URL (optional) that are required for versions 13.0, 13.1.48.47 and later, 14.1.4.42 and later.
  - IP address and FQDN of the Secure Private Access provider host machine (or a load balancer if the Secure Private Access provider is deployed as a cluster).
  - Authentication profile name and authentication virtual server name configured on NetScaler.
  - SSL server certificate configured on NetScaler.
  - Domain name.
  - Certificate configurations are complete. Admins must ensure that the certificate configurations are complete and the certificates are trusted. The Secure Private Access provider configures a self-signed certificate if no certificate is found in the machine.

Communication ports

The following table lists the communication ports that are used by the Secure Private Access provider.

Source	Destination	Type	Port	Details
NetScaler Gateway	Secure Private Access provider	HTTPS	443	Application authorization validation
	StoreFront	HTTPS	443	Authentication and Application enumeration

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Source	Destination	Type	Port	Details
	Web applications	HTTPS	443	NetScaler Gateway communication to configured Secure Private Access applications (Ports can differ based on the application requirements)
StoreFront	Cloud Connector	TCP	8443	Unless the customer is using custom ports
Secure Private Access provider	Cloud Connector	TCP	8443	Unless the customer is using custom ports
Cloud Connector	Internet	TCP	443	See Connectivity requirements
User device	NetScaler Gateway	HTTPS	443	Communication between the end-user device and NetScaler Gateway

Features and platforms supported by Citrix Secure Access client

Unsupported features: The following features are not supported by the Citrix Secure Access client in the hybrid deployment.

- Always On before Windows Logon (machine tunnel)
- DNS-TCP
- Intranet IP
- Server initiated connections

Unsupported platforms: The following platforms are not supported by the Citrix Secure Access client in the hybrid deployment.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

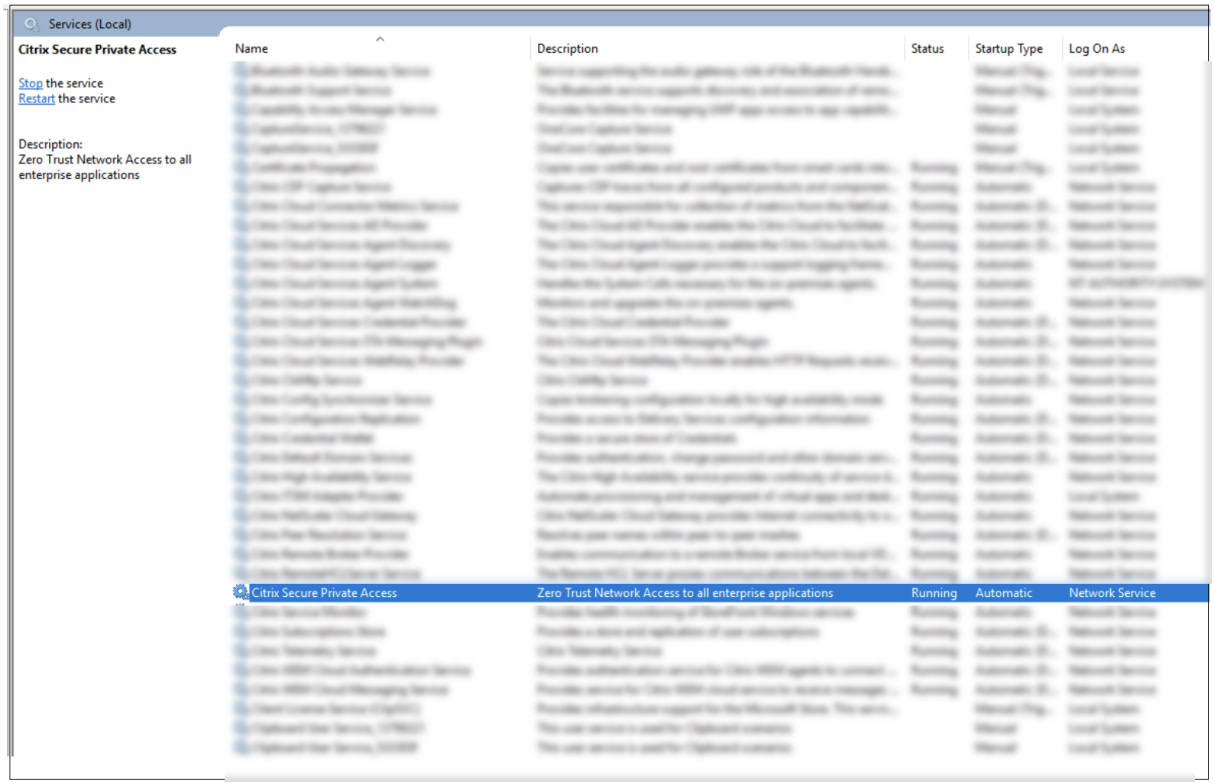
- Linux
- iOS
- Android

Cloud Connector for hybrid deployment

October 28, 2024

The Secure Private Access provider for the hybrid deployment is installed as part of Citrix Cloud Connector. After Citrix Cloud Connector is installed, the Citrix Secure Private Access service can be found in the Windows services. The Secure Private Access service operates under the network service account.

> **Important:**
>
> Once the Cloud Connector is updated, the Secure Private Access service is disabled. To enable the feature, customers must contact Citrix Support. Once enabled, the service status changes to **Running** and the Secure Private Access service automatically starts on the connector machine.



For details on Cloud Connector installation, see Cloud Connector Installation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Port configuration for Citrix Secure Private Access

Points to note:

- By default, Citrix Secure Private Access uses port 8443 as a plain HTTP service. Ensure that you add the inbound rule for port 8443 from the data center network.
- The internal load balancer for Citrix Secure Private Access adds the Cloud Connector backend service using port 8443.
- The port 8443 can be opened by manually configuring the firewall rules or by running the Citrix Secure Private Access config tool.

  Perform the following steps to run the config tool:

  1. Navigate to the Citrix Secure Private Access installation folder (default path - C:\Program Files\Citrix\AccessSecurityService).
  2. Run the command `.\Citrix.AccessSecurityService.exe /ENABLE_SPA_PORTS 8443`.

  After the command is run successfully, the firewall is configured automatically.

Enable TLS

By default, Citrix Secure Private Access operates as a standard HTTP service. This configuration works well if a load balancer is set up with full SSL offload. However, if you need to run the Citrix Secure Private Access service over TLS, follow these steps.

1. Install the TLS certificate in the Cloud Connector local machine personal certificate store.
2. Grant Network Service account permission to access the installed certificate. You can do this by using the Microsoft Management Console (MMC).

   a) Open the Microsoft Management Console.

   b) Add certificate snap-in for local Computer Account, follow the wizard, and click **OK**.

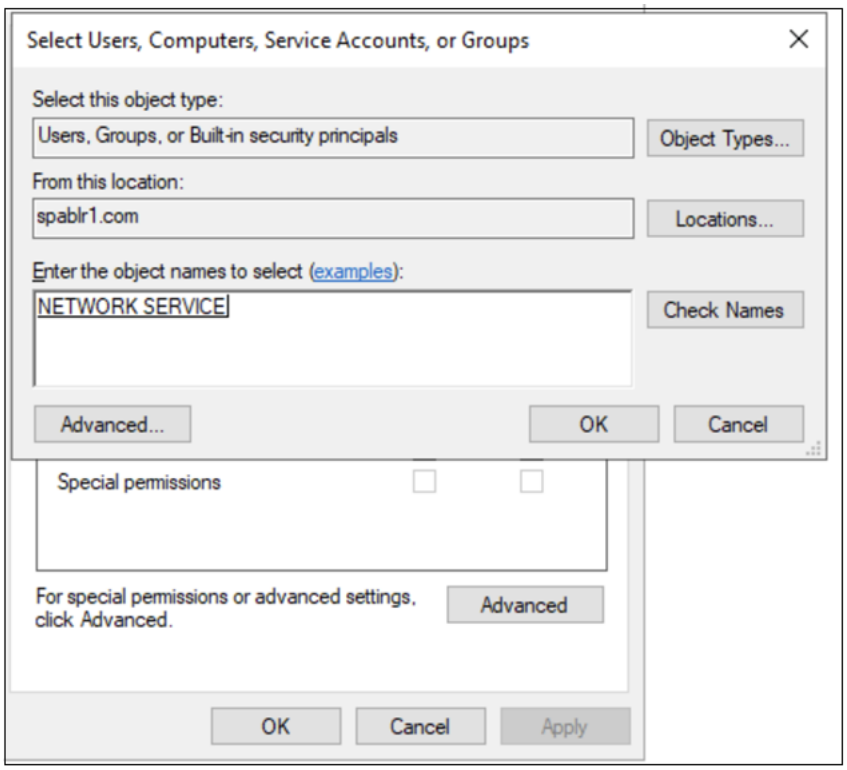
   c) In the Microsoft Management Console, go to **Console Root -> Certificates -> Personal -> Certificates**.

   d) Right-click the certificate that is required to configure for Secure Private Access.

   e) Click **All Tasks -> Manage Private Keys**.

   f) In the **Permissions** window, click **Add** and then search for the Network Service account.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

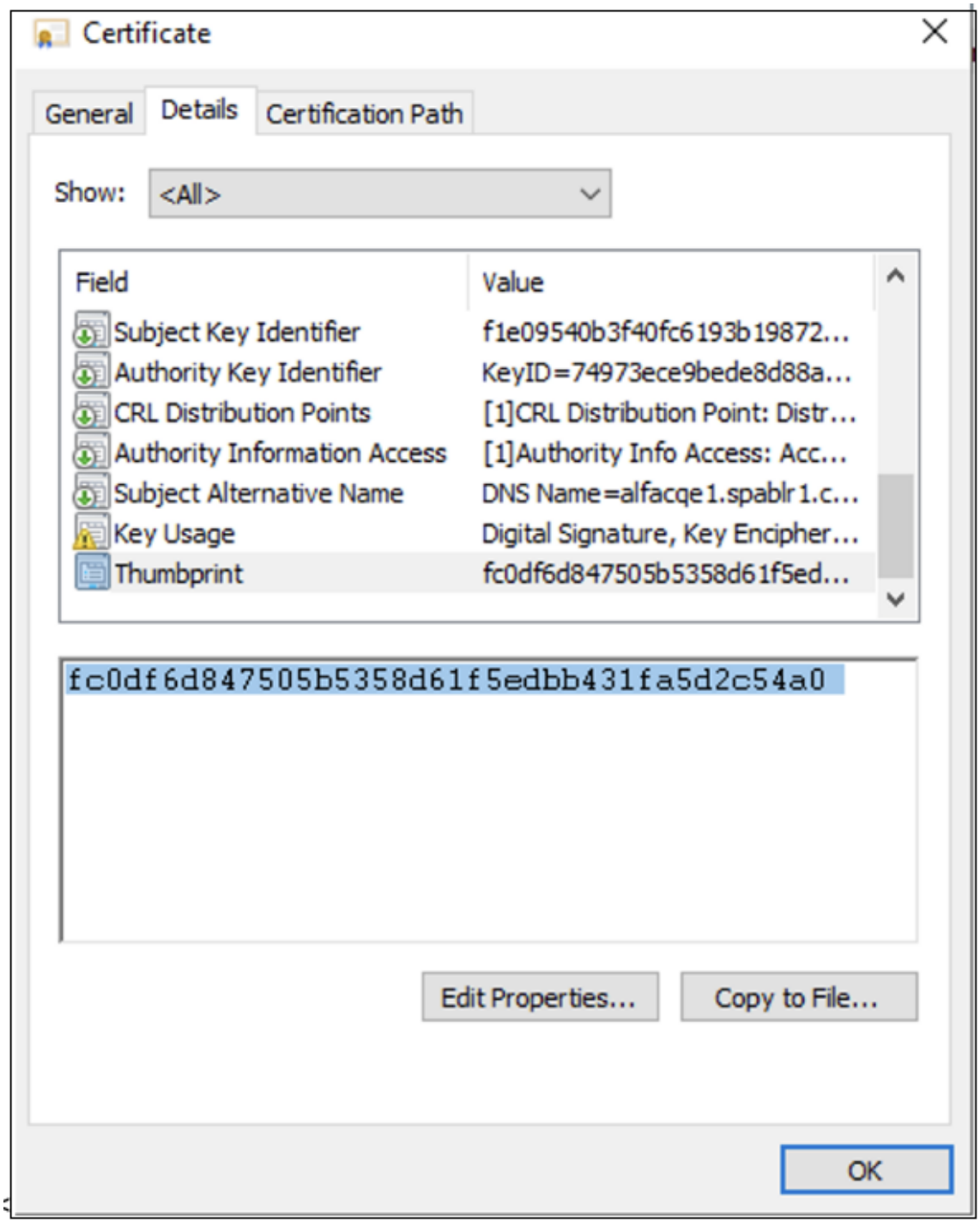


g) Choose the permission **Read only**.

h) Click **OK**.

i) Copy the thumbprint from **Certificate Details**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



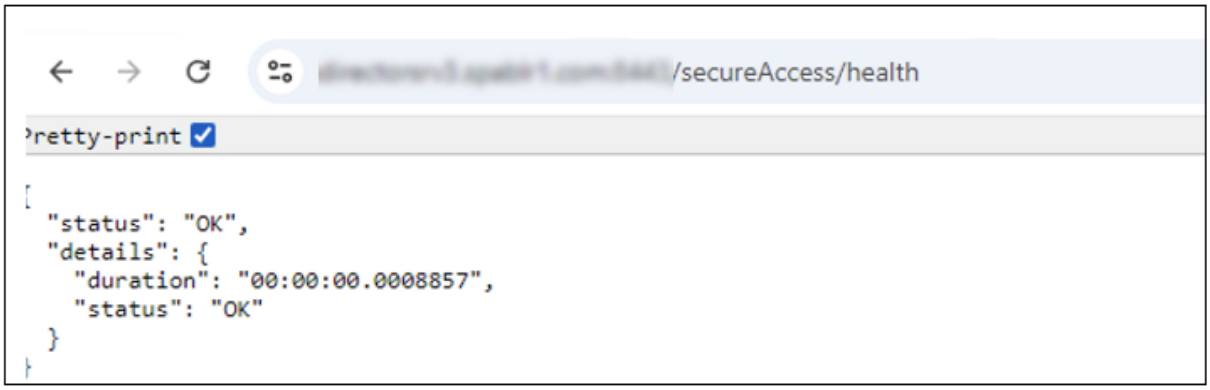
a) After copying the thumbprint, perform the following steps to enable TLS.

   i. Navigate to the Citrix Secure Private Access installation folder (default path - C:\Program Files\Citrix\AccessSecurityService).
   ii. Run `.\Citrix.AccessSecurityService.exe /CERTIFICATE_THUMBPRINT <ThumbprintValue>`.
   iii. Restart the Citrix Secure Private Access service.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

After the command runs successfully, the Secure Private Access service must be running as a TLS service. To confirm, enter the following URL in the browser.

```
https://<Cloud connector address>:<port>/secureAccess/health
```



Load balancer configuration

We recommend that you use the SSL bridge load balancer configuration for Cloud Connectors. For more information, see Configure SSL bridging.

Setup and configure for hybrid deployment

November 4, 2024

As part of the Secure Private Access hybrid deployment onboarding and setup process, the following steps must be completed.

1. Access to the Secure Private Access service admin console
2. Onboard and setup
3. Configure StoreFront
4. Configure NetScaler Gateway
5. Configure applications
    - Configure Web/SaaS applications
    - Configure TCP/UDP apps
    - Configure TCP/UDP - server to client apps
6. Configure access policies for applications

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Access the Secure Private Access admin console

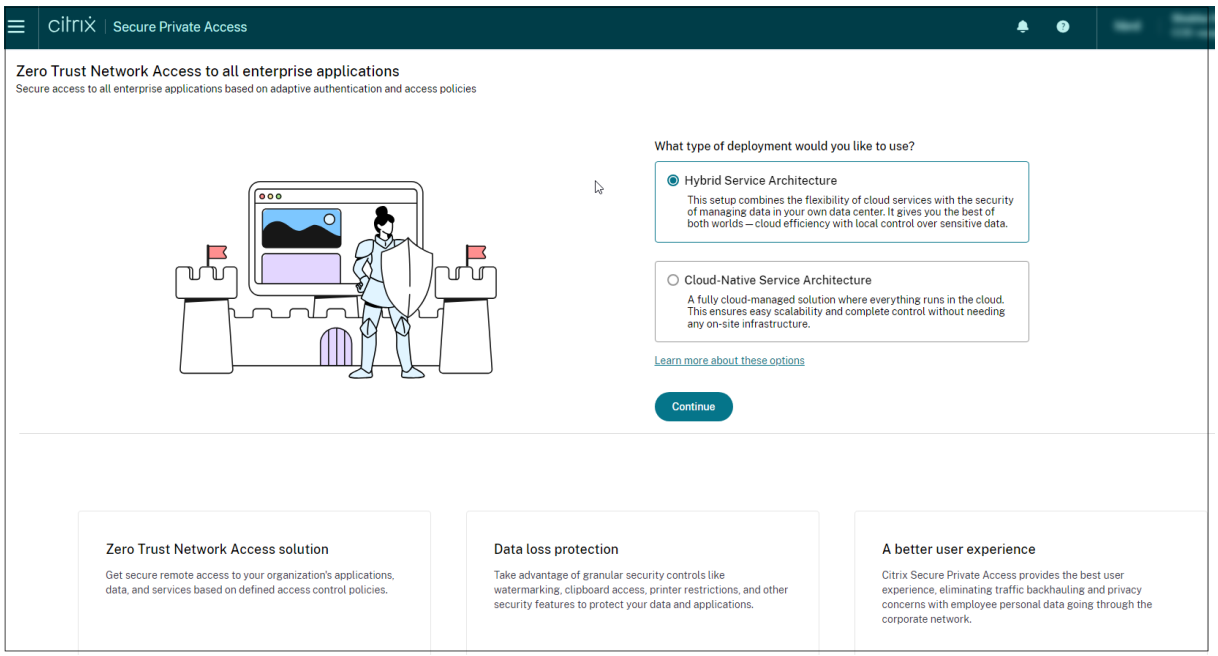
October 28, 2024

Ensure that the following requirements are met to access the Secure Private Access service admin console.

- Secure Private Access service entitlement.
- Citrix Cloud account. For details, see Create a Citrix Cloud account.

Perform the following steps to access the Secure Private Access admin console.

1. Log on to Citrix Cloud.
2. Click **Manage** on the Secure Private Access tile to access the admin console.
3. Select **Hybrid Service Architecture** and then click **Continue**.



Onboard and setup

October 22, 2024

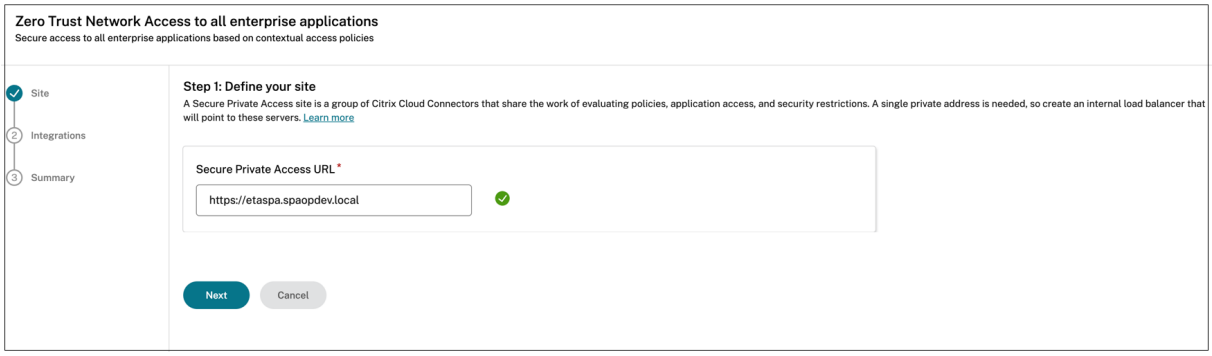
As part of the onboarding process, you must first define the Secure Private Access site and specify the servers associated with this deployment.

Step1 - Define your site:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

A Secure Private Access site is a group of cloud connectors that collaboratively handle the evaluation of policies, application access, and security restrictions. To facilitate this, a single private address is required to create an internal load balancer that distributes traffic among these servers. This load balancer distributes traffic among multiple cloud connectors to ensure load balancing, high availability, and efficient resource utilization.

In **Secure Private Access URL,** enter the URL of the load balancer.

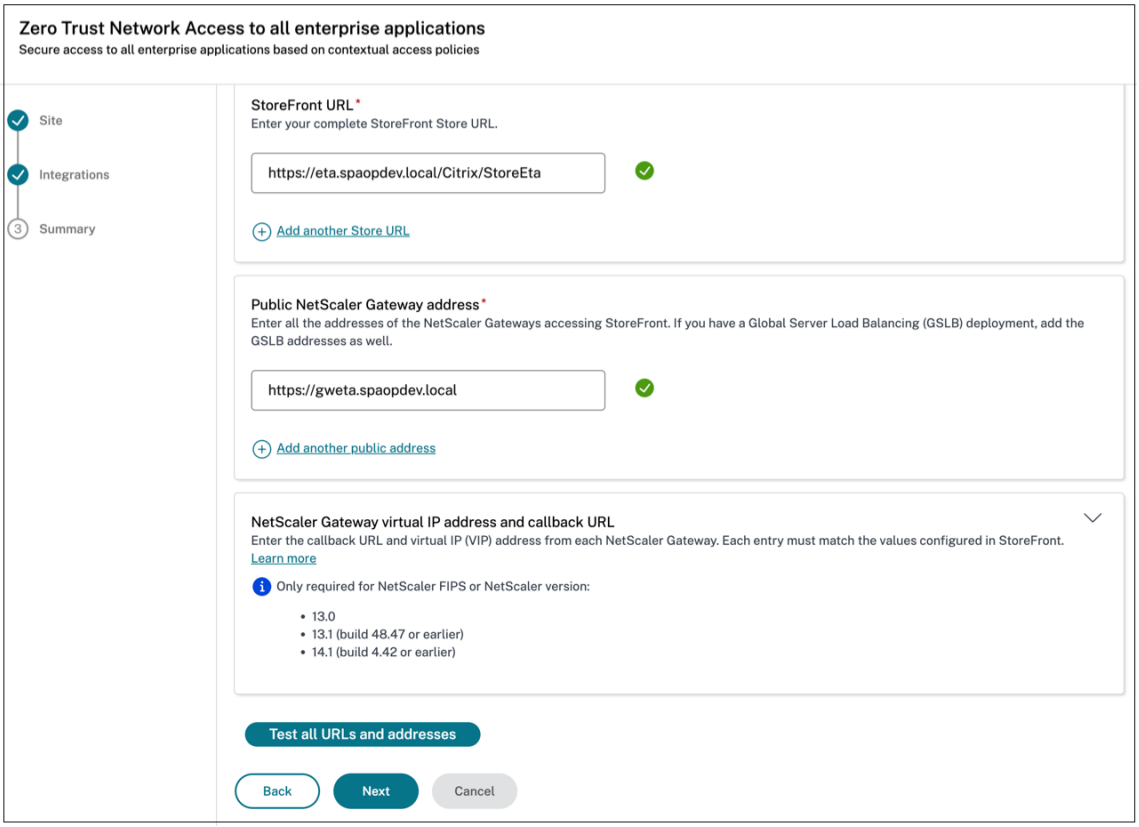


Step 2 - Integrate servers:

1. Enter the following details.

    - StoreFront Store URL. For example, `https://storefront.domain.com/Citrix/StoreMain`.
    - Public NetScaler Gateway Address –URL of the NetScaler Gateway. For example, `https://gateway.domain.com`.
    - NetScaler Gateway virtual IP address –This virtual IP address must be the same as the one configured in StoreFront for callbacks.
    - NetScaler Gateway Callback URL (Optional) –This URL must be the same as the one configured in StoreFront. For example, `https://gateway.domain.com`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Click **Test all URLs and addresses**.

   If any URLs are changed in the on-premises environment, click **Test all URLs and addresses** to confirm that the addresses are reachable.

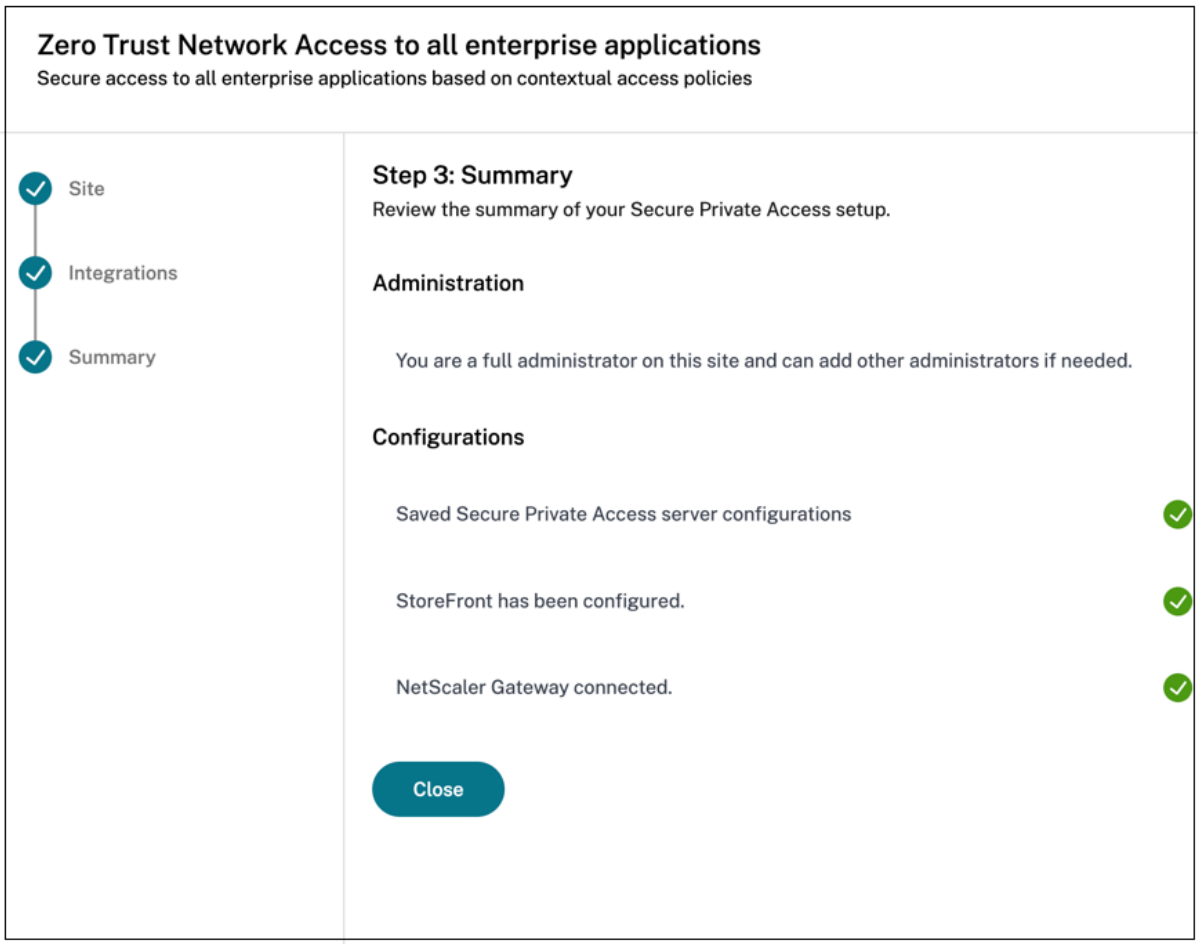
3. Click **Next**.

