## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What’s new</td>
<td>3</td>
</tr>
<tr>
<td>Known issues</td>
<td>10</td>
</tr>
<tr>
<td>Entitlements</td>
<td>10</td>
</tr>
<tr>
<td>Data Governance</td>
<td>15</td>
</tr>
<tr>
<td>Citrix App Delivery and Security service support matrix</td>
<td>18</td>
</tr>
<tr>
<td>Configure role-based access control</td>
<td>20</td>
</tr>
<tr>
<td>Get started with Citrix App Delivery and Security service – Citrix Managed</td>
<td>26</td>
</tr>
<tr>
<td>Overview of Citrix App Delivery and Security service – Citrix Managed</td>
<td>30</td>
</tr>
<tr>
<td>Create cloud access profiles</td>
<td>34</td>
</tr>
<tr>
<td>Manage an environment</td>
<td>35</td>
</tr>
<tr>
<td>Deliver a modern application</td>
<td>45</td>
</tr>
<tr>
<td>Create services</td>
<td>52</td>
</tr>
<tr>
<td>Create service profiles</td>
<td>55</td>
</tr>
<tr>
<td>Add endpoints</td>
<td>66</td>
</tr>
<tr>
<td>Configure authentication for the endpoints</td>
<td>74</td>
</tr>
<tr>
<td>Content Transform</td>
<td>76</td>
</tr>
<tr>
<td>Add security protection</td>
<td>93</td>
</tr>
<tr>
<td>Deliver a classic application</td>
<td>142</td>
</tr>
<tr>
<td>Create a classic application</td>
<td>148</td>
</tr>
<tr>
<td>Migrate the Citrix ADC configuration to the CADS service</td>
<td>158</td>
</tr>
<tr>
<td>Deliver a multi-site application</td>
<td>168</td>
</tr>
<tr>
<td>Activate radar for a private data center</td>
<td>189</td>
</tr>
<tr>
<td>Application analytics</td>
<td>195</td>
</tr>
</tbody>
</table>
Application analytics 196
Application details 199
Set thresholds for app score 202
Application usage and lean period analytics (Key metrics) 204
Application usage analytics (Web Insight) 206
Security 214
Integration with Splunk 222
Web Insight dashboard 227
Multi-site application analytics 231
Manage SSL certificates 234
Monitor self-healing 237
API definitions in the Citrix App Delivery and Security service 242
View audit log 244
How-to articles 248
Get an A+ security rating for your application in the Qualys SSL lab test 248
Rewrite HTTP headers for rewrite content transform 258
What’s new

July 26, 2022

Audit logging support when migrating an application from Citrix ADC to the CADS service

The CADS service supports migrating any existing audit related configurations when you migrate an application from Citrix ADC to the CADS service.

For more information, see Supported Citrix ADC features.

View and track the DNS query consumption details

You can now view and track your DNS query consumption details in the Citrix App Delivery and Security service GUI. Navigate to the Usage dashboard to view the validity, capacity, and consumption details of the DNS queries for your Entitlements. For more information, see View Usage Dashboard.

Support for OR condition in Allow and Block list

You can now use OR condition while adding multiple conditions for a rule in Allow and Block list. A combination of AND condition and OR condition is not supported. Previously, only AND condition was supported.

For more information, see Allow and Block list.

July 13, 2022

Support for search bar in multisite analytics

In Multisite analytics, you can now use the search bar to filter applications based on the application names.

Self-healing capability for standalone IP-type EC2 instances

The CADS service now supports Self-healing capability for standalone IP-type EC2 instances in AWS. You can either detect or auto replace a slow server when the server is hosted as an EC2 instance with an IP address.

For more information, see Self-heal slow application server.
**June 30, 2022**

**Stickiness IPv4 Mask**

You can now define an IPv4 subnet mask to identify the client requests coming to the multi-site application and send the requests to the same site.

For more information, see [Deliver a multi-site application](#).

**Improvements to Web Insight**

The *self-heal slow application server* capability in the CADS service detects a faulty server and takes remedial action. If you enable the *Detect slow server* and *Auto-replace slow server* options, and if the service identifies a faulty server, the service replaces the faulty server with a healthy server.

You can now view analytics in *Web Insight* whenever a faulty server is replaced.

In *Analytics*, click an application, and from *Web Insight*, click the *Server Processing Time* tab to get visibility on when a faulty server is replaced.

**Integration with Splunk**

You can now integrate CADS service with Splunk to view analytics for WAF and Bot violations in your Splunk dashboard. Splunk add-on enables you to:

- Combine all other external data sources
- Provide greater visibility of analytics in a centralized place

CADS service collects Bot and WAF events and sends to Splunk periodically. The Splunk Common Information Model (CIM) add-on converts the events to CIM compatible data. As an administrator, using the CIM compatible data, you can view the WAF and Bot violations in the Splunk dashboard.

For more information, see [Integration with Splunk](#).

**SQL injection and cross-site scripting enhancements**

You can now block a client that sends 20 or more security check violation requests within a 30 minutes duration.