Step 3 - Summary:

After the configuration is complete, validation must be done to ensure that all servers that are configured are reachable.

If an error is found during validation, an error message is displayed against that component. After resolving the issue, run the validation checks again to ensure that all components are correctly configured and reachable.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



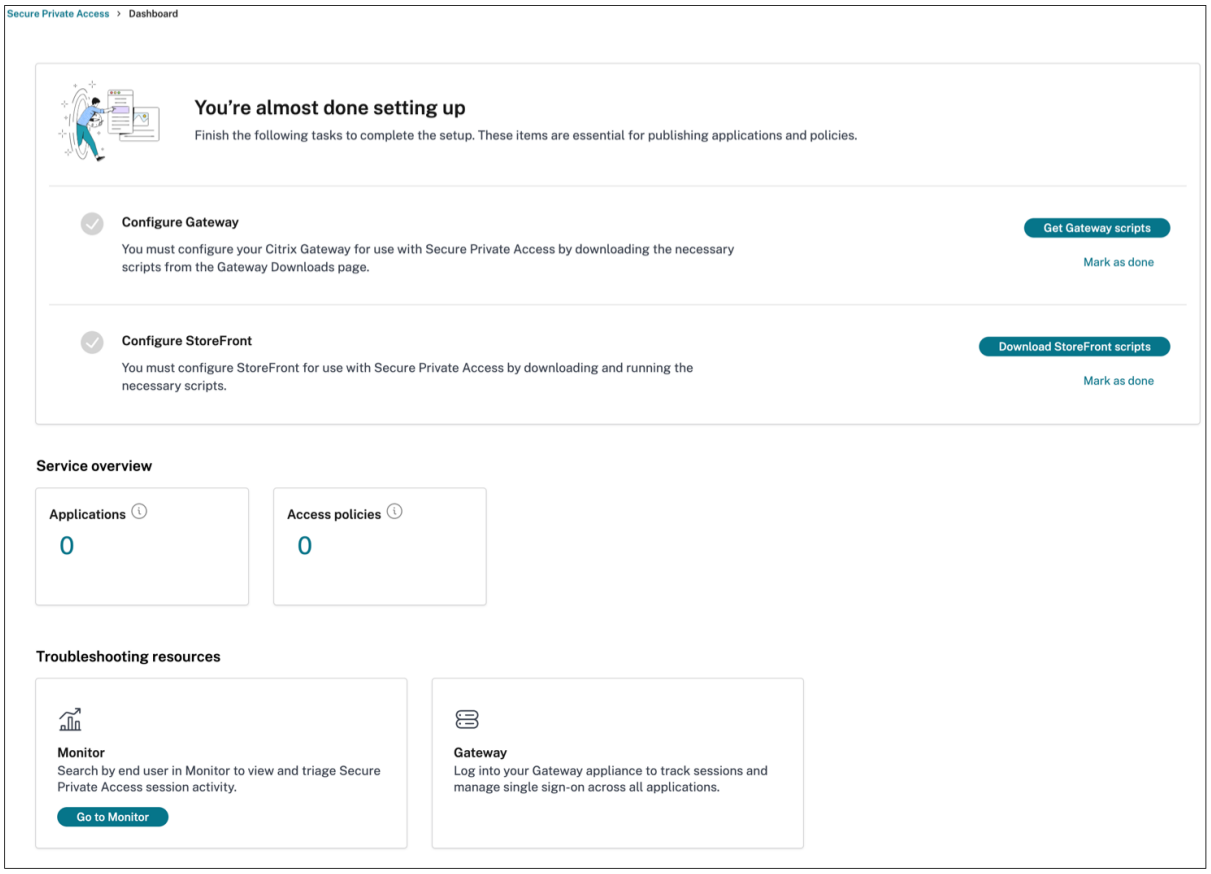
Click **Close**.

> **Note:**
>
> - You are prompted to download and run the StoreFront and NetScaler Gateway scripts to configure these components, if not already done. Once you run the scripts, click **Mark as done**. However, it is not mandatory to download and run the StoreFront and NetScaler Gateway scripts immediately after the initial setup. It is recommended to run these scripts to ensure that the configuration is complete.

Once you are done with the onboarding, you can create applications and associate access policies with the applications.

The following figure displays the Secure Private Access dashboard after the onboard and setup is complete.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Note:**
>
> From the dashboard, you can click **Go To Monitor** to monitor and troubleshoot app sessions and events from DaaS Monitor. For details, see Integration with DaaS monitor.

Configuration synchronization

All cloud configurations in the Secure Private Access console are automatically synced to Cloud Connector every five minutes. This sync occurs only when there are changes in the cloud configuration.

StoreFront

October 13, 2024

You must download the StoreFront script and manually run the scripts on the StoreFront machine.

Perform the following steps to configure StoreFront manually.

1. Download the script from the Secure Private Access admin console (**Settings > Integrations**).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Click **Download Script** corresponding to the StoreFront entry for which the configuration changes have to be done.

   The downloaded zip file contains a configuration script, a README file, and a configuration cleanup script. The cleanup script can be used in case integration between StoreFront and Secure Private Access is to be removed.

3. Run the script as an admin on a PowerShell 64-bit instance by using the command `./ConfigureStorefront.ps1`.

   - No other parameters are required.
   - The PowerShell script execution policy must be set to **Unrestricted** or **Bypass** to run the StoreFront script.
   - The script also propagates the configuration to other StoreFront servers if StoreFront is configured as a cluster.

Once StoreFront is configured with the Secure Private Access settings, the Secure Private Access provider configuration can be seen in the StoreFront admin UI (**Manage Delivery Controllers** screen).

The StoreFront script automatically configures the aggregation group setting for Secure Private Access if the same is configured for the Citrix Virtual Apps and Desktops delivery controller. By default, the script configures Secure Private Access for everyone (**User Mapping and Multi-Site Aggregation Configuration > Configured**).

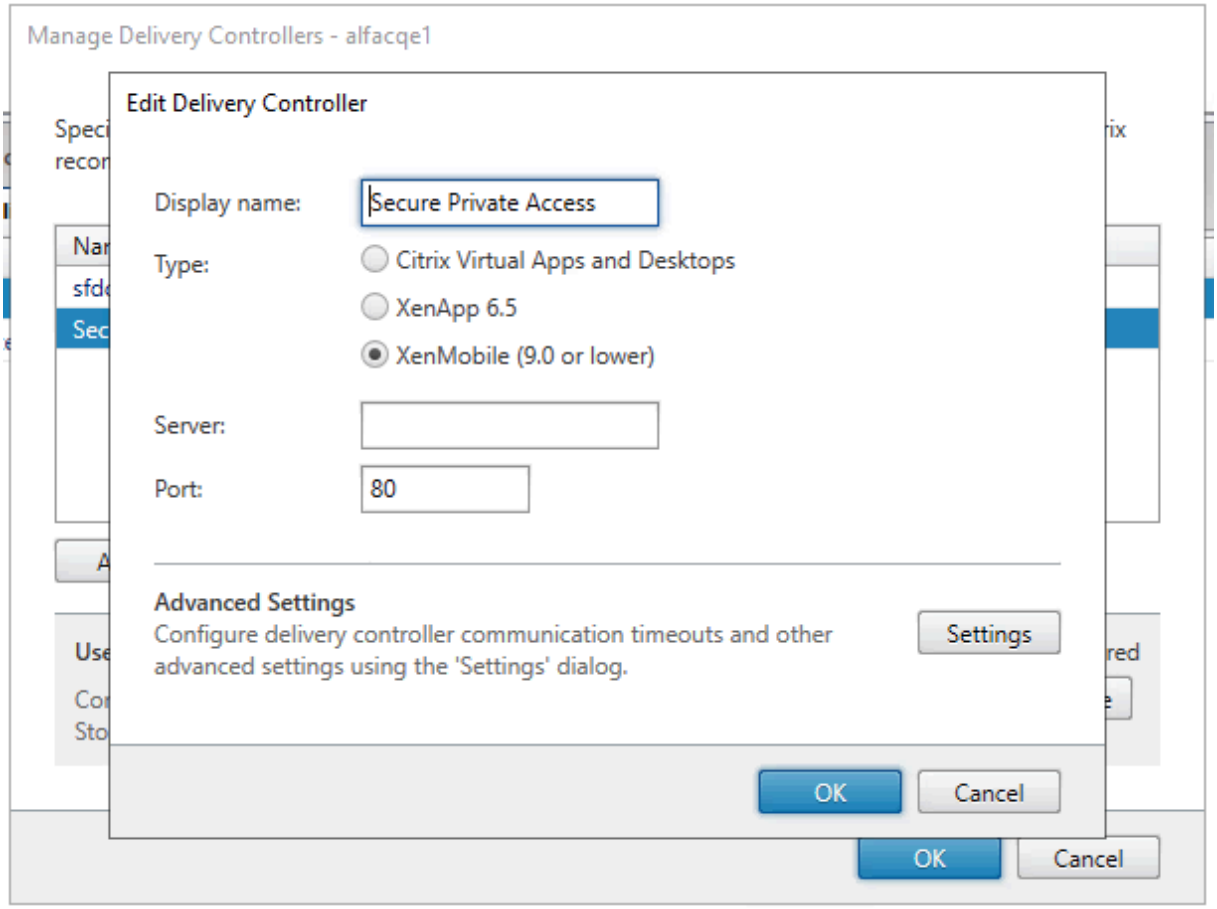
> **Important:**
>
> - It is recommended to use the StoreFront script downloaded from the Secure Private Access admin UI to configure StoreFront for Secure Private Access only. Do not configure Secure Private Access from the StoreFront admin UI as the UI does not cover all the required configuration on StoreFront. The script must be run to complete all the necessary configurations.
> - One Secure Private Access site can be configured on multiple StoreFront deployments (either on another store on the same StoreFront or a different StoreFront deployment) as well. StoreFront can be added from the **Settings > Integrations** page.
> - The StoreFront auto configuration doesn't work from **Settings > Integration** page even if Secure Private Access is co-hosted with StoreFront. Autoconfiguration is done only during the first-time setup. If a new store configuration is added from the **Settings** page, the StoreFront script must be downloaded and run on the corresponding StoreFront machine.

When using StoreFront version 2308 or earlier

If you are using StoreFront version 2308 or earlier, the StoreFront admin UI has the following known issues:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- The Secure Private Access provider type is shown as **XenMobile**.
- The Secure Private Access server URL is not displayed.
- The Secure Private Access port is always shown as **80**.



When using StoreFront version 2311 or later

In StoreFront version 2311 and later, the Citrix Workspace for Web client doesn't enumerate the Secure Private Access apps. This is because Secure Private Access doesn't support the Secure Private Access app launch in the Workspace for Web platform.

Configure NetScaler Gateway

October 28, 2024

NetScaler Gateway configuration is supported for both Web/SaaS and TCP/UDP applications. You can create a NetScaler Gateway or update an existing NetScaler Gateway configuration for Secure Private

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Access. It is recommended that you create NetScaler snapshots or save the NetScaler configuration before applying these changes.

> **Note:**
>
> - Support for TCP/UDP apps along with Web/SaaS apps is available starting from NetScaler Gateway version 14.1–25.56. However, Secure Private Access for TCP/UDP apps in hybrid deployments is supported from version 14.1-34.42 and this version significantly streamlines the configuration process.
> - Support for Web/SaaS apps is available from NetScaler Gateway versions 13.1, 14.1 and later. For details about the NetScaler Gateway configuration, see Configure NetScaler Gateway.
> - Secure Private Access for hybrid deployment can be enabled globally or per VPN virtual server. We recommend that you enable Secure Private Access per VPN virtual server. After Secure Private Access is enabled, TCP/UDP and Web/SaaS applications are enabled by default.

To create NetScaler Gateway for the Web/SaaS or TCP/UDP applications, perform the following steps:

1. Download the latest script `ns_gateway_secure_access.sh.` from https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/.
2. Upload these scripts to the NetScaler machine. You can use the WinSCP app or the SCP command. For example, `scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`.

   For example, `scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`

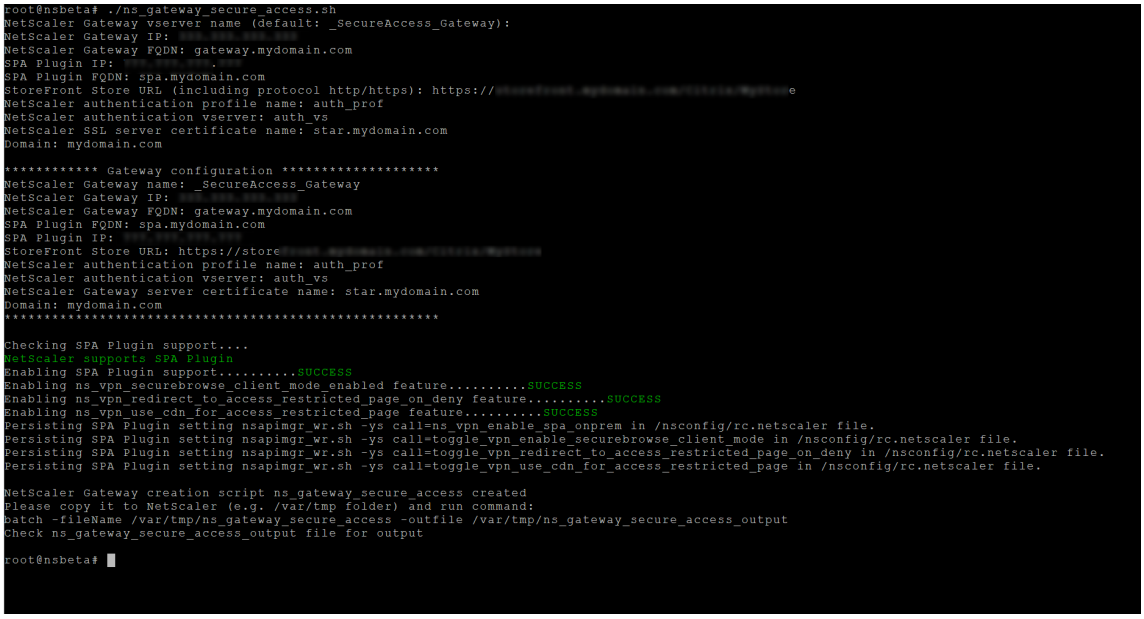
   > **Note:**
   >
   > - It's recommended to use NetScaler /var/tmp folder to store temp data.
   > - Make sure that the file is saved with LF line endings. FreeBSD does not support CRLF.
   > - If you see the error `-bash: /var/tmp/ns_gateway_secure_access.sh : /bin/sh^M: bad interpreter: No such file or directory`, it means that the line endings are incorrect. You can convert the script by using any rich text editor, such as Notepad++.

3. SSH to NetScaler and switch to shell (type 'shell'on NetScaler CLI).
4. Make the uploaded script executable. Use the chmod command to do so.

   ```
   chmod +x /var/tmp/ns_gateway_secure_access.sh
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Run the uploaded script on the NetScaler shell.

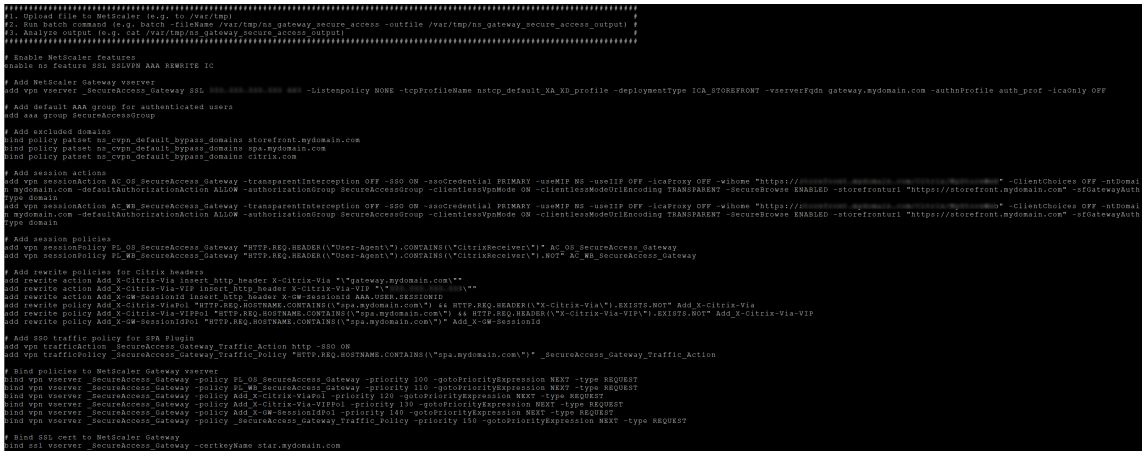


6. Input the required parameters. For the list of parameters, see Prerequisites.

   For the authentication profile and SSL certificate you have to provide names of existing resources on NetScaler.

   A new file with multiple NetScaler commands (the default is var/tmp/ns_gateway_secure_access) is generated.

> **Note:**
>
> During script execution, NetScaler and Secure Private Access provider compatibility is checked. If NetScaler supports the Secure Private Access provider, the script enables NetScaler features to support smart access tags sending improvements and redirection to a new Deny Page when access to a resource is restricted.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. Switch to the NetScaler CLI and run the resultant NetScaler commands from the new file with the batch command. For example;

   ```
   batch -fileName /var/tmp/ns_gateway_secure_access -outfile
   /var/tmp/ns_gateway_secure_access_output
   ```

   NetScaler runs the commands from the file one by one. If a command fails, it continues with the next command.

   A command can fail if a resource exists or one of the parameters entered in step 6 is incorrect.

8. Ensure that all commands are successfully completed.

> **Note:**
>
> - If a load balancer is configured, ensure that you provide the load balancer URL while binding the Secure Private Access provider to the VPN virtual server. Example: `bind vpn vserver spahybrid -securePrivateAccessUrl "https://spa.example.corp"`
> - If there's an error, NetScaler still runs the remaining commands and partially creates/updates/binds resources. Therefore, if you see an unexpected error because of one of the parameters being incorrect, it's recommended to redo the configuration from the start.

Points to note

- Existing NetScaler Gateway can be updated with script but there can be a significant number of possible NetScaler configurations that can't be covered by a single script.
- We recommend that you set **ICA Proxy** to OFF in the Secure Private Access enabled VPN virtual server.
- If you use NetScaler deployed in the cloud, you must make changes in the network. For example, allow communications between NetScaler and other components on certain ports. For details on the ports, see Communication ports.
- If you enable SSO on NetScaler Gateway, make sure that NetScaler communicates to StoreFront using a private IP address. You might have to add a StoreFront DNS record to NetScaler with a StoreFront private IP address.

Update existing NetScaler Gateway configuration

October 28, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

If you are updating an existing NetScaler Gateway configuration, it is recommended that you update the configuration manually. For details, see the following sections:

- Update existing NetScaler Gateway configuration for Web and SaaS apps
- Update existing NetScaler Gateway configuration for TCP/UDP apps

NetScaler Gateway virtual server settings

When you add or update the existing NetScaler Gateway virtual server, ensure that the following parameters are set to the defined values. For sample commands, see Example commands to update an existing NetScaler Gateway configuration.

Add a virtual server:

- tcpProfileName: nstcp_default_XA_XD_profile
- deploymentType: ICA_STOREFRONT (available only with the `add vpn vserver` command)
- icaOnly: OFF
- dtls: OFF

Update a virtual server:

- tcpProfileName: nstcp_default_XA_XD_profile
- icaOnly: OFF
- dtls: OFF

For details on the virtual server parameters, see vpn-sessionAction.

Update existing NetScaler Gateway configuration for Web and SaaS apps

You can use the `ns_gateway_secure_access_update.sh`script on an existing NetScaler Gateway to update the configuration for Web and SaaS apps. However, if you want to update the existing configuration (NetScaler Gateway version 14.1–4.42 and later) manually, use the Example commands to update an existing NetScaler Gateway configuration. Also, you must update the NetScaler Gateway virtual server and session action settings.

You can also use the scripts on an existing NetScaler Gateway to support Secure Private Access. However, the script does not update the following:

- Existing NetScaler Gateway virtual server
- Existing session actions and session policies bound to NetScaler Gateway

Ensure that you review each command before execution and create backups of the gateway configuration.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NetScaler Gateway session actions settings

Session action is bound to a gateway virtual server with session policies. When you create or update a session action, ensure that the following parameters are set to the defined values. For sample commands, see Example commands to update an existing NetScaler Gateway configuration.

- `transparentInterception`: OFF
- `SSO`: ON
- `ssoCredential`: PRIMARY
- `useMIP`: NS
- `useIIP`: OFF
- `icaProxy`: OFF
- `wihome`: `"https://storefront.mydomain.com/Citrix/MyStoreWeb"` - replace with real store URL. Path to Store `/Citrix/MyStoreWeb` is optional.
- `ClientChoices`: OFF
- `ntDomain`: mydomain.com - used for SSO (optional)
- `defaultAuthorizationAction`: ALLOW
- `authorizationGroup`: SecureAccessGroup (Make sure that this group is created, it's used to bind Secure Private Access specific authorization policies)
- `clientlessVpnMode`: ON
- `clientlessModeUrlEncoding`: TRANSPARENT
- `SecureBrowse`: ENABLED
- `Storefronturl`: `"https://storefront.mydomain.com"`
- `sfGatewayAuthType`: domain

Example commands to update an existing NetScaler Gateway configuration

Add/update a virtual server.

- `add vpn vserver SecureAccess_Gateway SSL 999.999.999.999 443 -Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -authnProfile auth_prof_name -icaOnly OFF -dtls OFF`

Add a session action.

- `add vpn sessionAction AC_OSspahybrid -transparentInterception OFF -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -wihome "https://storefront.example.corp/Citrix/SPAWeb"-ClientChoices OFF -ntDomain example.corp -`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -
SecureBrowse ENABLED -storefronturl "https://storefront.example.
corp"-sfGatewayAuthType domain
```

- `add vpn sessionAction AC_WBspahybrid -transparentInterception OFF -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -wihome "https://storefront.example.corp/Citrix/SPAWeb"-ClientChoices OFF -ntDomain example.corp -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "https://storefront.example.corp"-sfGatewayAuthType domain`

Add a session policy.

- `add vpn sessionPolicy PL_OSspahybrid "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")"AC_OSspahybrid`
- `add vpn sessionPolicy PL_WBspahybrid "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT && HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"plugin\").NOT"AC_WBspahybrid`

Bind the session policy to the VPN virtual server.

- `bind vpn vserver SecureAccess_Gateway -policy PL_OSspahybrid -priority 100 -gotoPriorityExpression NEXT -type REQUEST`
- `bind vpn vserver SecureAccess_Gateway -policy PL_WBspahybrid -priority 110 -gotoPriorityExpression NEXT -type REQUEST`

Bind the Secure Private Access provider to the VPN virtual server.

- `bind vpn vserver spahybrid -securePrivateAccessUrl "https://spa.example.corp"`

For details on session action parameters, vpn-sessionAction.

Update existing NetScaler Gateway configuration for TCP/UDP apps

Support for TCP/UDP apps in addition to Web/SaaS apps is available starting from NetScaler Gateway version 14.1–25.56. For hybrid deployments, it is recommended to use version 14.1-34.42 to fully leverage TCP/UDP features. If you are updating earlier versions, it is recommended that you update the configuration manually. For details, see Example commands to update an existing NetScaler Gateway configuration. Also, you must update the NetScaler Gateway virtual server and session action settings.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NetScaler Gateway session policy settings

Session action is bound to a gateway virtual server with session policies. When you create or update a session action, ensure that the following parameters are set to the defined values. For sample commands, see Example commands to update an existing NetScaler Gateway configuration. Also, you must update the NetScaler Gateway virtual server and session action settings.

- `transparentInterception`: ON
- `SSO`: ON
- `ssoCredential`: PRIMARY
- `useMIP`: NS
- `useIIP`: OFF
- `icaProxy`: OFF
- `ClientChoices`: ON
- `ntDomain`: mydomain.com - used for SSO (optional)
- `defaultAuthorizationAction`: ALLOW
- `authorizationGroup`: SecureAccessGroup
- `clientlessVpnMode`: OFF
- `clientlessModeUrlEncoding`: TRANSPARENT
- `SecureBrowse`: ENABLED

Example commands to update an existing NetScaler Gateway configuration

- Add a VPN session action to support Citrix Secure Access-based connections.

```
add vpn sessionAction AC_AG_PLGspahybrid -splitDns BOTH -splitTunnel
 ON -transparentInterception ON -defaultAuthorizationAction ALLOW
 -authorizationGroup SecureAccessGroup -SSO ON -ssoCredential
PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -ClientChoices ON -
ntDomain example.corp -clientlessVpnMode OFF -clientlessModeUrlEncoding
 TRANSPARENT -SecureBrowse ENABLED
```

- Add a VPN session policy to support Citrix Secure Access-based connections.

```
add vpn sessionPolicy PL_AG_PLUGINspahybrid "HTTP.REQ.HEADER
(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT && (HTTP.REQ
.HEADER(\"User-Agent\").CONTAINS(\"plugin\")|| HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"CitrixSecureAccess\"))"AC_AG_PLGspahybrid
```

- Bind the session policy to the VPN virtual server to support Citrix Secure Access-based connections.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
bind vpn vserver spahybrid -policy PL_AG_PLUGINspahybrid -priority
 105 -gotoPriorityExpression NEXT -type REQUEST
```

- Bind the Secure Private Access URL to the VPN virtual server.

```
bind vpn vserver spahybrid -securePrivateAccessUrl "https://spa.
example.corp"
```

> **Note:**
>
> NetScaler Gateway release 14.1-34.42 and later does not support the App Controller server. You must instead bind the Secure Private Access URL to the VPN virtual server.

NetScaler Gateway configuration for earlier versions

October 28, 2024

NetScaler Gateway configuration is supported for both Web/SaaS and TCP/UDP applications. You can create a NetScaler Gateway or update an existing NetScaler Gateway configuration for Secure Private Access. It is recommended that you create NetScaler snapshots or save the NetScaler configuration before applying these changes.

> **Important:**
>
> - Support for TCP/UDP apps in addition to Web/SaaS apps is available starting from NetScaler Gateway version 14.1–25.56. However, Secure Private Access for TCP/UDP apps in hybrid deployments is supported from version 14.1-34.42 and this version significantly streamlines the configuration process.
> - Support for Web/SaaS apps is available from NetScaler Gateway versions 13.1, 14.1 and later.
> - For details about the NetScaler Gateway configuration, see Configure NetScaler Gateway.

Support for smart access tags

> **Note:**
>
> - The information provided in this section is applicable only if your NetScaler Gateway version is before 14.1-25.56.
> - If your NetScaler Gateway version is 14.1–25.56 and later, then you can enable the Secure Private Access provider on NetScaler Gateway by using the CLI or GUI. For details, see Enable Secure Private Access provider on NetScaler Gateway.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

In the following versions, NetScaler Gateway sends the tags automatically. You do not have to use the gateway callback address to retrieve the smart access tags.

- 13.1–48.47 and later
- 14.1–4.42 and later

The smart access tags are added as a header in the Secure Private Access provider request.

Configure Secure Private Access toggles

The following table lists the toggles that must be used to support smart access tags for hybrid deployments.

Toggle name	Description
`nsapimgr_wr.sh -ys call= ns_vpn_enable_spa_onprem`	Enable Secure Private Access for hybrid deployments
`nsapimgr_wr.sh -ys call= ns_vpn_disable_spa_onprem`	Disable Secure Private Access for hybrid deployments
`nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3`	Enable TCP/UDP apps
`nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=0`	Disable TCP/UDP apps
`nsapimgr_wr.sh -ys call= toggle_vpn_enable_securebrowse_client_mode`	Enable SecureBrowse client mode for HTTP callout config
`nsapimgr -ys call= toggle_vpn_redirect_to_access_restricted_page_for_spa`	Enable redirection to the “Access restricted” page if access is denied.
`nsapimgr -ys call= toggle_vpn_use_cdn_for_access_restricted_page`	Use the “Access restricted”page hosted on CDN.

Note:

- To disable the toggles that do not have separate disable commands, run the same command again. This is applicable only for commands that have “toggle”in the command.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - To verify whether the toggle is on or off, run the `nsconmsg` command.
> - To configure smart access tags on NetScaler Gateway, see Configure contextual tags.

Persist Secure Private Access provider settings on NetScaler

To persist the Secure Private Access provider settings on NetScaler, do the following:

1. Create or update the file /nsconfig/rc.netscaler.
2. Add the following commands to the /nsconfig/rc.netscaler file.

```
nsapimgr -ys call=ns_vpn_enable_spa_onprem
nsapimgr -ys call=toggle_vpn_enable_securebrowse_client_mode
nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny

nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
```

3. Save the file.

The Secure Private Access provider settings are automatically applied when NetScaler is restarted.

Enable Secure Private Access provider on NetScaler Gateway

Starting from NetScaler Gateway 14.1–25.56 and later, you can enable the Secure Private Access provider on NetScaler Gateway by using the NetScaler Gateway CLI or the GUI.

CLI:

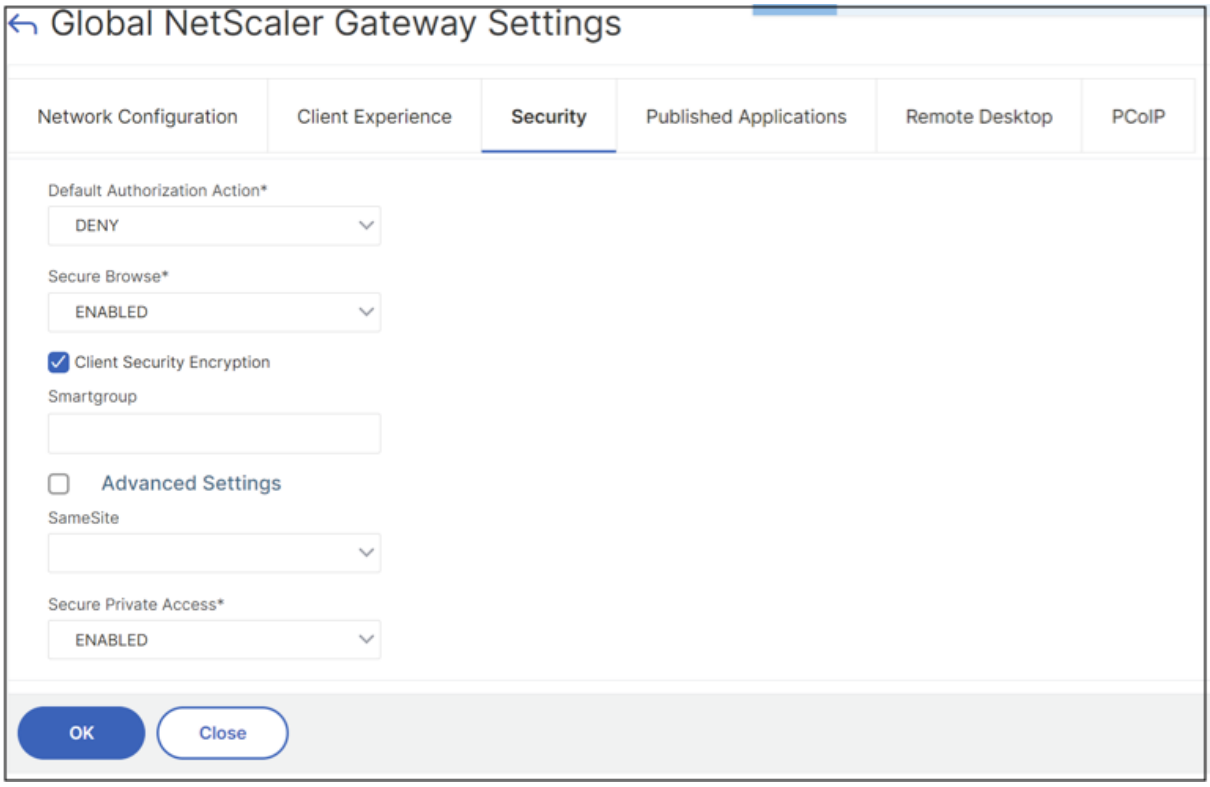
At the command prompt, type the following command:

```
set vpn parameter -securePrivateAccess ENABLED
```

GUI:

1. Navigate to **NetScaler Gateway > Global Settings > Change Global NetScaler Gateway Settings**.
2. Click the **Security** tab.
3. In **Secure Private Access**, select **ENABLED.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Upload public gateway certificate

If the public gateway is not reachable from the Secure Private Access machine, then you must upload a public gateway certificate to the Secure Private Access database.

Perform the following steps to upload a public gateway certificate:

1. Open PowerShell or the command prompt window with the admin privileges.
2. Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool").
3. Run the following command:

```
\AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
> <PublicGatewayCertificatePath>
```

Compatibility with the ICA apps

NetScaler Gateway created or updated to support the Secure Private Access provider can also be used to enumerate and launch ICA apps. In this case, you must configure Secure Ticket Authority (STA) and bind it to the NetScaler Gateway.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> STA server is usually a part of Citrix Virtual Apps and Desktops deployment.

For details, see the following topics:

- Configuring the Secure Ticket Authority on NetScaler Gateway
- FAQ: Citrix Secure Gateway/ NetScaler Gateway Secure Ticket Authority

Known limitations

- Existing NetScaler Gateway can be updated with script but there can be a significant number of possible NetScaler configurations that can't be covered by a single script.
- We recommend that you set **ICA Proxy** to OFF in the Secure Private Access enabled VPN virtual server.
- If you use NetScaler deployed in the cloud, you must make changes in the network. For example, allow communications between NetScaler and other components on certain ports. For details on the ports, see Communication ports.
- If you enable SSO on NetScaler Gateway, make sure that NetScaler communicates to StoreFront using a private IP address. You might have to add a StoreFront DNS record to NetScaler with a StoreFront private IP address.

Contextual tags

October 28, 2024

The Secure Private Access provider enables contextual access (smart access) to Web or SaaS applications based on the user session context such as device platform and OS, installed software, geolocation.

Administrators can add conditions with contextual tags to the access policy. The contextual tag on the Secure Private Access provider is the name of a NetScaler Gateway policy (session, preauthentication, EPA) that is applied to the sessions of the authenticated users.

The Secure Private Access provider can receive smart access tags as a header (new logic) or by making callbacks to Gateway. For details, see Smart access tags.

Configure custom tags using the GUI

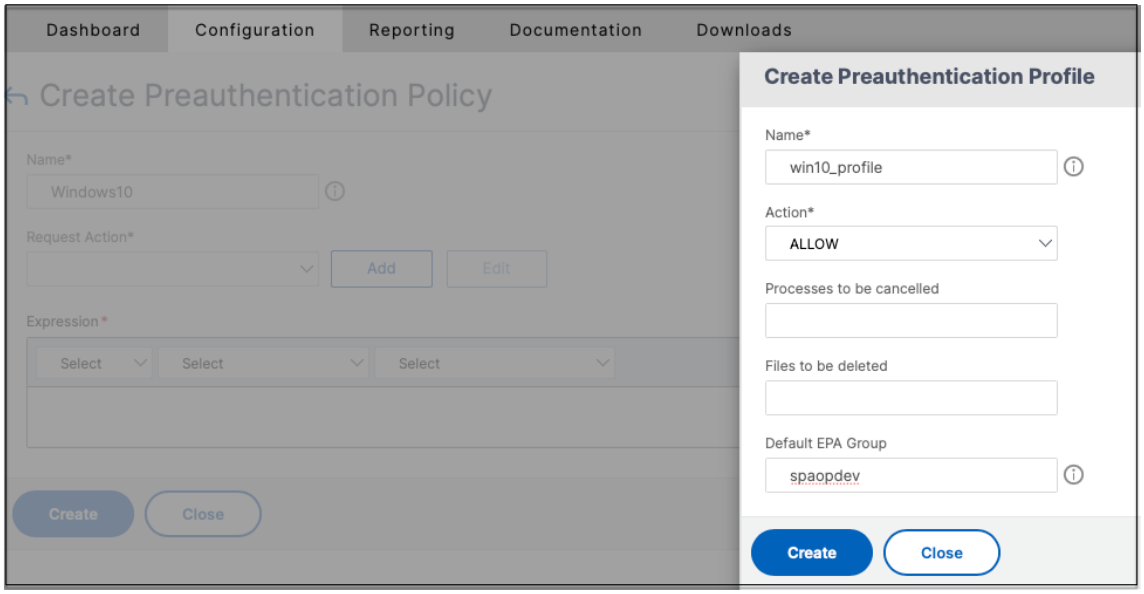
The following high-level steps are involved in configuring contextual tags.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Configure a classic gateway preauthentication policy.
2. Bind the classic preauthentication policy to the gateway virtual server.

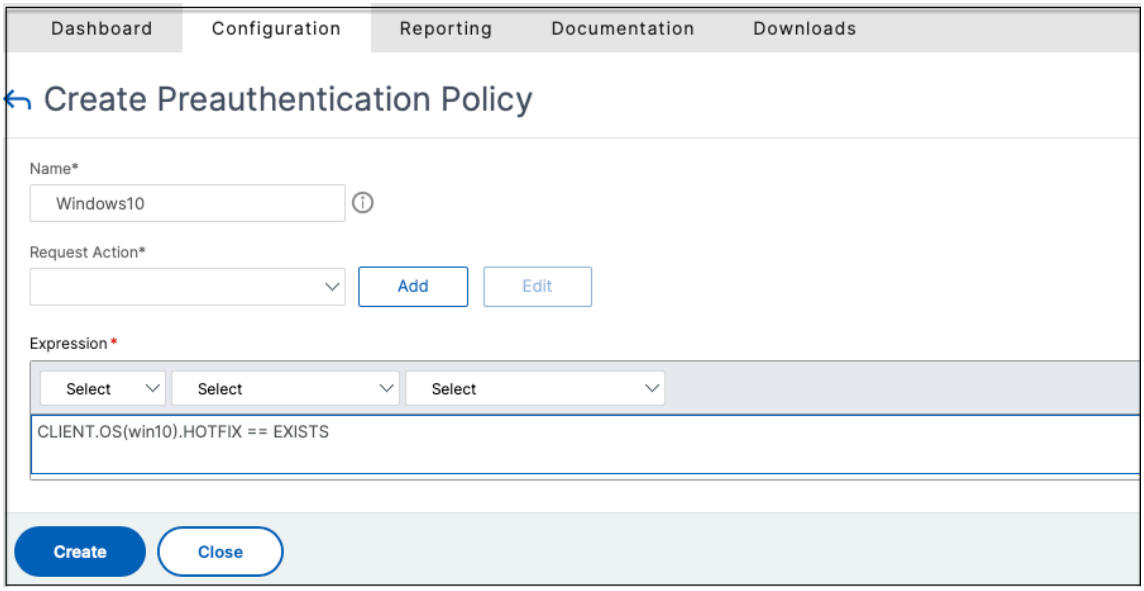
Configure a classic gateway preauthentication policy

1. Navigate to **NetScaler Gateway > Policies > Preauthentication** and then click **Add**.
2. Select an existing policy or add a name for the policy. This policy name is used as the custom tag value.
3. In **Request Action**, click **Add** to create an action. You can reuse this action for multiple policies, for example, use one action to allow access, another to deny access.



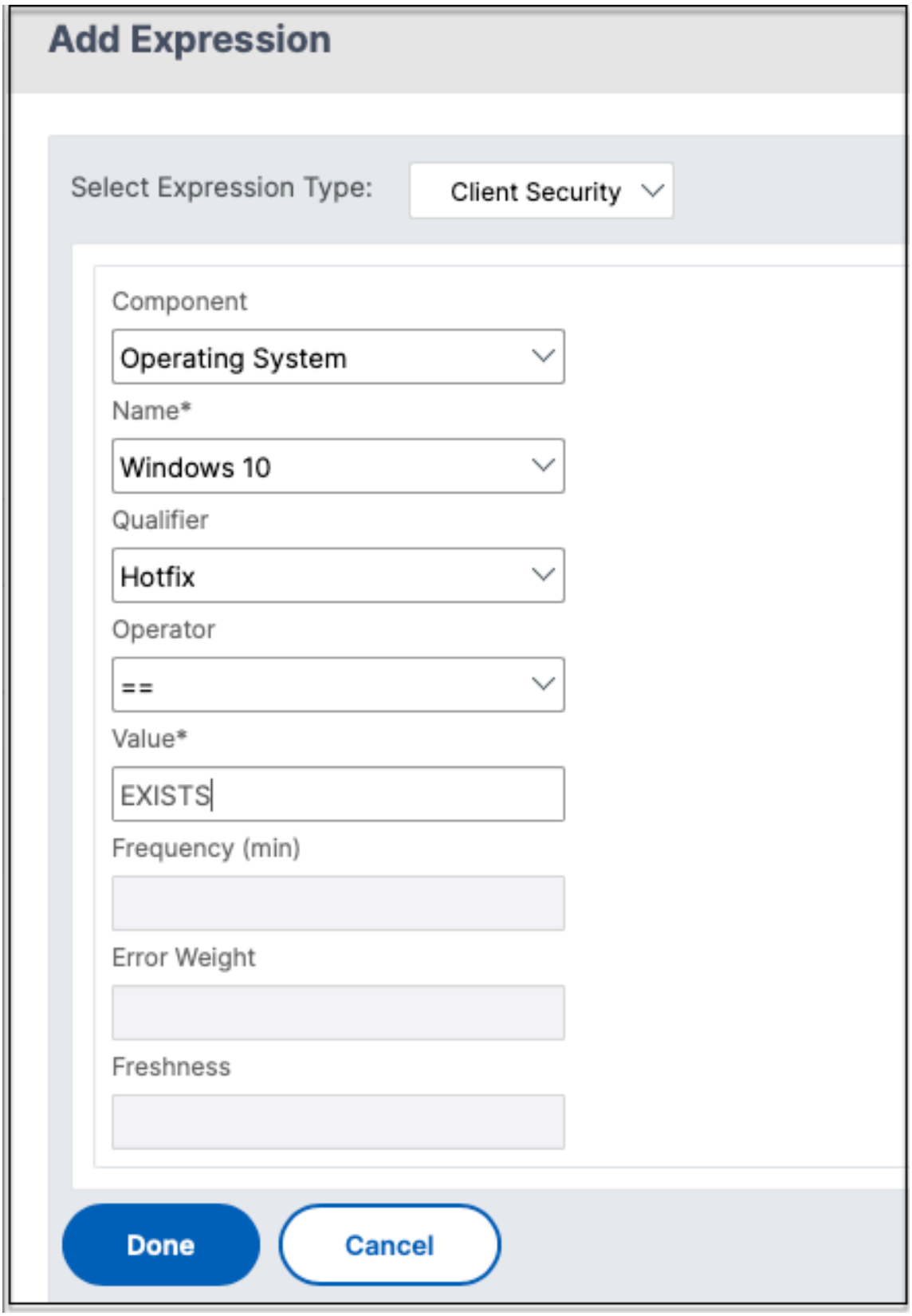
4. Fill in the details in the required fields and click **Create**.
5. In **Expression**, enter the expression manually or use the Expression editor to construct an expression for the policy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



The following figure displays a sample expression constructed for checking the Windows 10 OS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

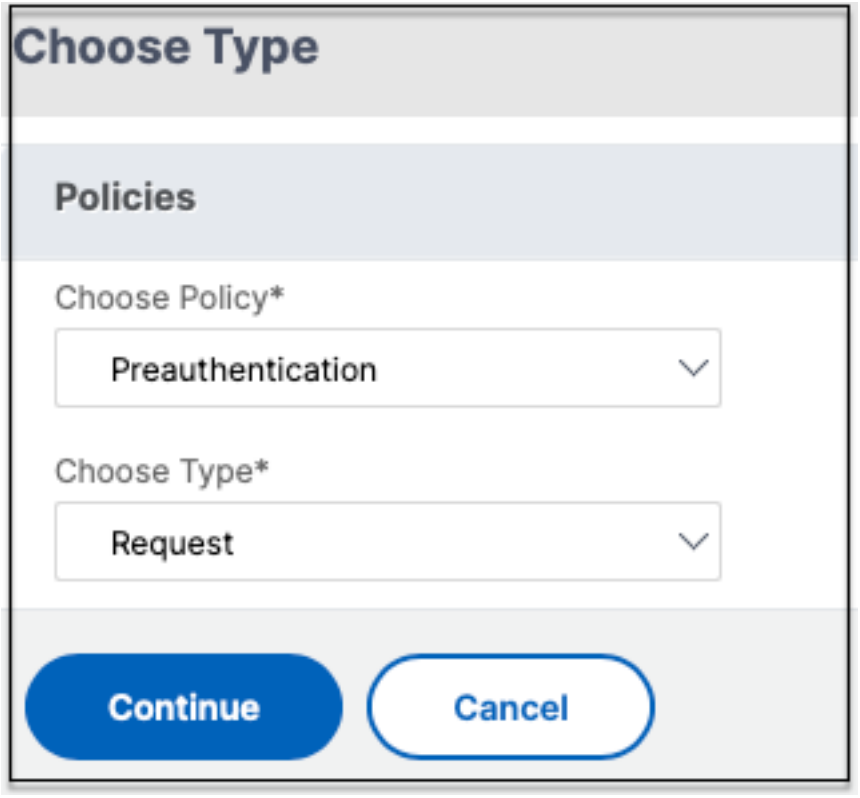


6. Click **Create**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

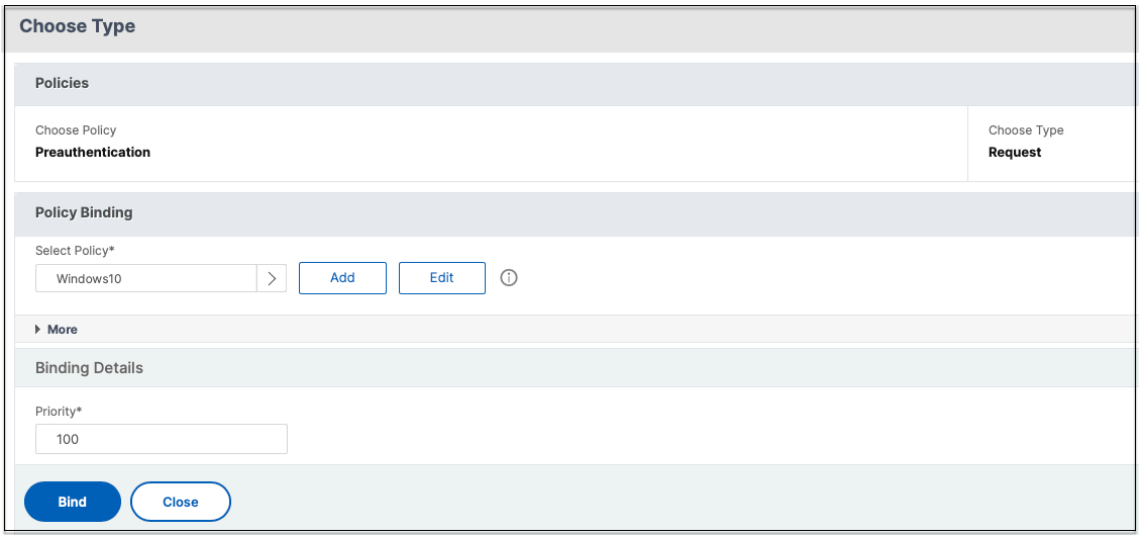
Bind the custom tag to NetScaler Gateway

1. Navigate to **NetScaler Gateway > Virtual Servers**.
2. Select the virtual server for which the preauthentication policy is to be bound and then click **Edit**.
3. In the **Policies** section, click **+** to bind the policy.
4. In **Choose Policy**, select the preauthentication policy and select **Request** in **Choose Type**.



5. Select the policy name and the priority for the policy evaluation.
6. Click **Bind**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configure custom tags using the CLI

Run the following sample commands on the NetScaler CLI to create and bind a preauthentication policy:

- `add aaa preauthenticationaction win10_prof ALLOW`
- `add aaa preauthenticationpolicy Windows10 "CLIENT.OS(win10)EXISTS "win10_prof`
- `bind vpn vserver _SecureAccess_Gateway -policy Windows10 -priority 100`

Run the following sample command on the NetScaler CLI to configure nFactor EPA policy:

- `add authentication epaAction epaallowact -csecexpr "sys.client_expr (\"proc_0_notepad.exe\")"-defaultEPAGroup allow_app -quarantineGroup deny_app`
- `add authentication Policy epaallow -rule true -action epaallowact`

Adding a new contextual tag

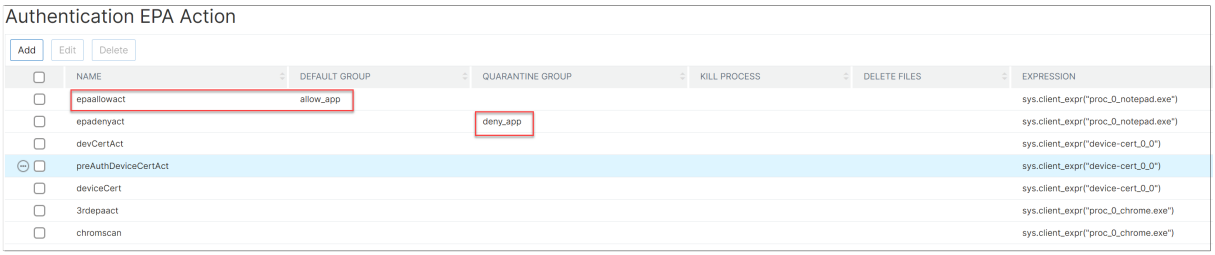
1. Open the Secure Private Access admin console and click **Access Policies**.
2. Create a new policy or edit an existing policy.
3. In the **Condition** section, click **Add condition** and select **Contextual Tags**, **Matches all of**, and then enter the contextual tag name (for example, `Windows10`).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Note on EPA tags sent to Secure Private Access provider

The EPA action name configured in nFactor EPA policy and the associated group name as smart access tags to the Secure Private Access provider. However, the tags that are sent are dependent on the outcome of the EPA action evaluation.

- If all EPA actions in an nFactor EPA policy results in action **DENY** and a quarantine group is configured in the last action, the quarantine group name is sent as the smart access.
- If an EPA action in an nFactor EPA policy results in action **ALLOW**, the EPA policy names associated with the action and the default group name (if configured) are sent as the smart access tags.



In this example, when the action is denied, deny_app is sent as the smart access tag to the Secure Private Access provider. When the action is allowed, epaallowact and allow_app are sent as the smart access tags to the Secure Private Access provider.

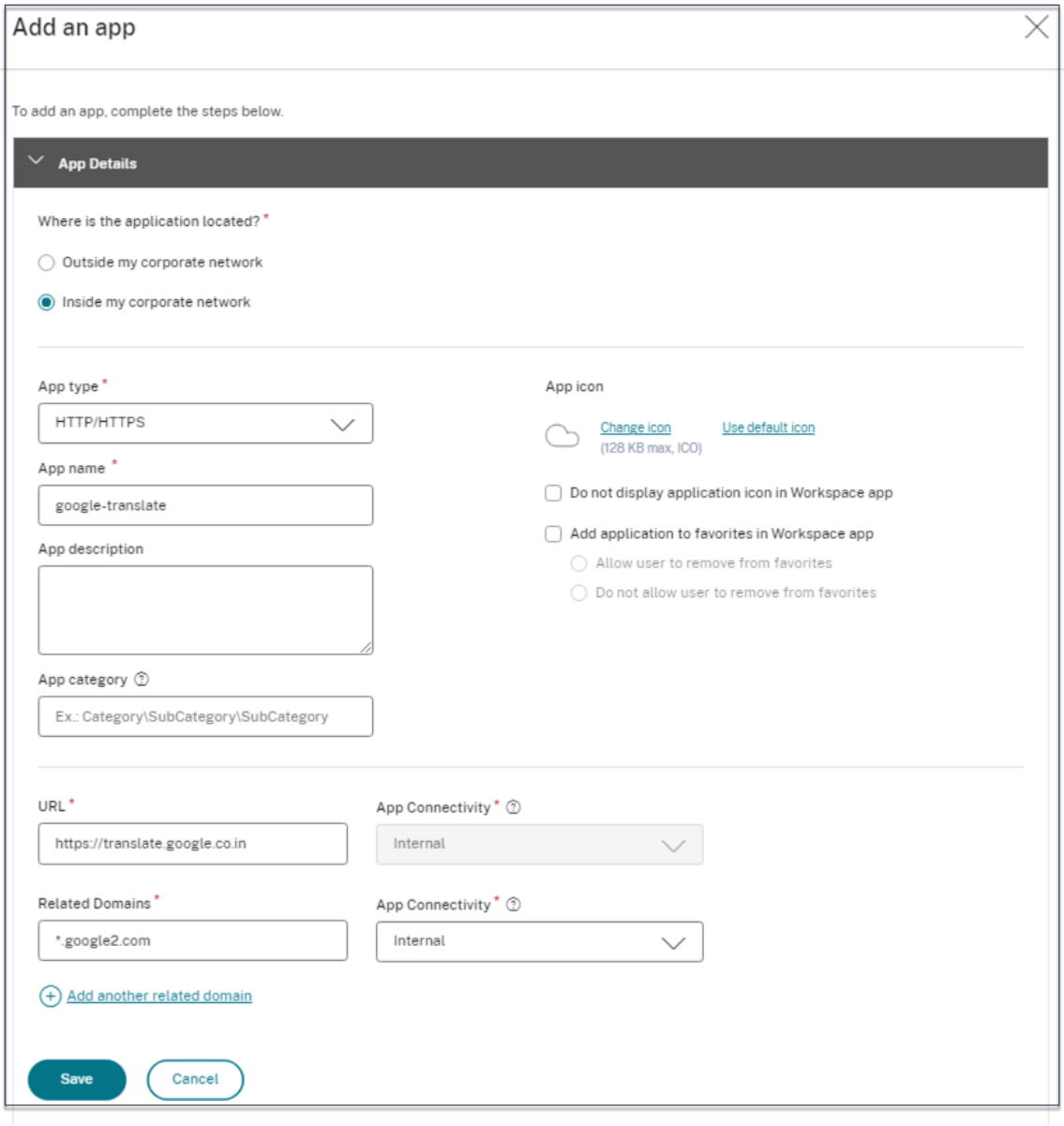
Configure Web/SaaS applications

October 17, 2024

After you have set up Secure Private Access, you can configure apps and access policies from the admin console.

1. In the admin console, click **Applications**.
2. Click **Add an app**.
3. Select the location where the app resides.
    - **Outside my corporate network** for external applications.
    - **Inside my corporate network** for internal applications.
4. Enter the following details in the App Details section and click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **App name** –Name of the application.
- **App description** - A brief description of the app. This description is displayed to your users in the workspace. You can also enter keywords for the applications in the format `KEYWORDS: <keyword_name>`. You can use the keywords to filter the applications. For details, see Filter resources by included keywords.
- **App category** - Add the category and the subcategory name (if applicable) under which the app that you are publishing must appear in the Citrix Workspace UI. You can add a new category for each app or use existing categories from the Citrix Workspace UI. Once you specify a category for a web or a SaaS app, the app shows up in the Workspace UI under the specific category.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - The category/subcategory are admin configurable and administrators can add a new category for every app.
  - The category/subcategory names must be separated by a backslash. For example, Business And Productivity\Engineering. Also, this field is case sensitive. Administrators must ensure that they define the correct category. If there is a mismatch between the name in the Citrix Workspace UI and the category name entered in the App category field, the category gets listed as a new category.

    For example, if you enter the Business and Productivity category incorrectly as Business And productivity in the App category field, then a new category named Business and productivity gets listed in the Citrix Workspace UI in addition to the Business And Productivity category.

- **App icon** –Click **Change icon** to change the app icon. The icon file size must be 128x128 pixels and only the ICO and PNG format are supported. If you do not change the icon, the default icon is displayed.
- **Do not display application to users** - Select this option if you do not want to display the app to the users.
- **URL** –URL of the application.
- **Related Domains** –The related domain is auto-populated based on the application URL. Administrators can add more related internal or external domains.

  > **Note:**
  >
  > - Ensure that an app's related domain does not overlap with another app's related domain. If this occurs, remove the related domain from all apps and create a new app with this domain and then set access accordingly in the access policy. You can also consider if you want to display this app in StoreFront or hide it. You can hide the app in StoreFront using the option **Do not display application to users** while publishing the app.
  > - Similarly, a published app's URL must not be added as another app's related domain.
  > - For more details, see Best practices for Web and SaaS application configurations.

- **Add application to favorites automatically** –Click this option to add the app as a favorite app in Citrix Workspace app. When you select this option, a star icon with a padlock appears at the top left-hand corner of the app in Citrix Workspace app.
  - **Allow user to remove from favorites** –Click this option to allow app subscribers to remove the app from the favorites apps list in Citrix Workspace app.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

When you select this option, a yellow star icon appears at the top left-hand corner of the app in Citrix Workspace app.

- **Do not allow user to remove from favorites**–Click this option to prevent subscribers from removing the app from the favorites apps list in Citrix Workspace app.

If you remove the apps marked as favorites from the Secure Private Access console, then these apps must be removed manually from the favorites list in Citrix Workspace. The apps are not automatically deleted from StoreFront if the apps are removed from the Secure Private Access console.

- **App Connectivity** - Select **Internal** for Web apps and **External** for SaaS apps.

5. Click **Save**, and then click **Finish**.

You can view all the application domains that are configured in **Settings > Application Domain**. For more details, see Manage settings after installation.

Next steps

Configure access policies for the applications.

Configure TCP/UDP apps

October 16, 2024

Prerequisites:

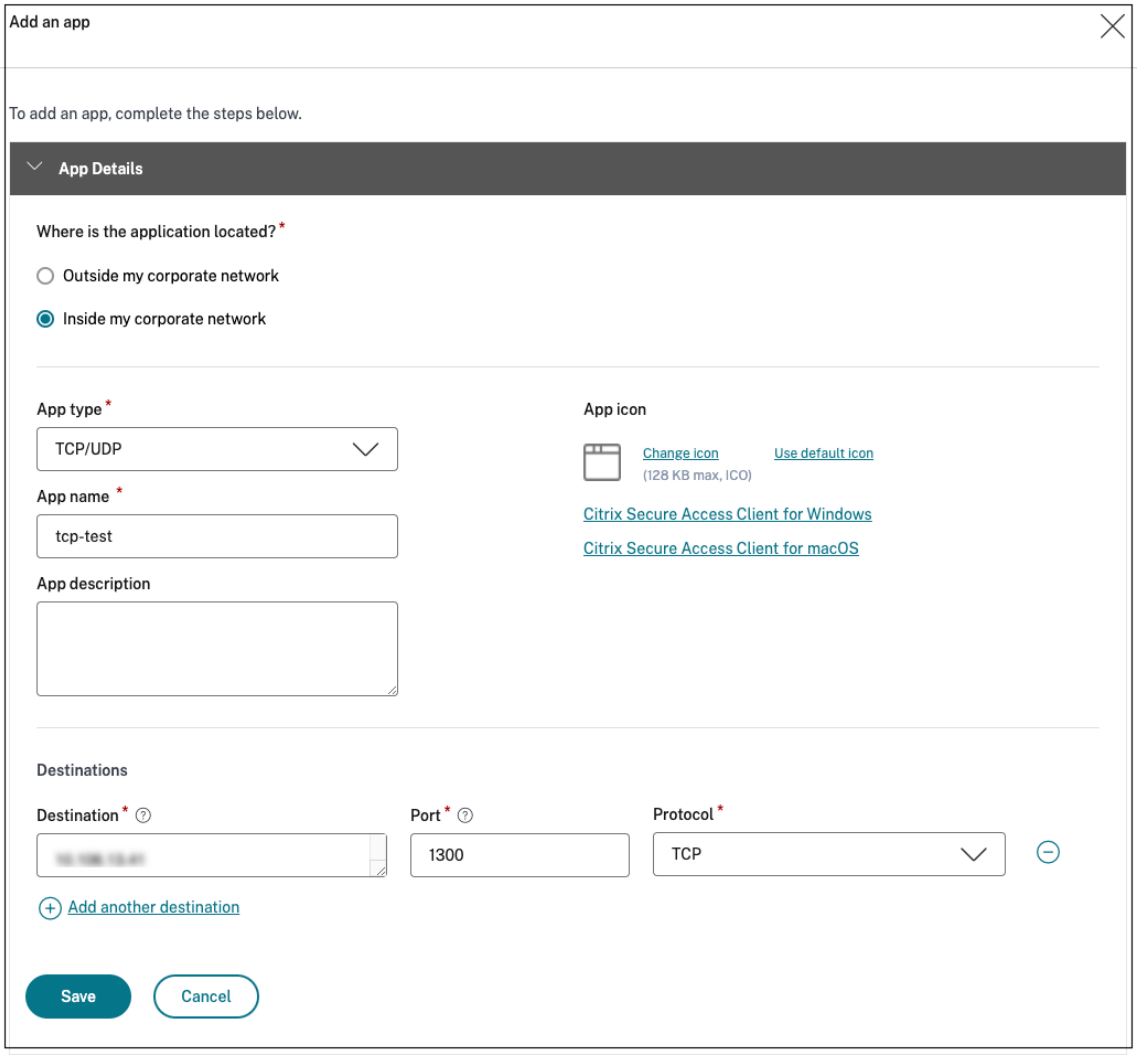
- Secure Private Access setup is complete.
- Client versions meet the following requirements:
  - Windows - 24.8.1.15 and later
  - macOS - 24.09.1 and later

  For details, see Citrix Secure Access client.

Perform the following steps to configure TCP/UDP apps from the admin console:

1. In the admin console, click **Applications** and then click **Add an app**.
2. Select the location **Inside my corporate network**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Enter the following details:

   - **App type** –Select **TCP/UDP** for initiating connections with the back-end servers residing in the data center.
   - **App name**–Name of the application.
   - **App description** –Description of the app you are adding. This field is optional.
   - **Destinations** –IP Addresses or FQDNs of the back-end machines residing in the data center. One or more destinations can be specified as follows.
     - **IP address v4**
     - **IP address Range** –Example: 10.68.90.10-10.68.90.99
     - **CIDR** –Example: 10.106.90.0/24
     - **FQDN of the machines or Domain name** –Single or wildcard domain. Example: ex.destination.domain.com, *.domain.com

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

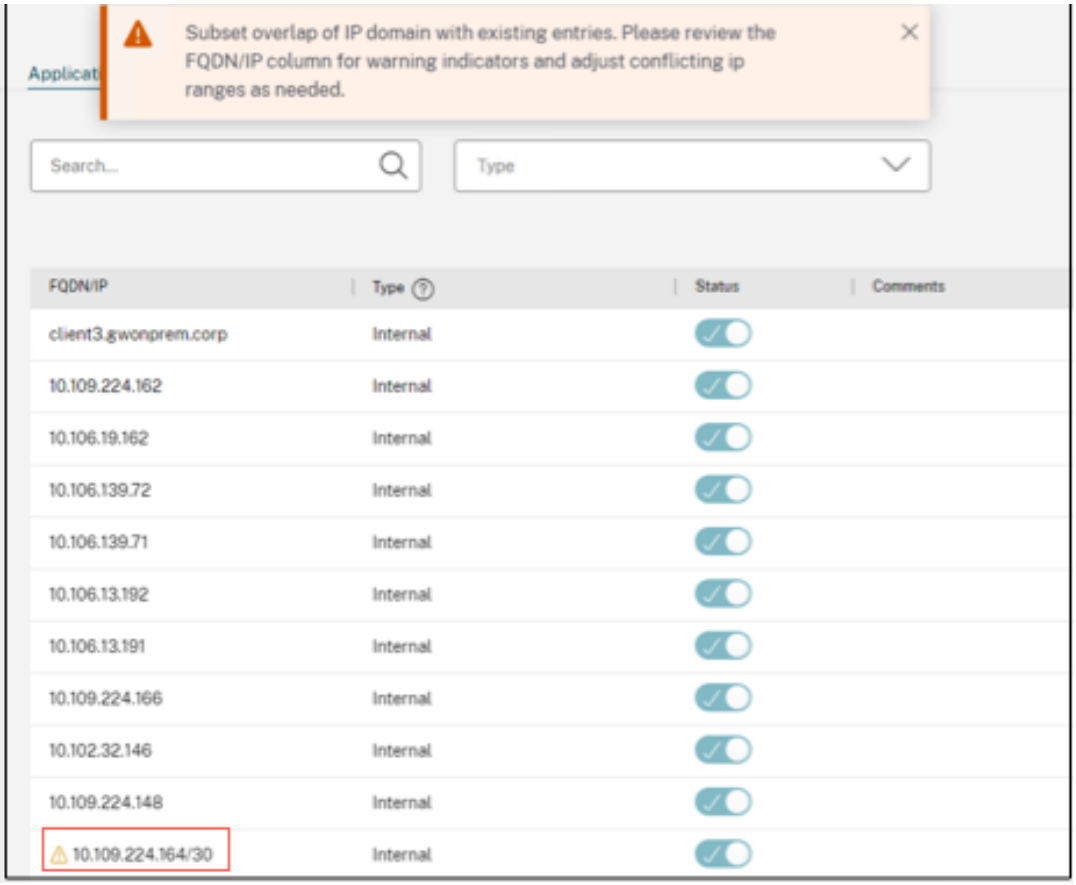
> **Note:**
>
> * End users can access the apps using FQDN even if the admin has configured the apps using the IP address. This is possible because the Citrix Secure Access client can resolve an FQDN to the real IP address.

The following table provides examples of various destinations and how to access the apps with these destinations:

Destination input	How to access the app
10.10.10.1-10.10.10.100	The end user is expected to access the app only through IP addresses in this range.
10.10.10.0/24	The end user is expected to access the app only through IP addresses configured in the IP CIDR.
10.10.10.101	End user is expected to access the app only through 10.10.10.101
`*.info.citrix.com`	End user is expected to access subdomains of `info.citrix.com` and also `info.citrix.com` (the parent domain). For example, `info.citrix.com`, `sub1.info.citrix.com`, `level1.sub1.info.citrix.com` **Note:** The wildcard must always be the starting character of the domain and only one *. is allowed.
info.citrix.com	End user is expected to access `info.citrix.com` only and no subdomains. For example, `sub1.info.citrix.com` is not accessible.

The destination IP address must be unique across resource locations. If a conflicting configuration exists, a warning symbol is displayed against the specific IP address in the Application Domain table (**Settings > Application Domain**).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Port** –The destination port on which the app is running. Admins can configure multiple ports or port ranges per destination.

  The following table provides examples of ports that can be configured for a destination.

Port input	Description
*	By default, the port field is set to “ * ” (any port). The port numbers from 1 to 65535 are supported for the destination.
1300–2400	The port numbers from 1300 to 2400 are supported for the destination.
38389	Only the port number 38389 is supported for the destination.
22,345,5678	The ports 22, 345, 5678 are supported for the destination.
1300–2400, 42000-43000,22,443	The port number range from 1300 to 2400, 42000–43000, and ports 22 and 443 are supported for the destination.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> Wildcard port (*) cannot co-exist with port numbers or ranges.

- **Protocol** –TCP/UDP

4. Click **Add** to add additional destinations or servers accordingly.
5. Click **Save**. The app is added to the **App Configuration** page. You can edit or delete an app from the **Applications** page after you have configured the application. To do so, click the ellipsis button in line with the app and select the actions accordingly.
    - **Edit Application**
    - **Delete**

Next steps

Configure access policies for the applications.

Configure TCP/UDP - server to client apps

November 4, 2024

The **TCP/UDP - server to client** app type can be used for supporting the following features:

- Software distribution using Microsoft Endpoint Configuration Manager or similar solutions
- Remote policy updates on managed devices using GPO Push
- Remote assistance to troubleshoot and debug user workstations.

Prerequisites:

- Secure Private Access setup is complete.
- Client versions meet the following requirements:
    - Windows - 24.6.1.18 and later
    - macOS - 24.06.2 and later
- The intranet IP address is configured on NetScaler Gateway and is bound to the respective VPN virtual server. Use the following sample commands for reference:

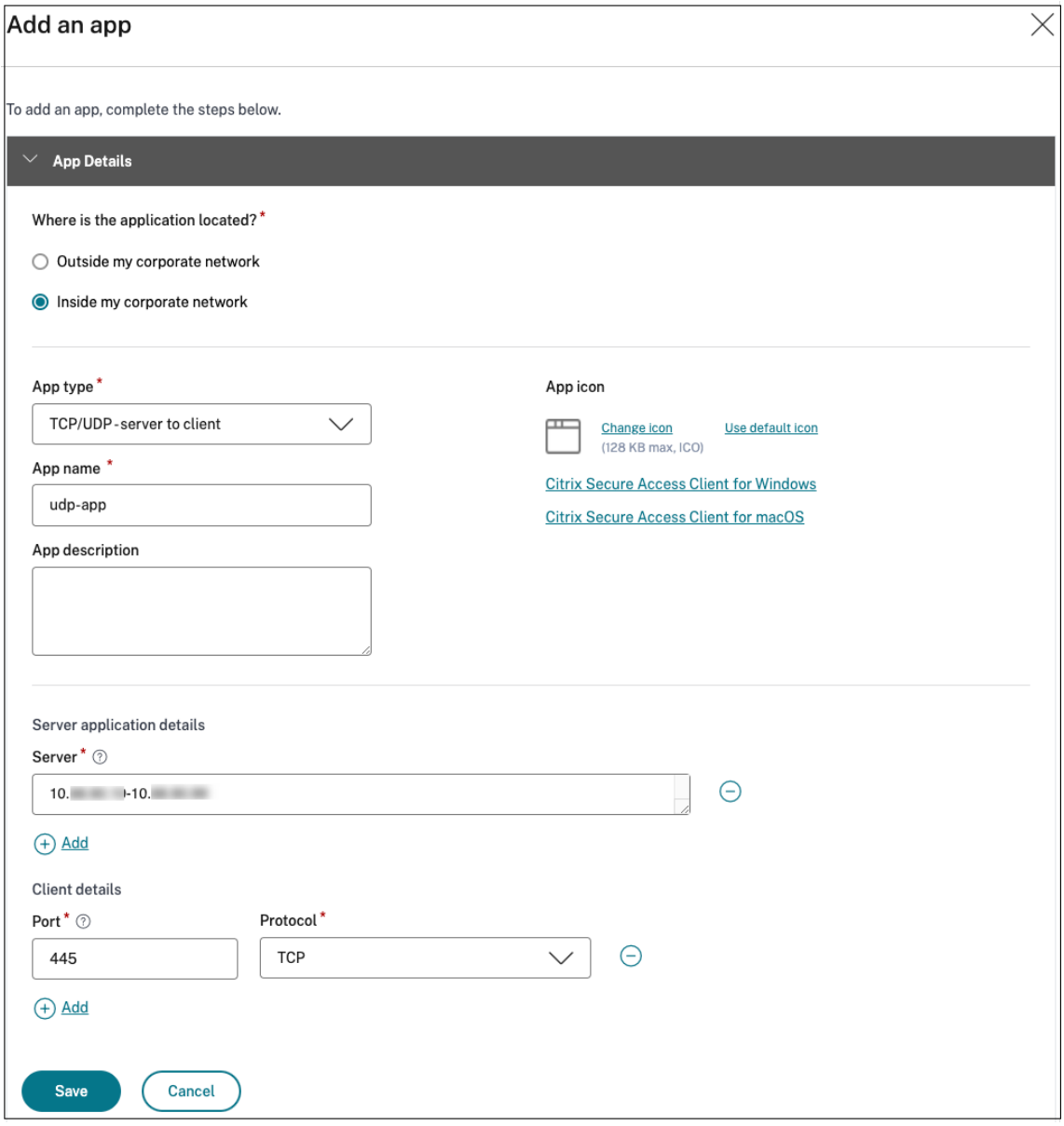
```
set vpn sessionAction AC_AG_PLGspaonprem -useMIP NS -useIIP
NOSPILLOVER

bind vpn vserver spaonprem -intranetIP <IP address>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Perform the following steps to configure TCP/UDP apps from the admin console:

1. In the admin console, click **Applications** and then click **Add an app**.
2. Select the location **Inside my corporate network**.



3. Enter the following details:

   - **App type** –Select **TCP/UDP - server to client**.
   - **App name**–Name of the application.
   - **App description** –Description of the app you are adding. This field is optional.
   - **Server** - Details of the application servers that are authorized to establish connection with the client. You can enter the IP address, IP address range, or the CIDR.
   - **Port** –The client port number.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

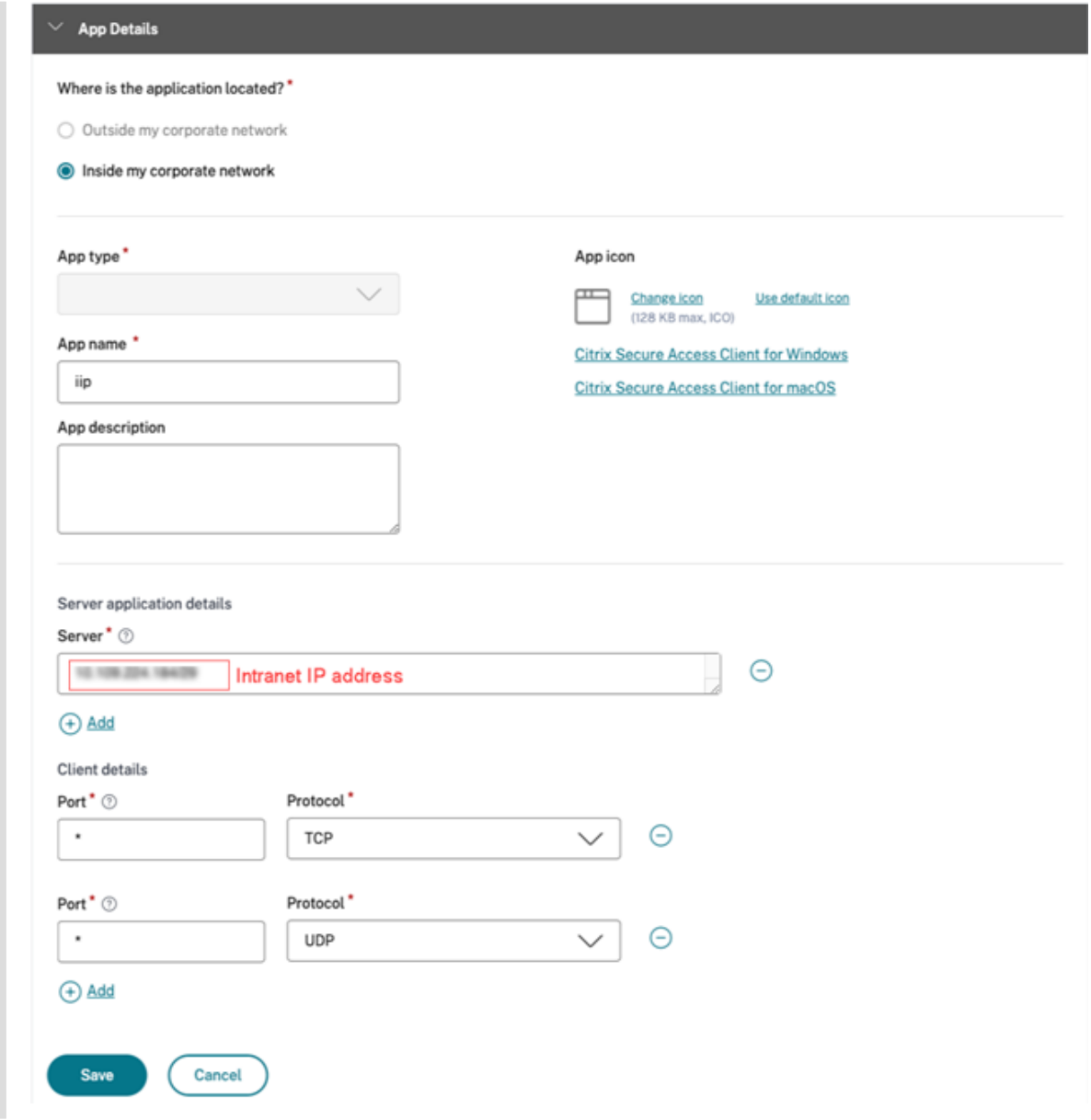
- **Protocol** –TCP/UDP.

4. Click **Add** to add additional servers.
5. Click **Save**. The app is added to the **App Configuration** page. You can edit or delete an app from the **Applications** page after you have configured the application. To do so, click the ellipsis button in line with the app and select the actions accordingly.

   - **Edit Application**
   - **Delete**

> **Important:**
>
> After you add an app for server-client communication, intranet IP address ranges configured on NetScaler Gateway must be added as a TCP/UDP app to enable server-client and client-client communication.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Next steps

Configure access policies for the applications.

Configure access policies for the applications

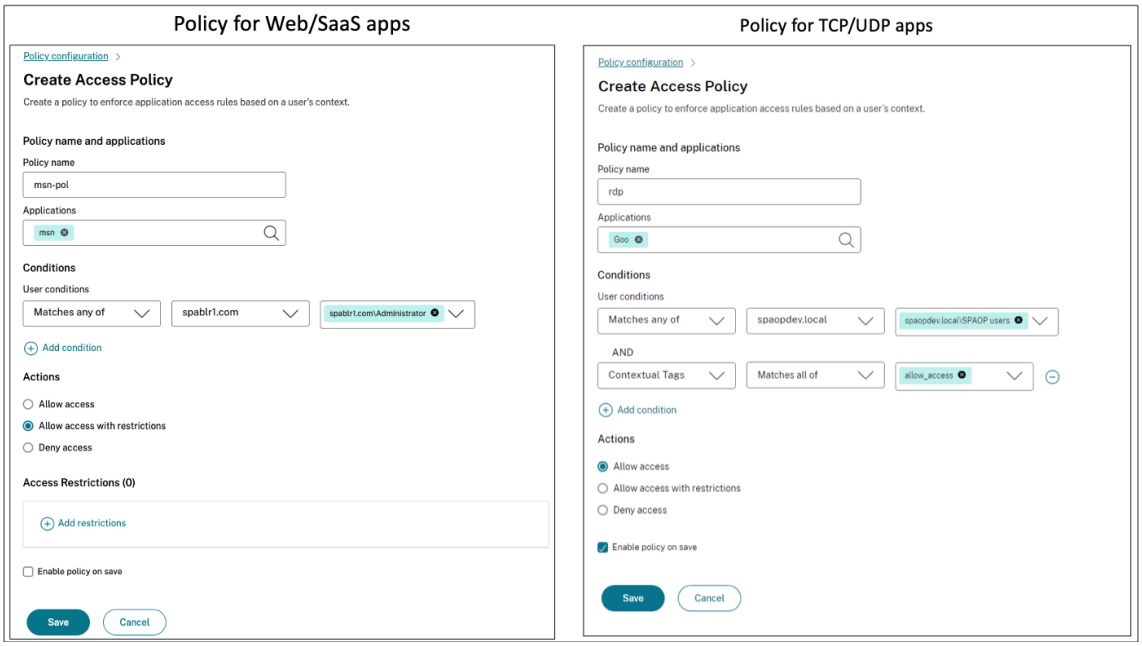
October 14, 2024

Access policies allow you to enable or disable access to the apps based on the user or user groups.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

In addition, you can enable restricted access to the apps (HTTP/HTTPS and TCP/UDP) by adding the security restrictions.

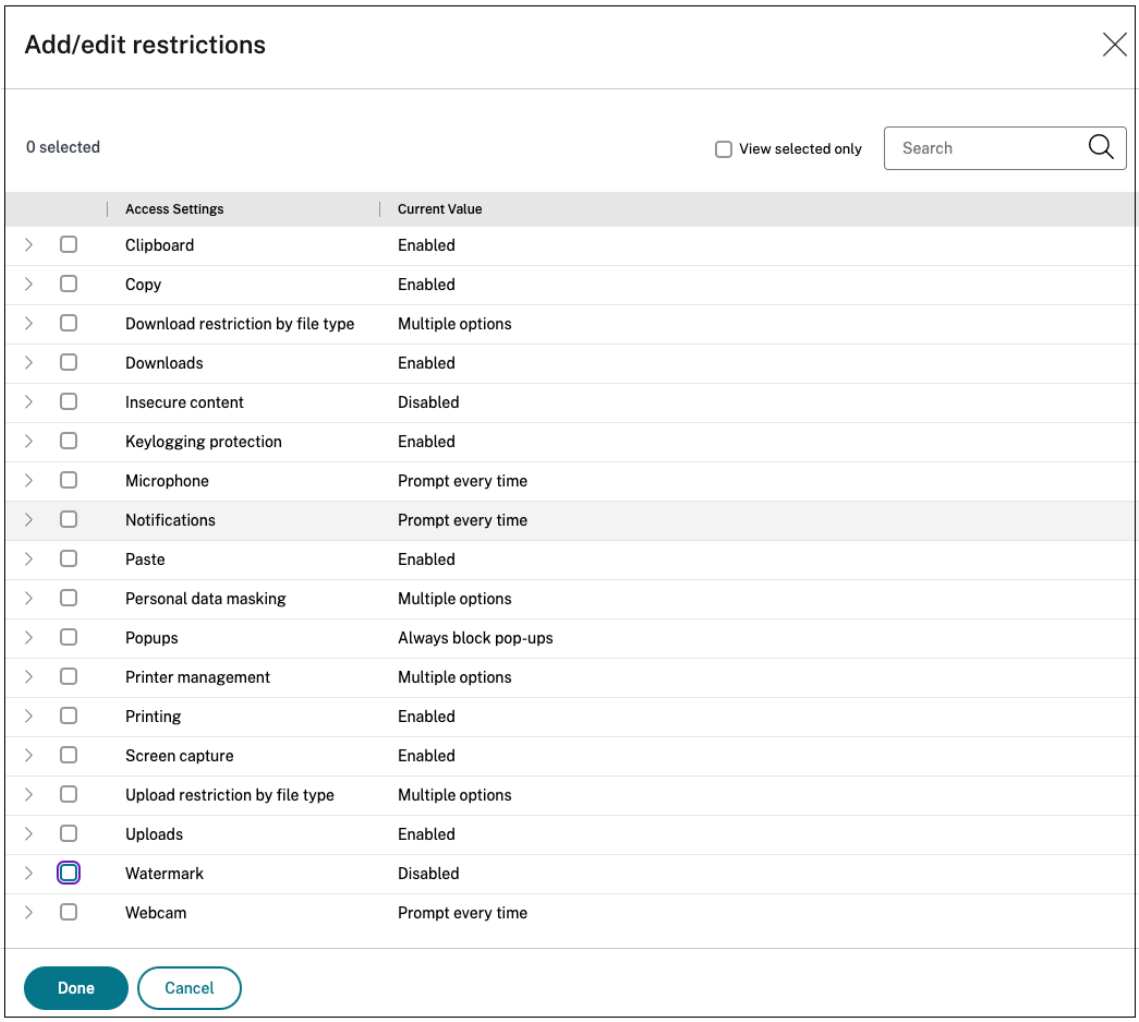
1. In the admin console, click **Access Policies**.
2. Click **Create Policy**.



3. a) In **Policy name**, enter a name for the policy.
4. In **Applications**, select the apps for which you want to enforce the access policies.
5. In **Users conditions** –Select the conditions and users or user groups based on which app access must be allowed or denied.
   - **Matches any of**: Only the users or groups that match any of the names listed in the field are allowed access.
   - **Does not match any**: All users or groups except those listed in the field are allowed access.
6. Click **Add condition** to add another condition based on contextual tags. These tags are derived from the NetScaler Gateway.
7. In **Actions**, select one of the following actions that must be enforced on the app based on the condition evaluation.
   - **Allow access**
   - **Allow access with restriction**
   - **Deny access**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> - The action **Allow access with restriction** is not applicable for the TCP/UDP apps.
> - When you select **Allow access with restrictions**, you must click **Add restrictions** to select the restrictions. For more information on each restriction, see Available access restrictions.



8. Select the restrictions and then click **Done**.
9. Select **Enable policy on save**. If you do not select this option, the policy is only created and not enforced on the applications. Alternatively, you can also enable the policy from the Access Policies page by using the toggle switch.

Access policy priority

After an access policy is created, a priority number is assigned to the access policy, by default. You can view the priority on the Access Policies home page.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

A priority with a lower value has the highest preference and is evaluated first. If this policy does not match the conditions defined, the next policy with the lower priority number is evaluated and so on.

You can change the priority order by moving the policies up or down by using the up-down icon in the **Priority** column.

Next steps

- Validate your configuration from the client machines (Windows and macOS).
- For the TCP/UDP apps, validate your configuration from the client machines (Windows and macOS) by logging into the Citrix Secure Access client.

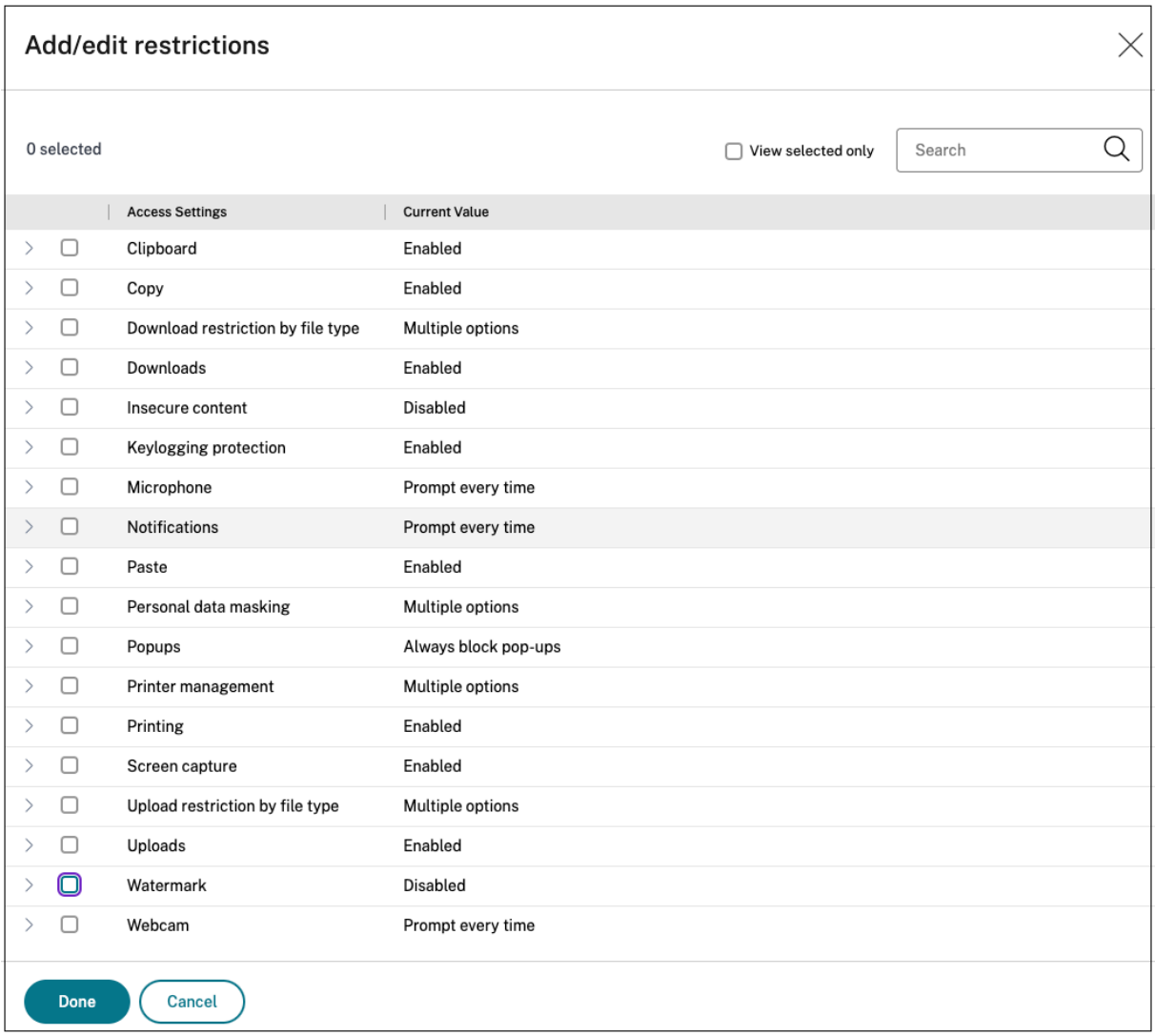
Sample configuration validation

Access restriction options

October 13, 2024

When you select the action **Allow access with restrictions**, you can select the security restrictions as per the requirement. These security restrictions are predefined in the system. Admins cannot modify or add other combinations.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Clipboard

Enable/disable cut/copy/paste operations on a SaaS or internal web app with this access policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

Copy

Enable/disable copying of data from a SaaS or internal web app with this access policy when accessed via the Citrix Enterprise browser. Default value: Enabled.

> **Note:**
>
> - If both **Clipboard** and **Copy** restrictions are enabled in a policy, the **Clipboard** restriction

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

takes precedence over the **Copy** restriction.
- End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.
- For granular control of copy operations within the apps, admins can use the **Security groups** restriction. For details, see Clipboard restriction for security groups.

Downloads

Enable/disable the user's ability to download from within the SaaS or internal web app with this policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

Note:

- If you have disabled the **Download** restriction for the end user, the end users can request download access from within the app when accessed via Citrix Enterprise Browser. For details, see Download access by request.
- If both **Downloads** and **Download restriction by file type** restrictions are enabled in a policy, the **Downloads** restriction takes precedence over the **Download restriction by file type**.

Download restriction by file type

Enable/disable the user's ability to download specific MIME (file) type from within the SaaS or internal web app with this policy when accessed via Citrix Enterprise Browser.

Note:

- The **Download restriction by file type** restriction is available in addition to the **Download** restriction.
- If both **Downloads** and **Download restriction by file type** restrictions are enabled in a policy, the **Downloads** restriction takes precedence over the **Download restriction by file type** restriction.
- End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

To enable downloading of MIME types, perform the following steps:

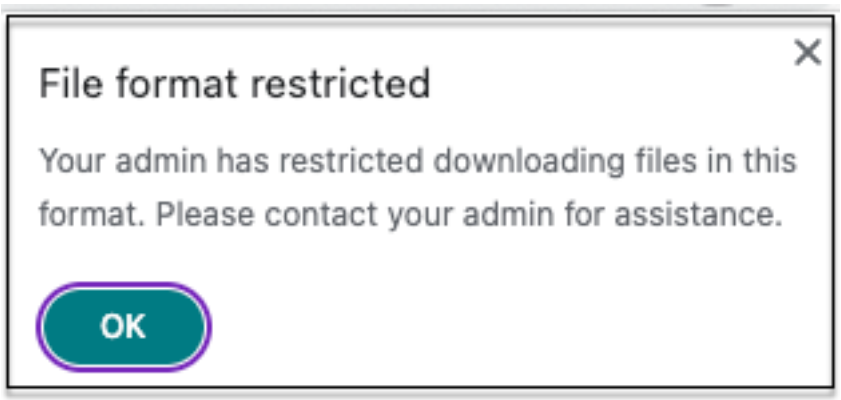
1. Create or edit an access policy. For details on creating an access policy, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Download restriction by file type** and then click **Edit**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. In the **Download restriction by file type settings** page, select one of the following:
   - **Allow all downloads with exceptions** –Select the types that must be blocked and allow all other types.
   - **Block all downloads with exceptions** –Select only the types that can be uploaded and block all other types.
5. If the file type does not exist in the list, then do the following:
   a) Click **Add custom MIME types**.
   b) In **Add MIME types**, enter the MIME type in the format `category/subcategory<extension>`. For example, `image/png`.
   c) Click **Done**.

   The MIME type now appears in the list of exceptions.

When an end user tries to download a restricted file type, Citrix Enterprise Browser displays the following warning message:



Insecure content

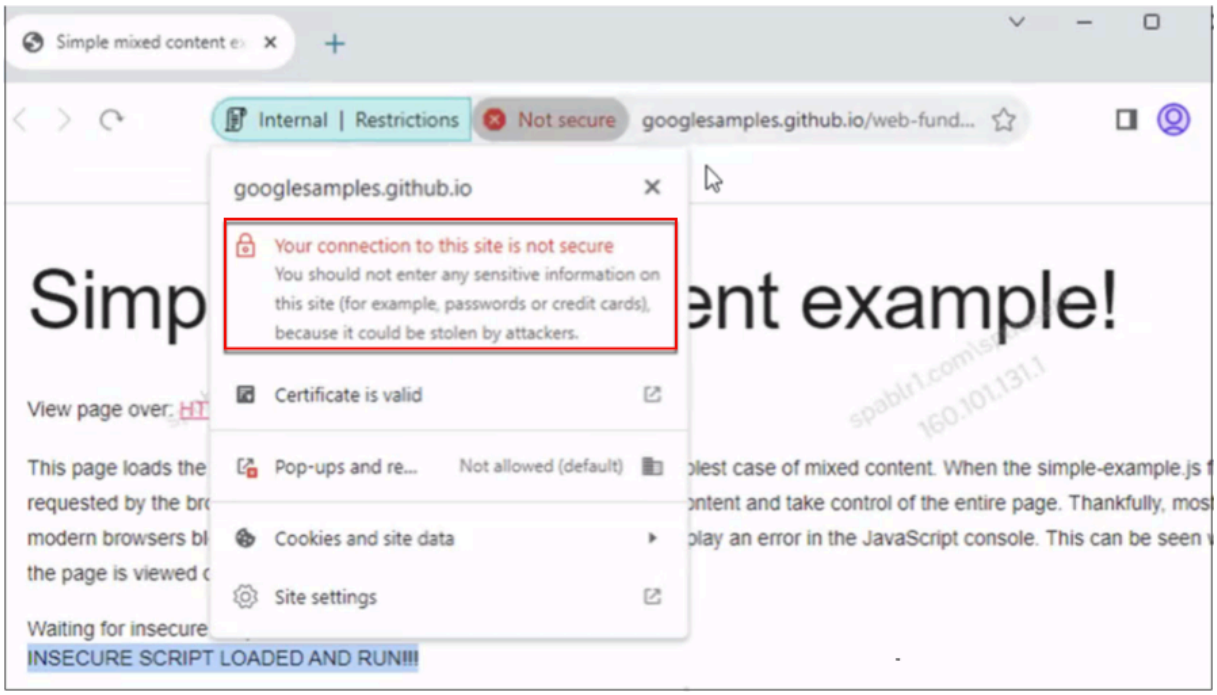
Enable/disable end users from accessing insecure content within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. Insecure content is any file linked to from a webpage using an HTTP link rather than an HTTPS link. Default value: Disabled.

To enable viewing insecure content, perform the following steps:

1. Create or edit an access policy. For details on creating an access policy, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Insecure content**.
4. Click **Save**, and then click **Done**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

The following figure displays a sample notification when you access an insecure content.



Keylogging protection

Enable/disable keyloggers from capturing keystrokes from the SaaS or internal web app with this access policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

Microphone

Prompt/do not prompt users every time to access the microphone within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. Default value: Prompt every time.

End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which the **Microphone** restriction is enabled.

To allow microphone every time without being prompted, perform the following steps:

1. Create or edit an access policy. For details, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Microphone** and then click **Edit**.
4. In the **Microphone settings** page, click **Always allow access**.
5. Click **Save**, and then click **Done**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> - If the **Microphone** restriction is enabled in the Secure Private Access policy, then Citrix Enterprise Browser displays the settings **Allow**.
> - If the option **Prompt every time** in the Secure Private Access policy, then the setting applied on Citrix Enterprise Browser varies depending on whether the Global App Configuration service (GACS) is used to manage Citrix Enterprise Browser.
>
> - If GACS is used, then the GACS setting is applied on Citrix Enterprise Browser.
> - If GACS is not used, then Citrix Enterprise Browser displays the setting **Ask**.
>
> - Currently, Secure Private Access does not support blocking of the microphone. If you must block a microphone, you must do it through GACS.

For more information on GACS, see Manage Citrix Enterprise Browser through Global App Configuration service.

Notifications

Allow/prompt users every time to view the notifications within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. Default value: Prompt every time.

End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled.

To block the display of notifications without prompting, perform the following steps.

1. Create or edit an access policy. For details, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Notifications** and then click **Edit**.
4. In the **Notification settings** page, click **Always block notifications**.
5. Click **Save**, and then click **Done**.

Paste

Enable/disable pasting of copied data into the SaaS or internal web app with this access policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

> **Note:**
>
> - If both **Clipboard** and **Paste** restrictions are enabled in a policy, the **Clipboard** restriction

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

takes precedence over the **Paste** restriction.
- End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.
- For granular control of paste operations within the apps, admins can use the **Security groups** restriction. For details, see Clipboard restriction for security groups.

Personal data masking

Enable/disable redacting or masking personally identifiable information (PII) on the SaaS or internal web app with this policy when accessed via Citrix Enterprise Browser.

> **Note:**
>
> End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

To redact or mask personally identifiable information, perform the following steps:

1. Create or edit an access policy. For details, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Personal data masking** and then click **Edit**.
4. Select the information type that you want to obscure or mask and then click **Add**.

   If the information type does not appear in the pre-defined list, then you can add a custom information type. For details, see Add custom information type.
5. Select the masking type.

   - **Full masking** –Completely cover the sensitive information to make it unreadable.
   - **Partial masking** –Partially cover the sensitive information. Only the relevant sections are covered leaving the rest intact.

     When you select **Partial marking**, you must select characters starting from the beginning or the end of the document. You must enter the numbers in the **First masked characters** and **Last masked characters** fields.

     The **Preview** field displays the masking format. This preview is not available for custom policies.
6. Click **Save** and then click **Done**.

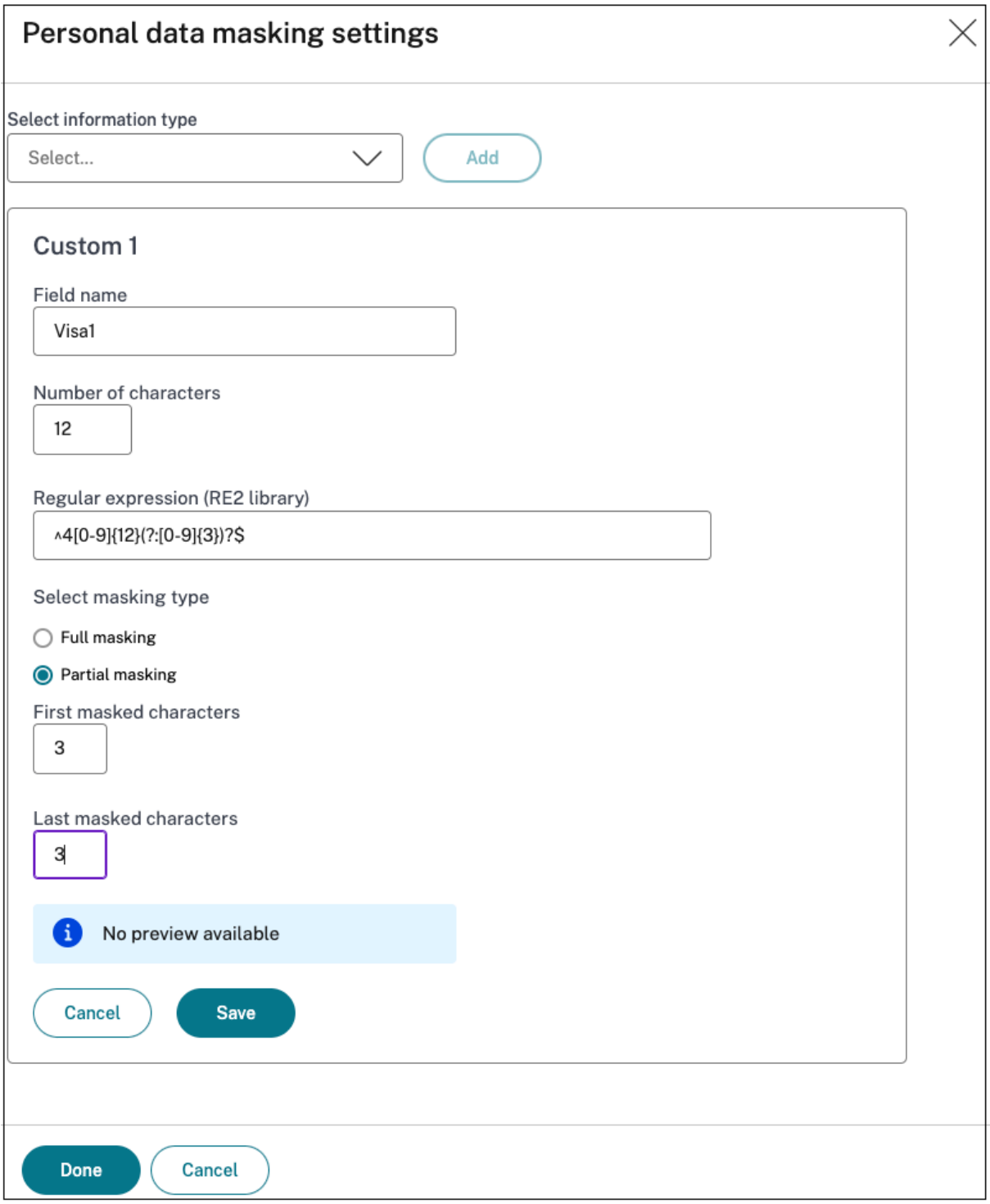
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Add custom information type

You can add a custom information type by adding the information type's regular expression.

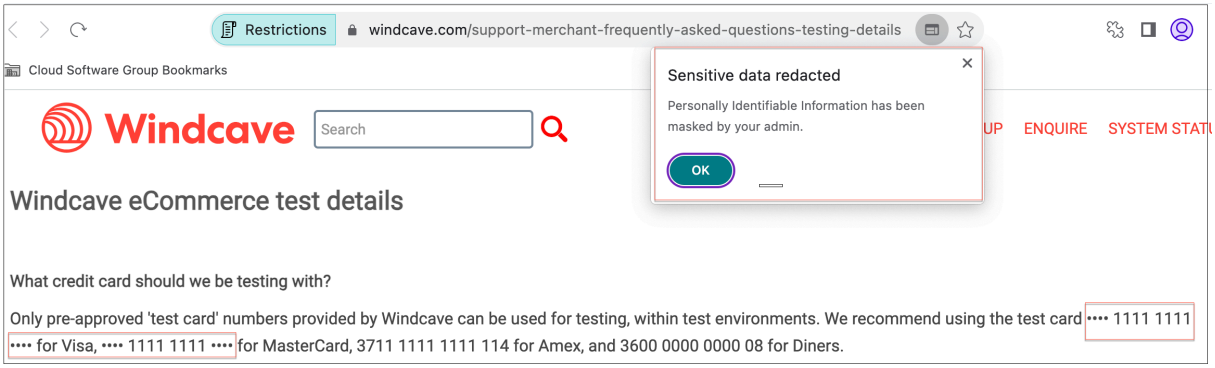
1. In **Select Information type**, select **Custom**, and then click **Add**.
2. In **Field name**, enter the name for the information type that you want to mask.
3. In **Number of characters**, enter the number of characters of the information type.
4. In **Regular Expression (RE2 library)**, enter the expression for the custom information type. For example, `^4[0-9]{ 12 } (?:[0-9]{ 3 } )?$`.
5. Select a masking type, if you want to mask the complete information or the first or last few characters.
6. Click **Save**, and then click **Done**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



The following figure displays a sample app in which the PII is masked. The figure also displays the notification related to masking of the PII.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Popups

Enable/disable the display of popups within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. By default popups are disabled within webpages. Default value: Always block pop-ups.

End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled.

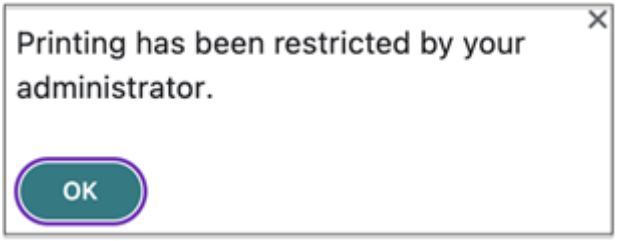
To enable display of popups, perform the following steps:

1. Create or edit an access policy. For details, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Popups** and then click **Edit**.
4. In the **Popups settings** page, click **Always allow pop-ups**.
5. Click **Save**, and then click **Done**.

Printing

Enable/disable printing data from the configured SaaS or Internal web apps with this policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

The following message appears when an end user tries to print content from the application for which the printing restriction is enabled.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> - If you have disabled the printing option for the end user, the end users can request printing access from within the app when accessed via Citrix Enterprise Browser. For details, see Print access by request.
> - If both **Printing** and **Printer management** restrictions are enabled in a policy, the **Printing** restriction takes precedence over the **Printer management** restriction.

Printer management

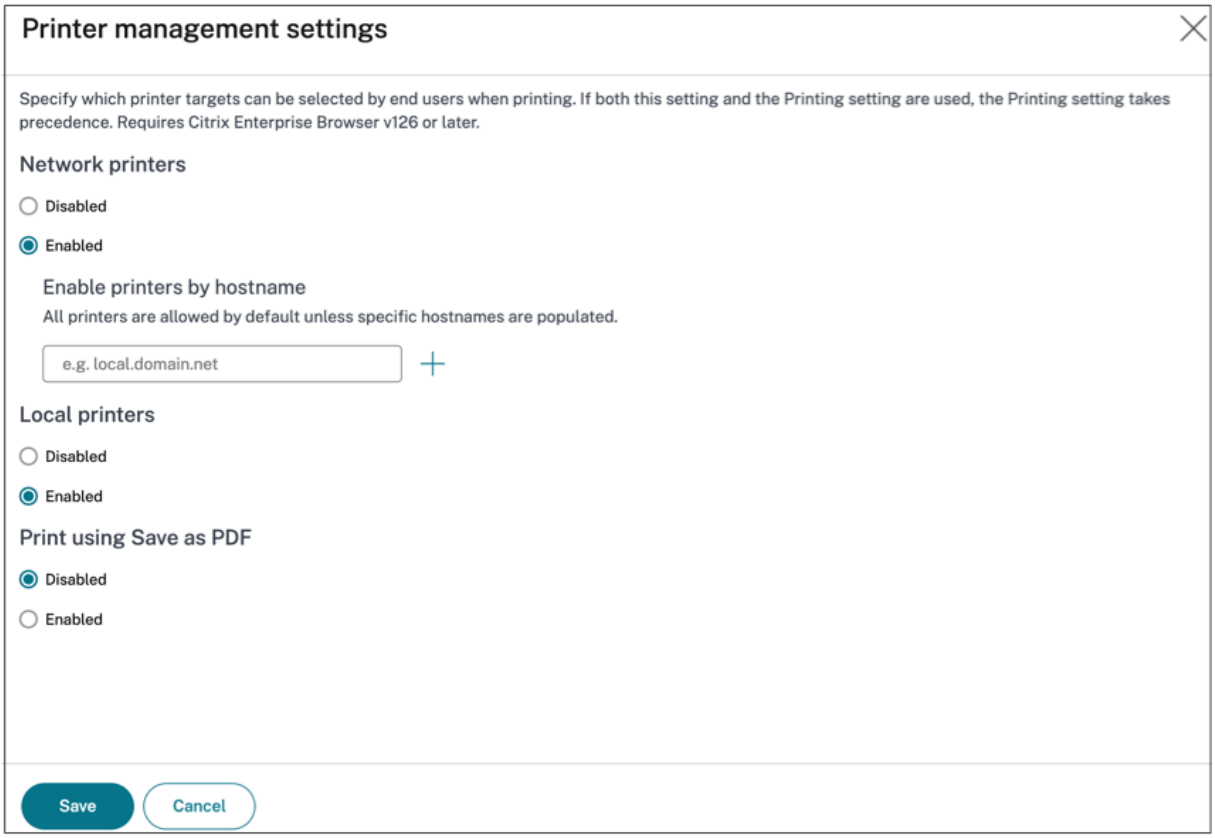
Enable/disable printing data by using the admin-configured printers from the configured SaaS or internal web apps with this policy when accessed via Citrix Enterprise Browser.

> **Note:**
>
> - The **Printer management** restriction is available in addition to the **Printing** restriction where printing is either enabled or disabled.
>
> If both **Printing** and **Printer management** restrictions are enabled in an access policy, the **Printing** restriction takes precedence over the **Printer management** restriction.
> - End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

To enable/disable printing restrictions, perform the following steps:

1. Create or edit an access policy. For details on creating an access policy, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Printer management** and then click **Edit**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. Select the exceptions as per your requirement.

   - **Network printers** - A network printer is a printer that can be connected to a network and used by multiple users.

     - **Disabled:** Printing from any printers in the network is disabled.
     - **Enabled:** Printing from all network printers is enabled. If printer host names are specified, then all other network printers apart from the ones specified are blocked.

     Note: Network printers are identified by their host names.

   - **Local printers** - A local printer is a device directly connected to an individual computer through a wired connection. This connection is typically facilitated through USB, parallel ports, or other direct interfaces.

     - **Disabled:** Printing from all local printers is disabled.
     - **Enabled:** Printing from all local printers is enabled.

   - **Print using Save as PDF**

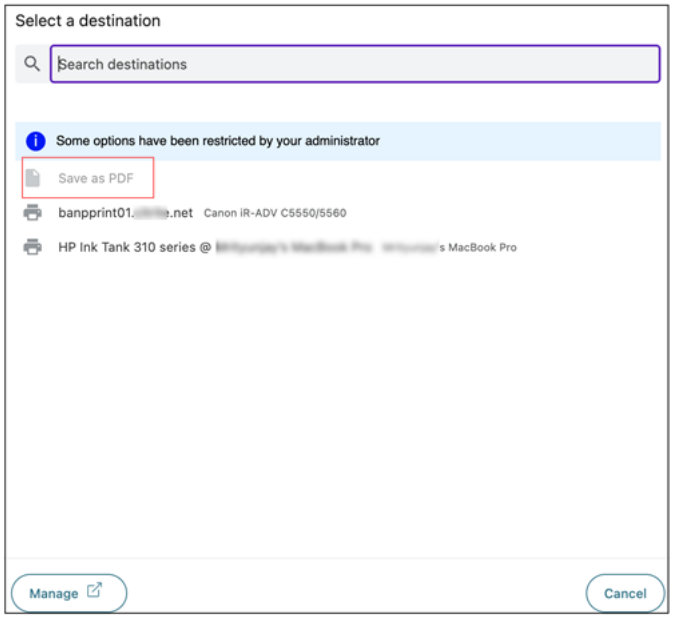
     - **Disabled**: Saving the content from the application in a PDF format is disabled.
     - **Enabled:** Saving the content from the application in a PDF format is enabled.

2. Click **Save**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

If a network printer is disabled, then the specific printer name appears grayed out when you try to select the printer in the **Destination** field.

Also, if **Print using Save as PDF** is disabled, then when you click the **See more** link in the **Destination** field, the **Save as PDF** option appears grayed out.



Screen capture

Enable/disable the ability to capture the screens from the SaaS or internal web app with this policy when accessed via Citrix Enterprise Browser using any of the screen capture programs or apps. If a user tries to capture the screen, a blank screen is captured. Default value: Enabled.

Upload restriction by file type

Enable/disable the user's ability to download specific MIME (file) type from the SaaS or internal web app with this policy when accessed via Citrix Enterprise Browser.

> **Note:**
>
> - The **Upload restriction by file type** restriction is available in addition to the **Upload** restriction.
> - If both **Upload** and **Upload restriction by file type** restrictions are enabled in a policy, the **Uploads** restriction takes precedence over the **Upload restriction by file type** restriction.
> - End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To enable/disable uploading of MIME types, perform the following steps:

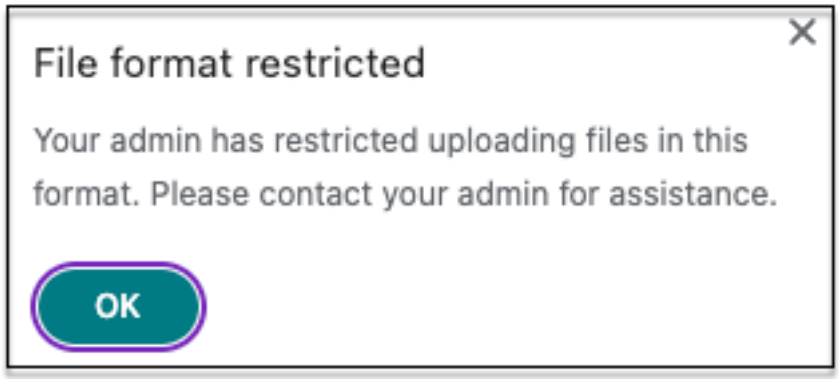
1. Create or edit an access policy. For details, see Create access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Upload restriction by file type** and then click **Edit**.
4. In the **Upload restriction by file type settings** page, select one of the following:

   Allow all uploads with exceptions –Upload all files except the selected types.
   Block all uploads with exceptions –Blocks all file types from uploading except the selected types.
5. If the file type does not exist in the list, then do the following:

   a) Click **Add custom MIME types**.
   b) In **Add MIME types**, enter the MIME type in the format `category/subcategory<extension>`. For example, `image/png`.
   c) Click **Done**.

   The MIME type now appears in the list of exceptions.

When an end user tries to upload a restricted file type, Citrix Enterprise Browser displays a warning message.



Uploads

Enable/disable the user's ability to upload within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

> **Note:**
>
> If both **Uploads** and **Upload restriction by file type** restrictions are enabled in a policy, the **Uploads** restriction takes precedence over the **Upload restriction by file type** restriction.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Watermark

Enable/disable the watermark on the user's screen displaying the user name and IP address of the user's machine. Default value: Disabled.

Webcam

Prompt/do not prompt users every time to access the webcam within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. Default value: Prompt every time.

End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which the **Webcam** restriction is enabled.

To allow webcam every time without being prompted, perform the following steps:

1. Create or edit an access policy. For details, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Webcam** and then click **Edit**.
4. In the **Webcam settings** page, click **Always allow access**.
5. Click **Save**, and then click **Done**.

> **Note:**
>
> - If the Webcam restriction is enabled in the Secure Private Access policy, then Citrix Enterprise Browser displays the settings **Allow**.
> - If the option **Prompt every time** in Secure Private Access policy, then the setting applied on Citrix Enterprise Browser varies depending on whether the Global App Configuration service (GACS) is used to manage Citrix Enterprise Browser.
>
> - If GACS is used, then the GACS setting is applied on Citrix Enterprise Browser.
> - If GACS is not used, then Citrix Enterprise Browser displays the setting **Ask**.
>
> - Currently, Secure Private Access does not support blocking of the webcam. If you must block webcam, you must do it through GACS.

For more information on GACS, see Manage Citrix Enterprise Browser through Global App Configuration service.

Clipboard restriction for security groups

You can enable clipboard access for a designated group of apps by using the **Security groups** restriction **(Applications > Security groups)**. Security groups are assigned a set of apps within which the

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

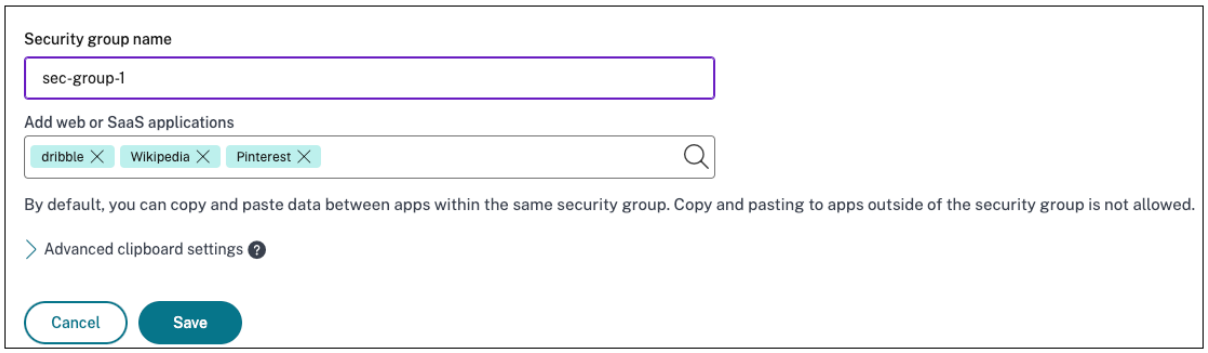
copy and paste operations can be performed. To enable clipboard access within the apps in a security group, you must just have an access policy configured with the action **allow** or **allow with restrictions** without selecting any access setting.

- When the **Security groups** restriction is enabled, you cannot copy / paste data between applications in different security groups. For example if the app "ProdDocs"belongs to security group "SG1"and the app "Edocs"belong to security group "SG2", you cannot copy / paste content from "Edocs"to "ProdDocs"even if **Copy** / **Paste** restriction is enabled for both groups.
- For apps not part of a security group, you can have an access policy created with action **allow with restrictions** and selecting the restrictions (**Copy**, **Paste**, or **Clipboard**). In this case, the app is not part of a security group and hence the **Copy** / **Paste** restriction can be applied on that app.

> **Note:**
>
> You can also restrict clipboard access for apps accessed via Citrix Enterprise Browser through the Global App Configuration service (GACS). If you are using GACS to manage Citrix Enterprise Browser, then use the **Enable Sandboxed Clipboard** option to manage the clipboard access. When you restrict clipboard access through GACS, it applies to all apps accessed via Citrix Enterprise Browser. For more information on GACS, see Manage Citrix Enterprise Browser through Global App Configuration service.

To create a security group, perform the following steps:

1. In the Secure Private Access console, click **Applications** and then click **Security groups**.
2. Click **Add a new security group**.



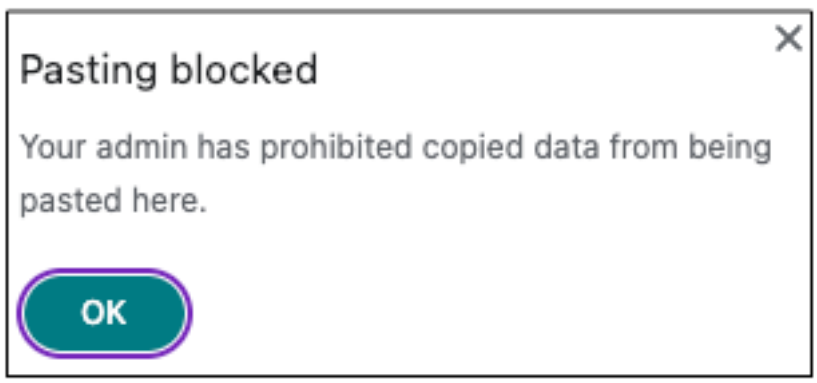
1. Enter a name for the security group.
2. In **Add web or SaaS applications**, choose the applications that you want to group to enable the copy and paste control. For example, Wikipedia, Pinterest and Dribble.
3. Click **Save**.

For details on Advanced clipboard settings, see Enable copy / paste controls for native applications and unpublished apps.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

When end users launch these applications (Wikipedia, Pinterest and Dribble) from Citrix Workspace, they must be able to share data (copy / paste) from one application to the other applications within the security group. The copy / paste occurs irrespective of other security restrictions that are already enabled for the applications.

However, end users cannot copy and paste content from their local applications on their machines or unpublished applications to these designated applications and conversely. The following notification appears when the content is copied from the designated application into another application:



> **Note:**
>
> You can enable copy / paste content from local applications on user machines or unpublished applications controls by using the options in the **Advanced clipboard settings** section. For details, see Enable copy / paste controls for native applications and unpublished apps.

Enable granular level copy / paste

You can enable granular level clipboard access within the applications in a designated group. You can do so by creating access policies for the applications and enabling the **Copy** / **Paste** restriction as per your requirement.

> **Note:**
>
> Ensure that the specific access policy that you have created for granular level clipboard access has a higher priority than the policy that you have created for the security groups.

Example:

Consider that you have created a security group with three applications namely, Wikipedia, Pinterest, and Dribble.

Now, you want to restrict the pasting of content from Wikipedia or Dribble into Pinterest. To do so, perform the following steps:

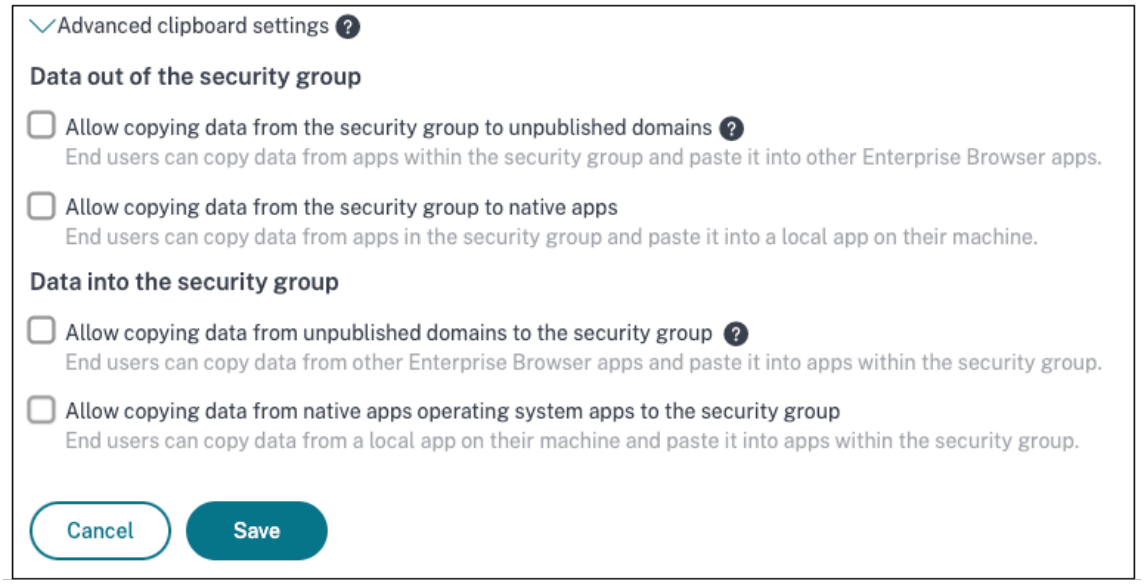
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Create or edit an access policy assigned for the application `Pinterest`. For details on creating an access policy, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Select **Paste**.

Although Pinterest is part of a security group which also contains Wikipedia and Dribble, users cannot copy content from Wikipedia or Dribble to Pinterest because of the access policy associated with Pinterest in which the **Paste** restriction is enabled.

Enable copy / paste controls for native applications and unpublished apps

1. Create a security group. For details, see Clipboard security groups for Copy and Paste restrictions.
2. Expand **Advanced clipboard settings**.



3. Select the following options as per your requirement:

   - **Allow copying of data from the security group to unpublished domains** –Enable copying of data from applications in the security groups to the apps that are not published in Secure Private Access.
   - **Allow copying of data from the security group to native apps** - Enable copying of data from the applications in the security groups to the local applications on your machines.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Allow copying of data from the unpublished domains to the security group** –Enable copying of data from the apps not published through Secure Private Access to the applications in the security groups.
- **Allow copying of data from native apps operating system the security group** - Enable copying of data from local applications on the machines to the applications.

Known issues

- The routing table in (**Settings > Application Domain**) retains the domains of a deleted application. Hence, these applications are also considered as published applications in Secure Private Access. If these domains are accessed directly from Citrix Enterprise Browser, copy / paste is disabled from these applications irrespective of the options that you have selected in **Advanced clipboard settings**.

  For example, assume the following scenario:

  - You have deleted an application named Jira2 (`https://test.citrite.net`) that was part of a security group.
  - You have enabled the option **Allow copying of data from the security group to unpublished domains**.

  In this scenario, if the user tries to copy data from this application into another application in the same security group, the pasting control is disabled. A notification regarding the same is displayed to the user.
- For a SaaS app, the app access can be denied if the application is configured with an access policy with action **Deny access.** The end users can still access the app because the app traffic is not tunneled through Secure Private Access. Also, if the application is part of the security group, the security group settings are not honored and hence you cannot copy / paste content from the application.

End user flow

October 13, 2024

SaaS app

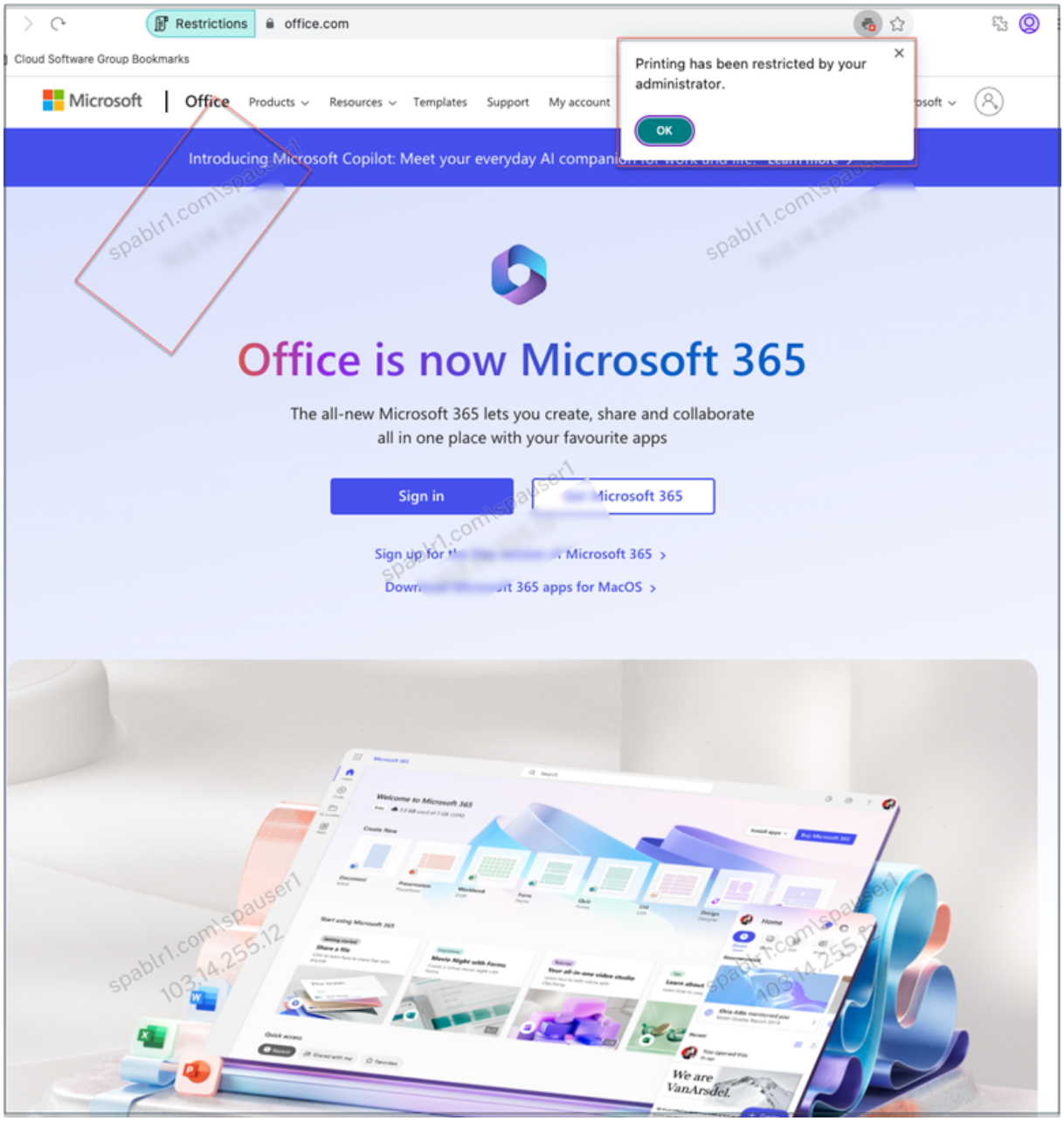
Assume that an admin has configured the Office 365 app with the watermark and print restriction for the end user. Now, when the end user accesses the Office 365 app, the watermark and print restrictions must be applied on the app.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

The end user must perform the following steps to access the Office 365 app:

1. Access the StoreFront store from the Citrix Workspace app.
2. Log on to the store.
3. Click the **Apps** tab, and then click the **Office365** application.

   The end user must now notice that the Office 365 application is launched and contains the watermark. Also, if the end user tries to print some data from the Office 365 application, the print restriction message must be displayed to the user.



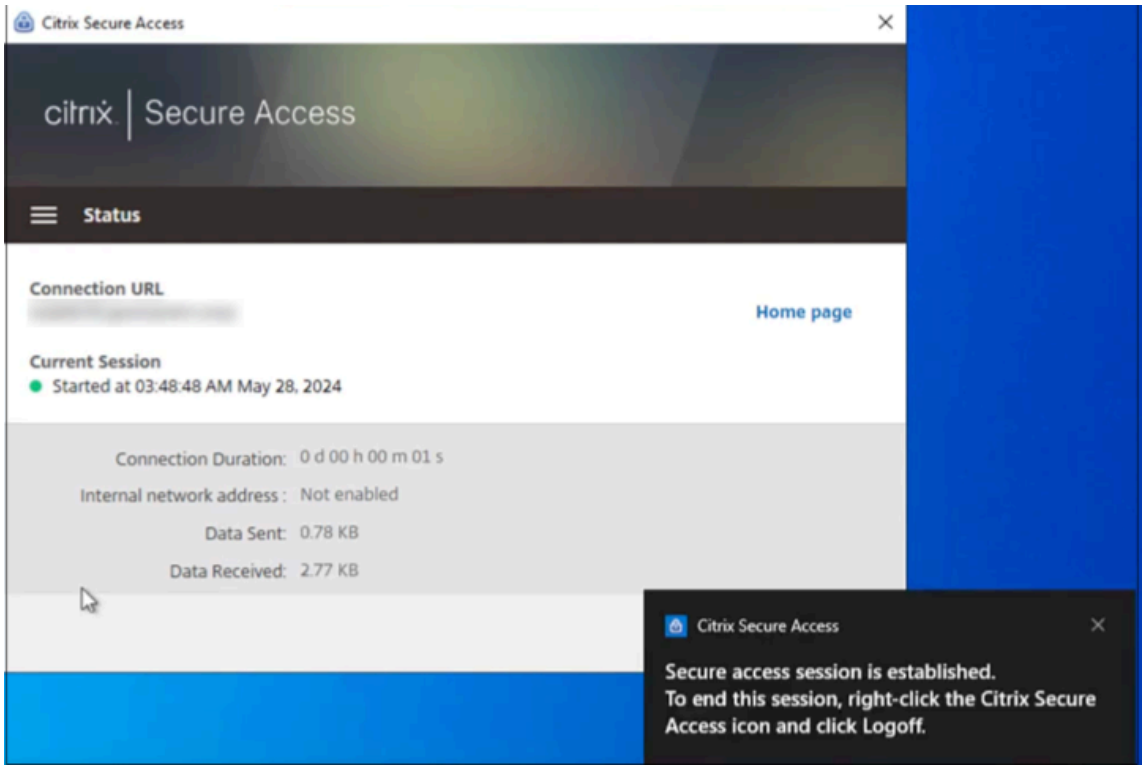
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> Administrators must provide users with the account information that they need to access virtual desktops and applications. For details, see Adding store URL to Citrix Workspace app.

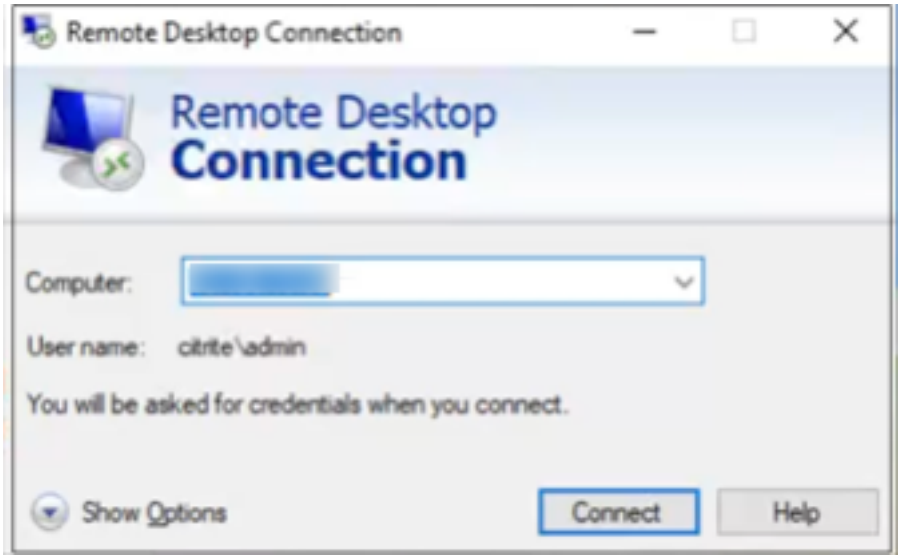
TCP/UDP app

If RDP is configured, end users must perform the following steps to access the TCP/UDP app.

1. Log in to the Citrix Secure Access client.
2. After the secure access session is established, start a remote desktop connection.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



a) Press the **Windows** key, type **Remote Desktop Connection**, and press **Enter**.
b) Enter the IP address or host name of the computer that you trying to connect to.
c) Click **Connect**. You might be prompted to enter the credentials.
d) Enter the user name and password for the remote computer and then click **OK**.

A remote desktop connection is established now and the end user can interact with the remote computer.

Advanced features

October 28, 2024

Secure Private Access service supports the following advanced features.

Application Discovery: The Application Discovery feature helps an admin get visibility into the external and internal applications (HTTP/HTTPS and TCP/UDP apps) that are being accessed in an organization. This feature discovers and lists all the domains/IPs addresses, published or unpublished. Thus, admins can see what domains/IP addresses are getting accessed, by whom, and decide if they want to publish them as applications, providing access to those users. For details, see Discover domains or IP addresses accessed by end users.

Policy modeling tool: The policy modeling tool (**Access policies > Policy modeling**) provides the administrators full visibility into the expected application access result (allowed/allowed with restriction/denied). Admins can check the access results for specific users and add a user condition for contextual tags. For details, see Policy modeling tool.

Support for unsanctioned websites: Applications (intranet or internet) that are not configured within Secure Private Access are regarded as "Unsanctioned Websites". By default, Secure Private

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Access denies access to all intranet web applications if there are no applications and access policies configured for those applications. For all other internet URLs or SaaS applications that do not have an app configured, admins can use the **Settings > Unsanctioned Websites** tab from the admin console to allow or deny access via Citrix Enterprise Browser. For details, see Unsanctioned websites.

Discover domains or IP addresses accessed by end users

October 13, 2024

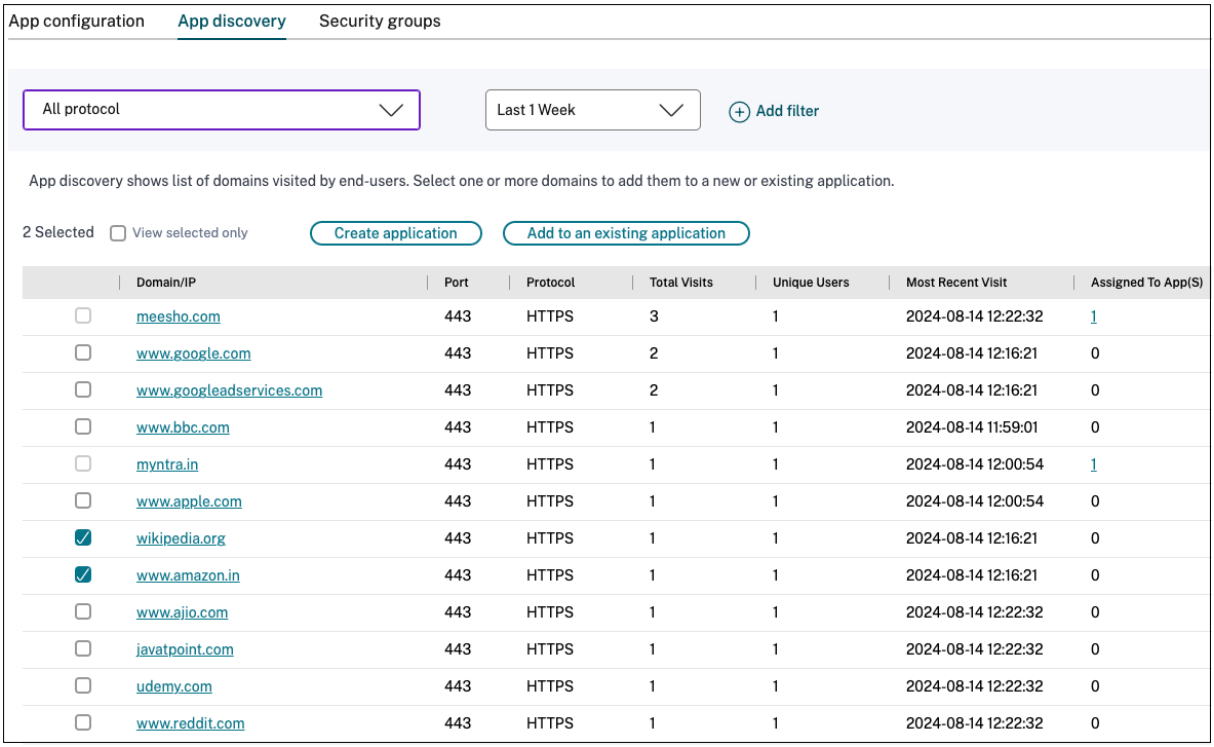
The Application Discovery feature helps an admin get visibility into the external and internal applications (HTTP/HTTPS and TCP/UDP apps) that are being accessed in an organization. This feature discovers and lists all the domains/IPs addresses, published or unpublished. Thus, admins can see what domains/IP addresses are getting accessed, by whom, and decide if they want to publish them as applications, providing access to those users.

The Application Discovery feature provides the following capabilities to the admins:

- Provides visibility into both internal or external domains/IPs addresses accessed by the end users.
- Provides a comprehensive visibility into all types of applications accessed (HTTP, HTTPS, TCP, and UDP). Access Citrix Enterprise Browser and Citrix Secure Access agent are supported.
- Displays both published or unpublished domains/IP addresses accessed by the end users.

The following figure displays a sample **App discovery** page. The **App discovery** page allows filtering of domains based on the protocol (HTTP/HTTPS, TCP/UDP) and Domain/IP address and port numbers. It also displays the unpublished (not assigned to any app) domains accessed by the end users.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



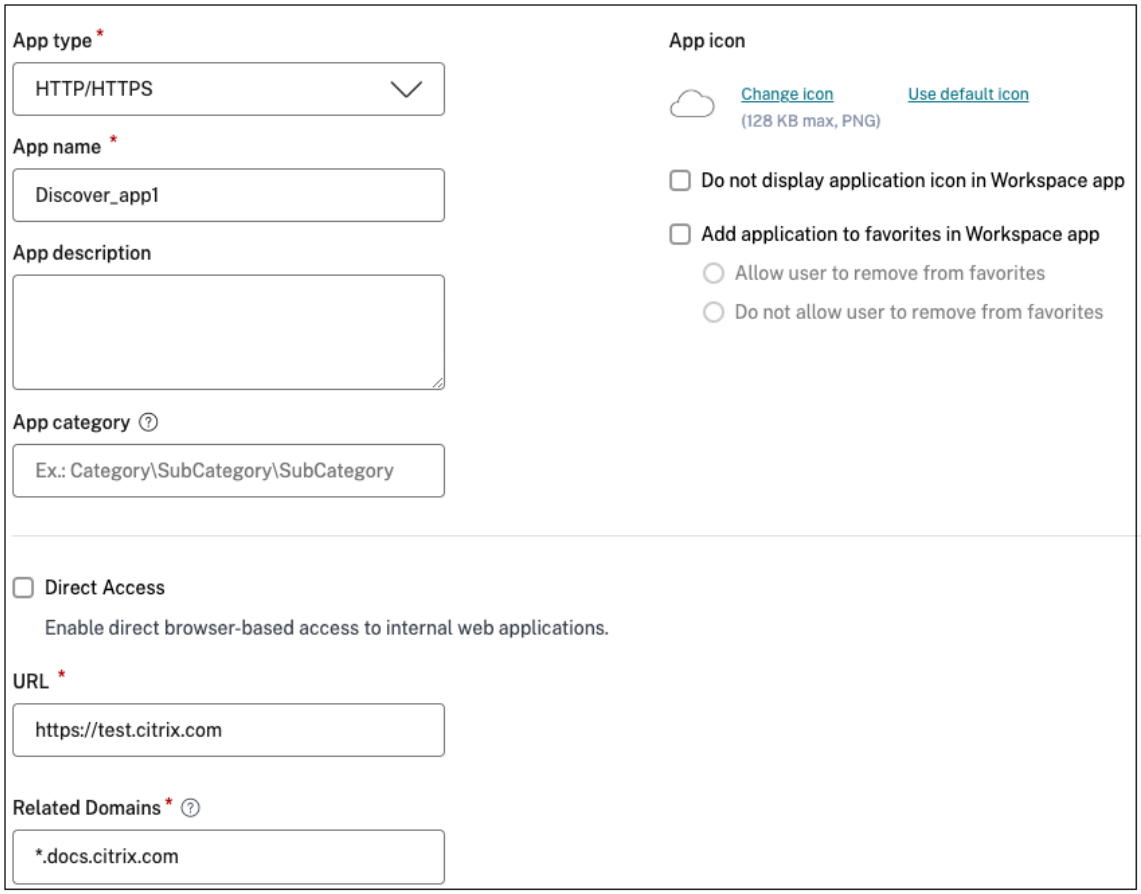
Application Discovery for internal domains in a new environment

The Application Discovery feature can be used if you are setting up a new Secure Private Access environment and want visibility into the applications that are to be configured. This feature discovers and lists all domains/IPs addresses that are accessed by your end users so you can configure them as applications. Use the following steps to enable the Application Discovery feature when you are setting up your Secure Private Access environment:

- To discover internal web applications, configure an application within Secure Private Access and specify the wildcard related domain that belongs to the domain/subdomain of the applications that you want to discover.

  For example, if you want to discover all applications with the domain citrix.com, create an application with a related wildcard domain as `*.citrix.com`. To allow completion of application configuration, add any test URL as the main web app URL section.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



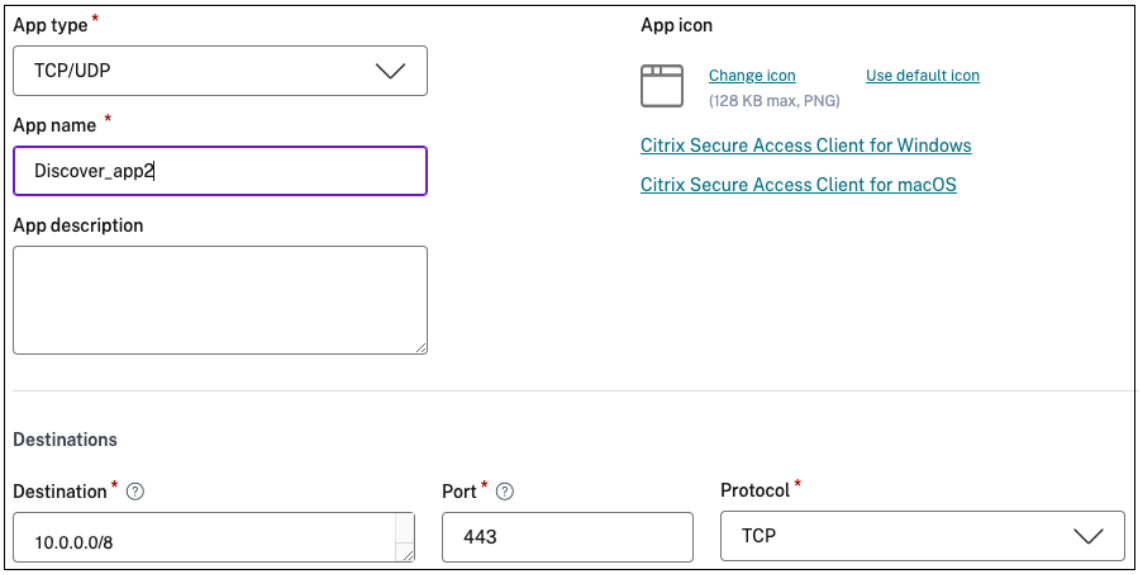
Web app URL: `https://test.citrix.com/`
Related domain: `*.citrix.com`

- For internal TCP/UDP apps, configure an application within Secure Private Access and specify the subnet along with the TCP/UDP protocol and range of ports (enter * to include the entire range). This enables discovering all TCP and UDP apps from the Citrix Secure Access agent. For example, if you want to discover all applications within subnet 10.0.0.0/8, then configure the app with the following details: Example: 10.0.0.0/8:

  Port: (*)

  Protocol: TCP

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Once you have created the applications, you must also define users that are allowed access to apps with the configured domains and IP subnets. Create an access policy and assign users to whom you want to allow access to the FQDNs/IP addresses configured in the applications created. These can be an initial set of test users or a limited number of users you want to give access to initially.
- After creating the applications and corresponding access policies, users can continue to access applications from the Citrix Workspace app and access different domains. All FQDN/IP addresses accessed by the end users start to show up in the Application Discovery page.

> **Note:**
>
> - Once you have discovered and identified most of the applications over a few days/weeks, we recommend deleting the initially created applications so that the wider access given via the wildcard domains and IP subnets can be closed down, and only specific application URLs and IP addresses that are discovered must be allowed access via new applications.
> - Add the prefix `Discover` in the app name to indicate that this is a special app configuration to enable discovery monitoring and reporting. This naming helps you identify to remove the wild card domains or IP subnets or both so you can reduce the overall app access zone to just the specific FQDNs and IP/port combinations later in weeks or a month.
> - To access TCP/UDP apps, users must use the Citrix Secure Access agent. App access from various access methods is monitored based on the apps' domains and subnets configuration and reported within the **App Discovery** page.
> - Even after you have removed the discovered applications, this feature keeps on discovering domains/IP addresses accessed by your users. So at any time, you can come back to the **App Discovery** page to see what is being accessed and if there are any new domains/IP addresses discovered that must be configured as applications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For details on adding the domains, FQDNs, or IP address, see the following topics.

- Configure HTTP/HTTPS applications
- Configure TCP/UDP apps

Create an application from the App discovery page

To create an application for main domains and unpublished domains from the **App discovery** page, do the following steps:

1. Navigate to **Applications > App discovery**.
2. Select a domain from the list.

   > **Note:**
   >
   > - You cannot select domains belonging to different protocols to create an application. An error message is displayed when you select domains belonging to different protocols.
   > - If a domain is already associated with an application, you cannot select that domain again to create an application. The checkbox corresponding to that domain appears grayed out and when you hover the mouse over the checkbox, a tooltip appears.

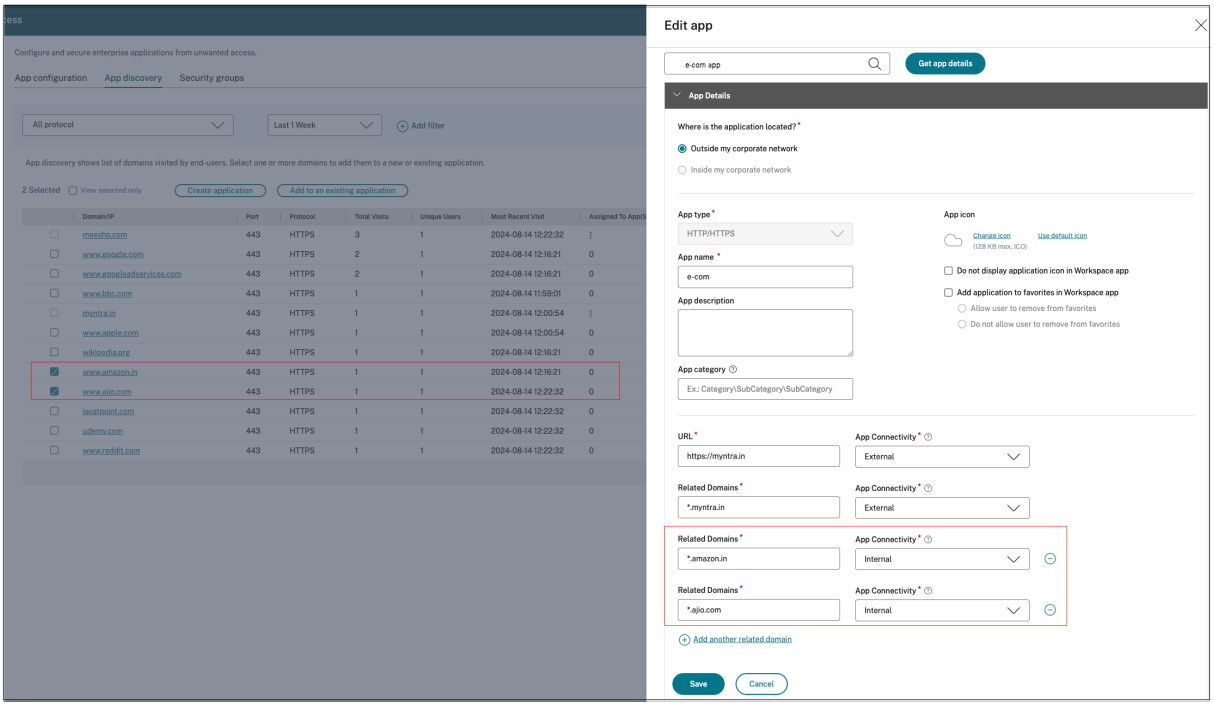
3. Click **Create application**. For details on creating an application, Configure HTTP/HTTPS applications and Configure TCP/UDP apps.

Update an existing application

To add a domain to an existing application, perform the following steps:

1. Select the domain that must be added to an application.
2. Click **Add to an existing application**.
3. In **Applications**, select the application to which you want to add these domains.
4. Click **Get app details**.
5. The **Related Domains** field displays all the domains that you selected earlier in separate rows.
6. Click **Finish**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Note:

- You can only add a TCP/UDP destination IP address to an existing TCP/UDP application. The **Applications** field lists only the TCP/UDP apps configured in the system.
- You can select an existing HTTP/HTTPS or TCP/UDP app to add domains (main or single entry) whose protocol is HTTP/HTTPS.
- You cannot select a domain that is already associated with an application.

Policy modeling tool

October 13, 2024

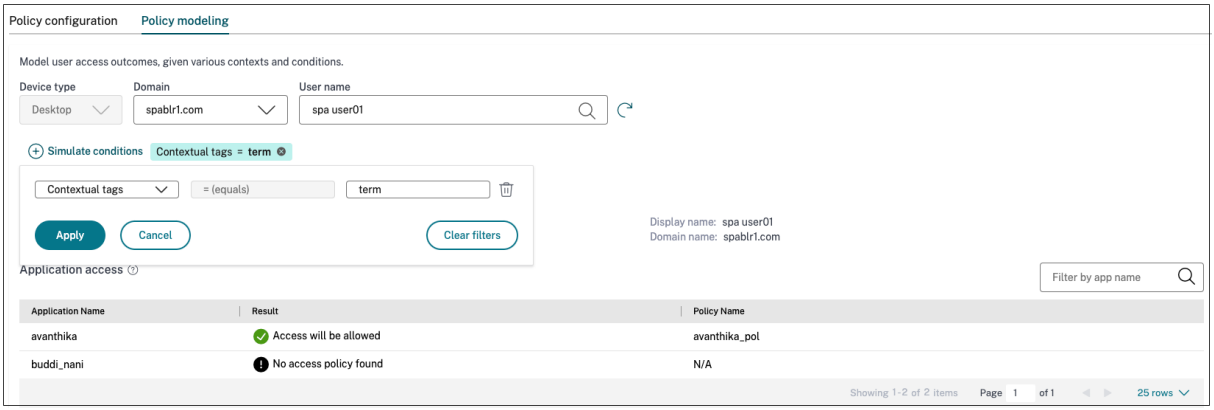
Admins can create multiple policies and assign these policies to multiple applications. As a result, it might become difficult for admins to understand the application access results for their end-users. That is, if the end-user is allowed or denied access based on the application and access policy configurations. The policy modeling tool (**Access policies > Policy modeling**) helps resolve these issues by giving the administrators full visibility into the expected application access result (allowed/allowed with restriction/denied). Admins can check the access results for specific users and add a user condition for contextual tags. The tool also displays the list of policies associated with the applications.

To analyze the access policy configuration, perform the following steps.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. In the Secure Private Access console, click **Access Policies** and then click the **Policy modeling** tab.
2. Add the following details:
    - **Device type**: Desktop is selected by default.
    - **Domain**: Select the domain associated with the user.
    - **User**: Select the user name for which you want to analyze the applications and associated policies.
3. You can also simulate a condition based on contextual tags on the end user and their devices.
    a) Click **Simulate conditions**. The condition **Contextual tags** is selected by default.
    b) Enter the contextual tag in **Value**.
    c) Click the **+** sign to add other conditions.
4. Click **Apply**.

The applications and associated policies for the selected user are displayed in a tabular format.



Unsanctioned websites

October 13, 2024

Applications (intranet or internet) that are not configured within Secure Private Access are regarded as “Unsanctioned Websites”. By default, Secure Private Access denies access to all intranet web applications if there are no applications and access policies configured for those applications.

For all other internet URLs or SaaS applications that do not have an app configured, admins can use the **Settings > Unsanctioned Websites** tab from the admin console to allow or deny access via Citrix Enterprise Browser.

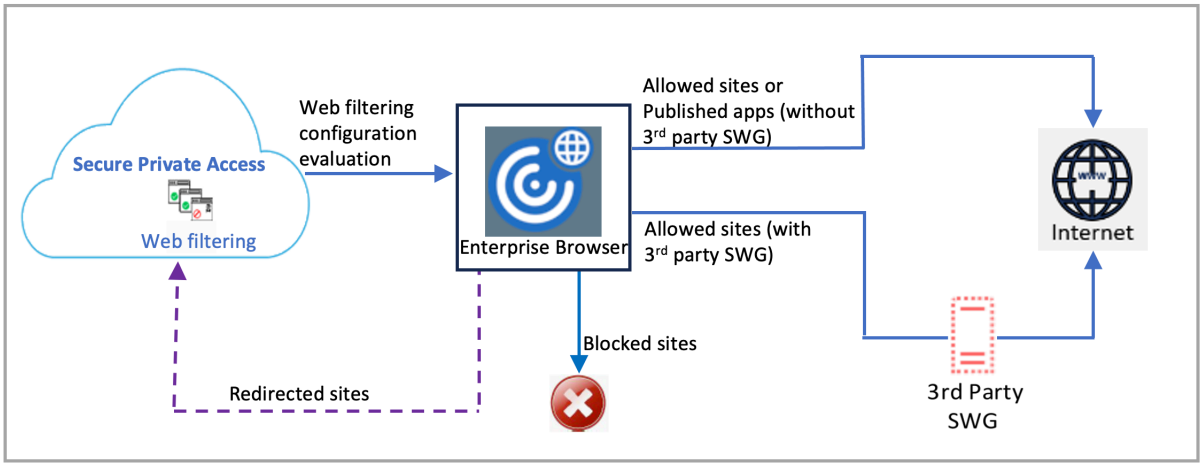
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> By default, settings are configured to ALLOW access to all internet URLs or SaaS apps via Citrix Enterprise Browser.

How unsanctioned websites work

1. URL analysis check is done to determine if the URL is a Citrix service URL.
2. The URL is then checked to determine if it is an Enterprise web or SaaS app URL.
3. The URL is then checked to determine if it is identified as a blocked URL or if the URL can be allowed to be accessed.

The following illustration explains the end user traffic flow.



When a request arrives, the following checks are performed, and corresponding actions are taken:

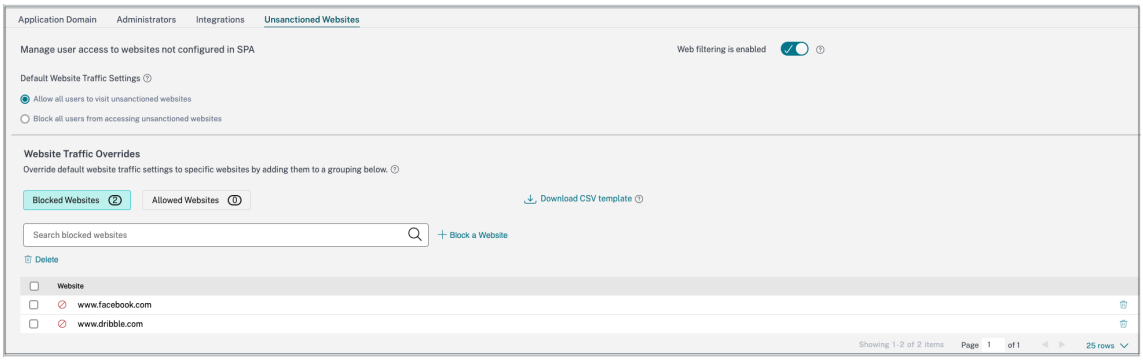
1. Does the request match the global allow list?
    a) If it matches, the user can access the requested website.
    b) If it does not match, website lists are checked.
2. Does the request match the configured website list?
    a) If it matches, the following sequence determines the action.
        i. Block
        ii. Allow
    b) If it does not match, the default action (ALLOW) is applied. The default action cannot be changed.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure rules for unsanctioned websites

1. In the Secure Private Access admin console, click **Settings > Unsanctioned Websites**.

   > **Note:**
   >
   > - The web filtering feature is enabled by default and access to all unsanctioned internet URLs is allowed.
   > - You can change the setting to **Block all users from accessing unsanctioned websites** to block access to any internet URL via Citrix Enterprise Browser for all users.



   You can also change settings for specific URLs by adding them to blocked websites or allowed websites.

   For example, if you have blocked access to all unsanctioned URLs by default and you want to allow access to only a few specific internet URLs, then you can do so by performing the following steps:

   a) Click the **Allowed Websites** tab, and then click **Allow a Website**.

   b) Add the website address that must be allowed access. You can either manually add the website address or drag and drop a CSV file containing the website address.

   c) Click **Add a URL** and then click **Save**.

      The URL is added to the list of allowed websites.

Upgrade

October 22, 2024

Periodically, Citrix releases updates to enhance the performance, security, and reliability of the Cloud Connector. By default, Citrix Cloud installs these updates on each connector, one at a time, when

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

they become available. Secure Private Access is upgraded as part of the Cloud Connector upgrade by default.

For details on Cloud Connector upgrade, see, Connector updates.

Refer to the following topics for details about the other components upgrade:

- StoreFront
- NetScaler Gateway

Manage configurations

October 13, 2024

After you have installed Secure Private Access, you can modify the settings from the **Settings** page. You can manage routing of application domains and modify the integration settings.

To modify the settings, you must sign into the Secure Private Access admin console with a Secure Private Access administrator account.

For details on how to update or modify the settings, see the following topics:

- Manage routing of application domains
- Modify integration settings

Manage settings after installation

October 13, 2024

Manage routing of application domains

You can view a list of application domains added in your Secure Private Access setup. The application domains table lists all the related domains and how the app traffic is routed (externally or internally).

1. Click **Settings > Application Domain**.
2. You can click the edit icon and change the routing type, if necessary.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Manage administrators

You can view the list of administrators and also add administrators from the **Settings > Administrators** page. The administrator who installs the Secure Private Access the first time is granted full permission. This admin can then add other administrators to the setup.

You can also add admin groups so that access is enabled for all the admins in that group.

1. In the **Administrators** page, click **Add**.
2. In **Domain**, select the domain to which this administrator must be added.
3. In **Users or user group**, select the user or a group to which this user belongs.
4. In **Admin Type**, select the permission type that must be assigned to this user.

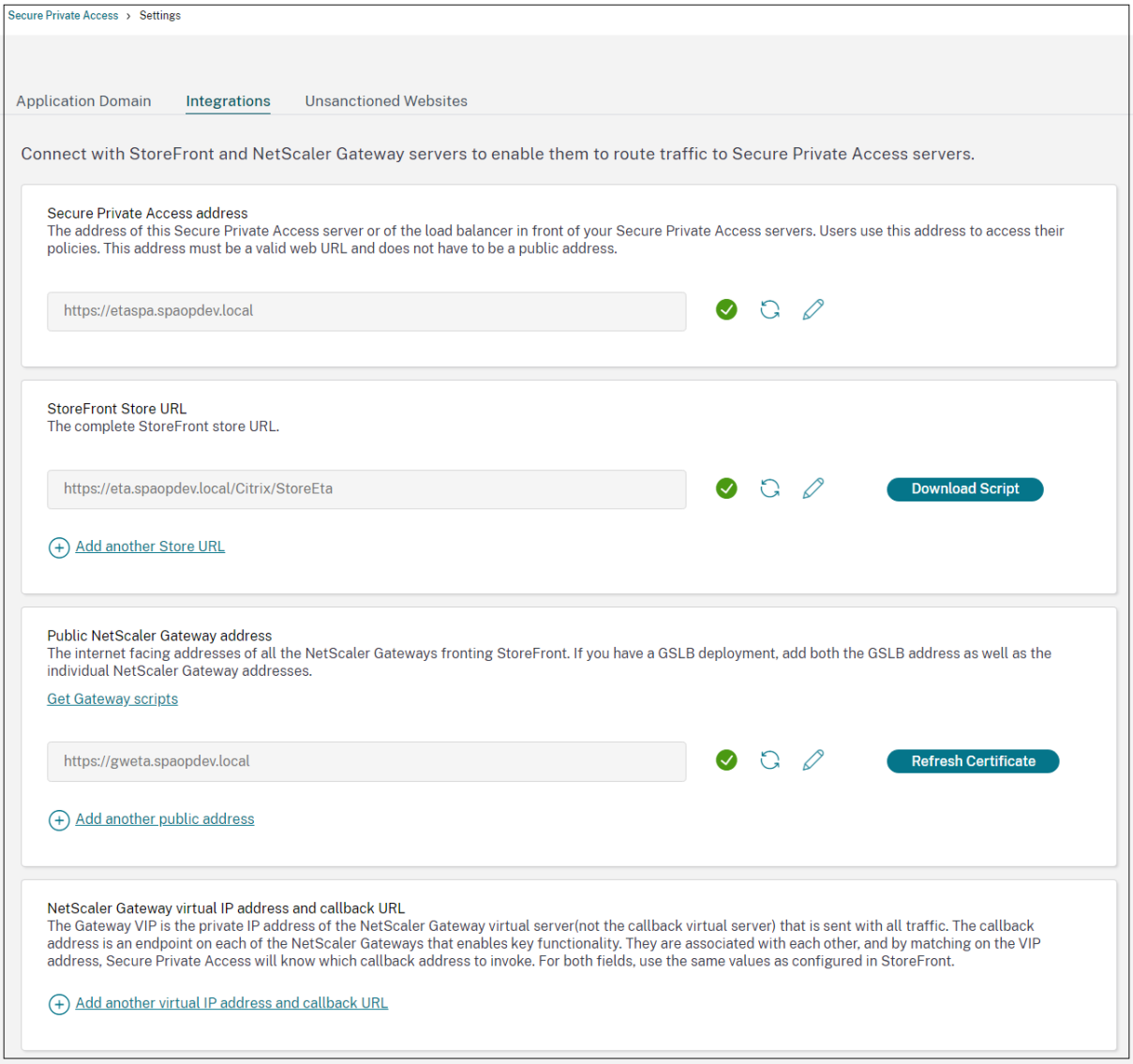
Modify integration settings

After you have set up Secure Private Access, you can modify or update the StoreFront and NetScaler Gateway entries from the **Integrations** tab.

1. Click **Settings > Integrations**.
2. Click the edit icon in line with the setting that you want to modify and update the entry.
3. Click the refresh icon to ensure that the settings are valid.

> **Note:**
>
> - If the Secure Private Access address is changed, then download the StoreFront script and run it on the StoreFront host.
> - If Secure Private Access is installed on a machine different that StoreFront, then download the StoreFront script and run it on the StoreFront.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Manage applications and policies

October 13, 2024

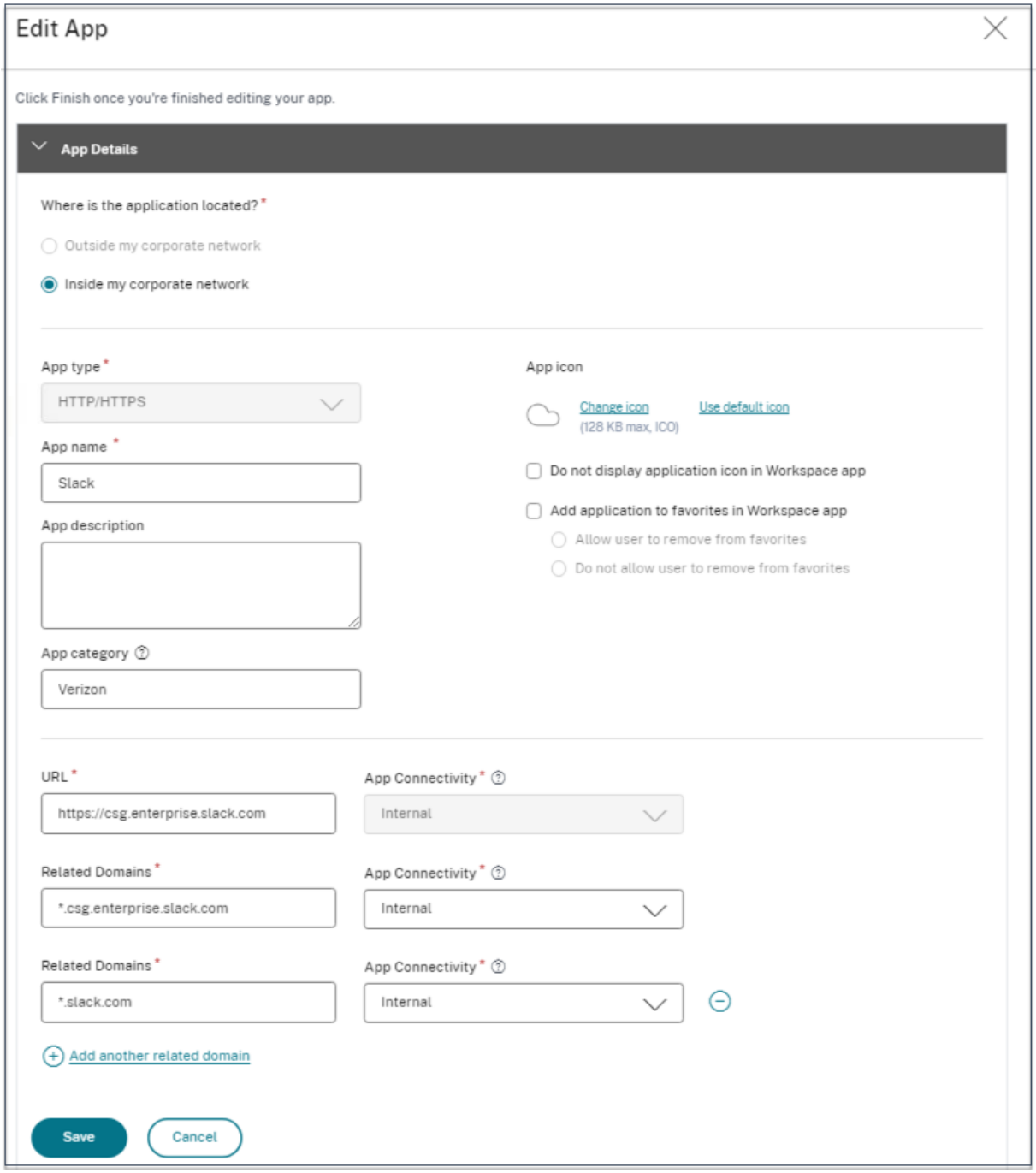
After configuring the applications and access policies, you can edit them if necessary.

Edit an application

1. In the Secure Private Access admin console, click **Applciations**.
2. Click the ellipsis button in line with the application that you want to modify and then click **Edit Application**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Edit the app details.
4. Click **Save**.



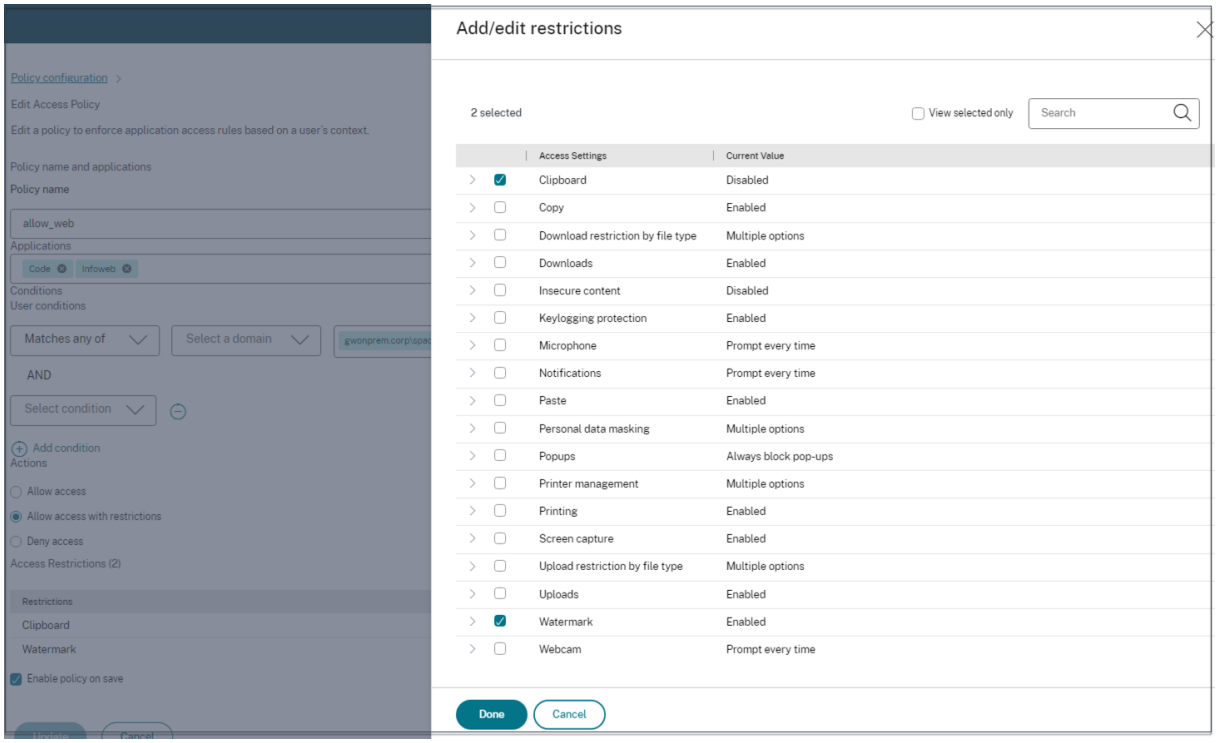
Edit an access policy

1. In the Secure Private Access admin console, click **Access Policies**.
2. Click the ellipsis button in line with the policy that you want to modify and then click **Edit access**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

policy.

3. Edit the policy details.
4. Click **Update**.



Integration with DaaS monitor

October 28, 2024

Secure Private Access is integrated with Monitor, the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can monitor and troubleshoot Web/SaaS and TCP/UDP app sessions and events from the DaaS Monitor, in addition to the Secure Private Access dashboard.

Service entitlements

To use the DaaS Monitor feature with Secure Private Access, you must have both Secure Private Access and DaaS entitlements.

Supported clients

- Citrix Workspace app - 2409 and later

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Secure Access for Windows - 24.8.1.19 and later
- Citrix Secure Access for macOS - 24.10.1 and later

How to access Monitor

You can access Monitor from the Secure Private Access dashboard (**Go to Monitor**) or from the Citrix DaaS service tile.

In the **Monitor** page, search for the user to view the sessions.

Session definitions

For the DaaS Monitor context, the app session start and end are defined as follows:

Web/SaaS app sessions

The session start and end for Web/SaaS apps is defined as follows:

- Start: Citrix Enterprise Browser is opened in the Citrix Workspace app and applications are accessed.
- End: A session ends in the following scenarios.
  - You close the Citrix Enterprise Browser.
  - After 30 minutes of inactivity, if no session activity is reported.

    The Citrix Enterprise Browser client sends a session activity to Monitor every 15 minutes to Monitor. If this session activity is not received for 30 minutes, which might occur due to reasons such as:

    * Network failure.
    * Internet connectivity issues.
    * Session is automatically closed after the 30-minute interval without session activity.

> **Note:**
>
> For apps launched through native browsers (agentless), the session ends after 120 minutes of inactivity.

TCP/UDP app sessions

The session start and end for TCP/UDP apps is defined as follows:

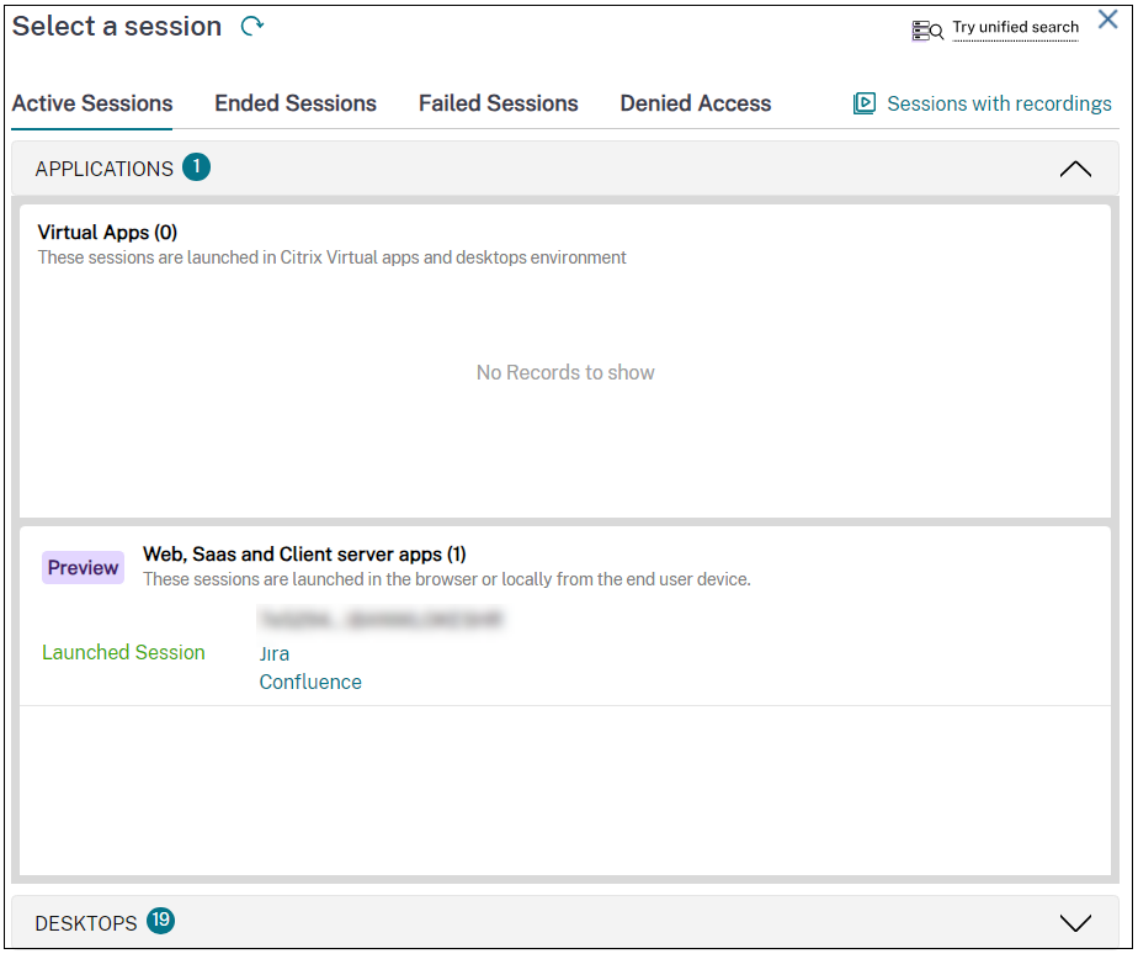
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Start: You log in to the Citrix Secure Access client and access the apps.
- End: A session ends in the following scenarios.
  - You log out of the Citrix Secure Access client.
  - After 30 minutes of inactivity, if no session activity is reported.

View user sessions

Perform the following steps to view a user session:

1. Search for a user to view the sessions.
   - The **Select a session** page displays all active sessions. If you do not find your session in the **Active Sessions** tab, check in the **Denied Access** tab.
   - The **Ended Sessions** and **Failed Sessions** tabs are not applicable to Secure Private Access.



2. In the **Active Sessions** tab, click the session ID to view the details of the session.

   The **Activity Manager** page appears.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

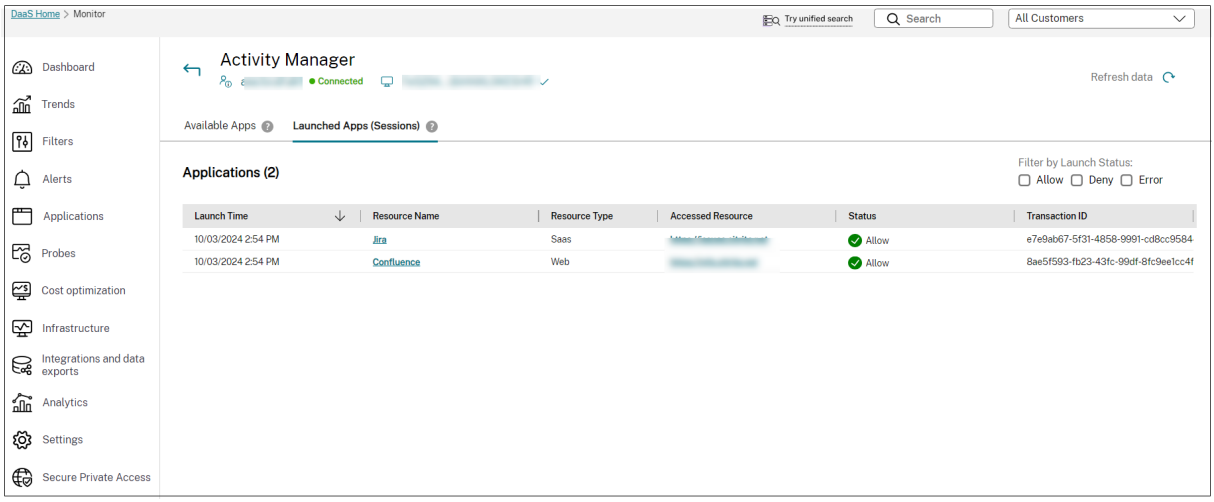
3. Click one of the following tabs:

   - **Launched apps:** View all applications launched by the user and the results (allow or deny) of the access policy evaluation.

     If an application was accessed multiple times in the same session, only the latest launch details are captured.

   - **Available Apps:** View app enumeration details of all the applications that were launched by this user.

     - If multiple enumeration requests were sent by Citrix Workspace app for a user, only the latest enumeration details are captured.
     - For TCP/UDP apps (web and ZTNA), although there is no concept of app enumeration, all apps configured and associated with the user are listed in the **Available Apps** list.
     - The **Available Apps** list does not contain external apps that are enumerated through the Citrix Secure Access client as they are not tunneled by Secure Private Access.
     - For the Citrix Secure Access agent, the **Available Apps** list only displays only the internal web and TCP/UDP apps.



Application topology

When you click an app from the **Launched Apps** or **Available Apps** tabs, the application topology page appears, displaying complete information about the app.

- **Session Topology:** Displays the app launch flow.
- **About:** Displays app-related information such as app type, number of policy rules, security restrictions, and accessed resources. The data that appears in the **Accessed Resources** section varies depending on the app type.

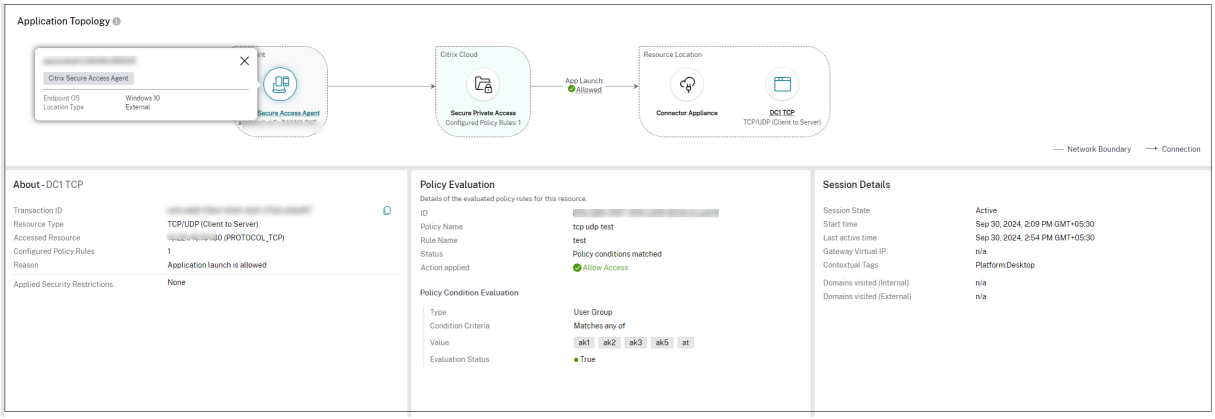
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Web apps - URL or the app FQDN
  - TCP/UDP –IP address/FQDN, port, and protocol
  - Web app (launched via Citrix Secure Access client) - FQDN, port, and protocol
  - Web app (launched via Citrix Workspace) - URL

- **Policy evaluation:** Displays information related to the access policy, such as rules, actions, and conditions.
- **Session Details:** Displays information related to the session, including session start and end time, session state, and contextual tags associated with the policy.

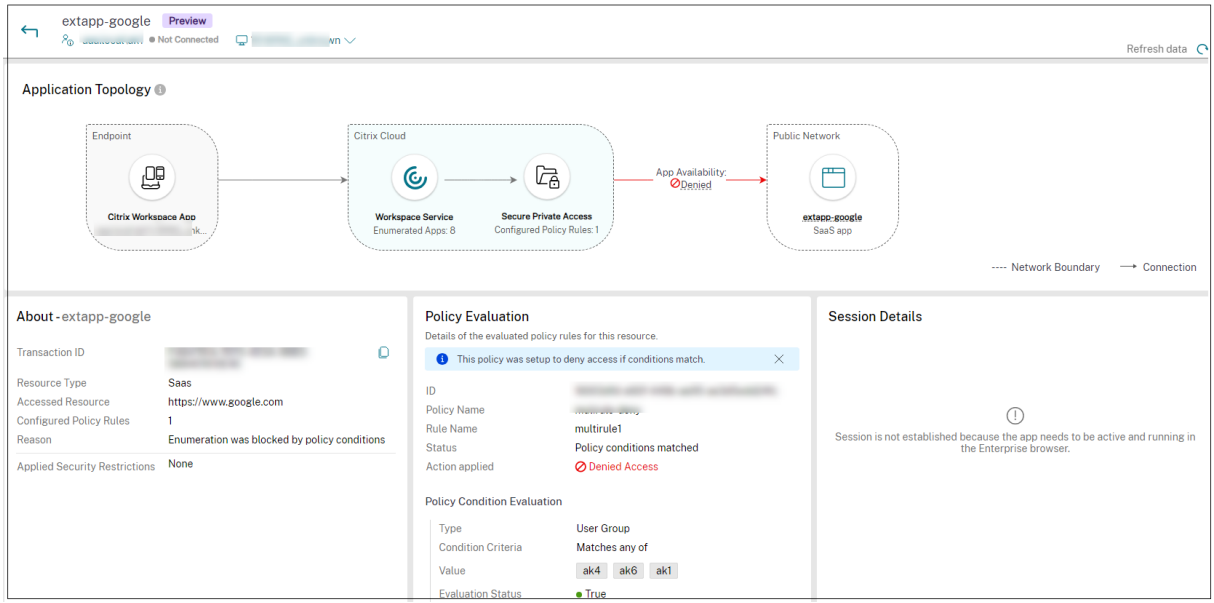
  - The **Domains Visited** field is applicable only for the Web/SaaS apps and is updated only after 15 minutes, as the Citrix Enterprise Browser clients on macOS and Windows send session activity every 15 minutes.
  - The **Session Details** column section remains empty for apps clicked from the **Available Apps** tab, as app enumeration is not associated with a session.

The following figure displays a sample topology diagram for a successfully launched app.



The following figure displays a sample topology diagram for an access denied app.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Basic troubleshooting

October 20, 2024

This topic list some of the errors that you might come across while or after setting up Secure Private Access.

Certificate errors

StoreFront failures

Public gateway/callback gateway failures

Secure Private Access Server not reachable

Certificate errors

Error message: Unable to get the certificates automatically from one or more gateway servers.

This error message appears when you try to add a public NetScaler Gateway address and there is an issue fetching the certificate. This issue can occur when setting up Secure Private Access or updating settings after the setup is complete.

Workaround: Update the gateway certificate the same way in which you would for Citrix Virtual Apps and Desktops.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

StoreFront failures

- **Error message**: Failed to create StoreFront entry for: <Store URL>

  Update the StoreFront entries from the **Settings** tab if it is not visible. After you have set up Secure Private Access using the wizard, you can edit StoreFront entries from the **Settings** tab. Note down the StoreFront Store URL for which this error occurred.

  Resolution:

  1. Click **Settings** and then click the **Integrations** tab.
  2. In **StoreFront Store URL**, add the StoreFront entry if it is not visible.

- **Error message**: Failed to configure StoreFront entry for: <Store URL>

  Resolution:

  1. There might be a PowerShell execution policy restriction in place. Run the PowerShell script command `Get-ExecutionPolicy` for details.
  2. If it is restricted, you must bypass this and run a StoreFront configuration script manually.
  3. Click **Settings** and then click the **Integrations** tab.
  4. In **StoreFront Store URL**, identify the StoreFront URL entry for which the error occurred.
  5. Click the **Download Script** button next to this Store URL and run this PowerShell script with admin privileges on the machine on which the corresponding StoreFront installation is present. This script must be run on all the StoreFront machines.

  > **Note:**
  >
  > If you are retrying the installation after uninstalling, ensure that you don't have an entry with the name "Secure Private Access"in the StoreFront configuration (**StoreFront > store> Delivery Controller -> Secure Private Access**). If Secure Private Access is present, delete this entry. Manually download and run the script from the Settings > Integrations page.

- **Error message**: StoreFront configuration is not local for: <Store URL>

  After you have set up Secure Private Access using the wizard, you can edit gateway entries from the Settings tab. Note down the StoreFront Store URL for which this error occurred.

  Resolution:

  This issue occurs if StoreFront is not installed on the same machine as Secure Private Access. You must manually run the StoreFront configuration on the machine where you have installed StoreFront.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Click **Settings** and then click the **Integrations** tab.
2. In **StoreFront Store URL**, identify the StoreFront URL entry for which the error occurred.
3. Click the Download Script button next to this Store URL and run this PowerShell script with admin privileges on the machine on which the corresponding StoreFront installation is present. This script must be run on all the StoreFront machines.

> **Note:**
>
> To run the StoreFront PowerShell script, open the Windows x64 compatible PowerShell window with admin privileges and then run ConfigureStorefront.ps1. StoreFront script is not compatible with Windows PowerShell (x86).

- **Error message**: "Get-STFStoreService : Exception of type 'Citrix.DeliveryServices.Framework.Feature.Except was thrown."while running StoreFront script using PowerShell.

  This error occurs when the StoreFront script is run on a x86-compatible PowerShell window.

  Resolution:

  To run the StoreFront PowerShell script, open the Windows x64 compatible PowerShell window with admin privileges and then run `ConfigureStorefront.ps1`.

Public gateway/callback gateway failures

Error message: Failed to create Gateway entry for: <`Gateway URL`> OR Failed to create Callback Gateway entry for: <`Callback Gateway URL`>

Resolution:

Note the Public Gateway or Callback Gateway URL for which the failure occurred. After you have set up Secure Private Access using the wizard, you can edit gateway entries from the **Settings** tab.

1. Click **Settings** and then click the **Integrations** tab.
2. Update the public gateway address or the callback gateway address and the virtual IP address for which the failure occurred.

Secure Private Access Server not reachable

Error message: Failed to update IIS pool. Failed to restart IIS pool

Resolution:

Go to Application pools in Internet Information Services (IIS) and check that the following application pools have started and are running:

- Secure Private Access Runtime Pool

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Secure Private Access Admin Pool

Also check that the default IIS site `"Default Web Site"` is up and running.

Application enumeration failure

Application enumeration breaks if the StoreFront URL or the NetScaler Gateway URL contains a trailing slash (/).

Resolution:

Delete the trailing slash in the StoreFront store URL or the NetScaler Gateway URL. For details, see Update StoreFront or the NetScaler Gateway server details after the setup.

Create Secure Private Access diagnostics support bundle

Perform the following steps to create a Secure Private Access diagnostics support bundle:

- Open the PowerShell or the command prompt window with admin privileges.
- Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool").
- Run the following command:

  `.\AdminConfigTool.exe /SUPPORTBUNDLE <output folder>`

Change log level for troubleshooting logs

Troubleshooting logs are the default error log level.

To change the log level for the troubleshooting logs, in the runtime service appsettings.json (C:\Program Files\Citrix\Citrix Access Security\Runtime\RuntimeService) update `restrictedToMinimumLeve` for `TroubleshootingSql` to one of the following values:

```
-  Information
-  Debug
-  Warning
-  Error

"TroubleshootingSql": {

  "restrictedToMinimumLevel": "Error",
  "batchPostingLimit": 50,
  "batchPeriod": "00:00:05" // 5 seconds
 }
```

© 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).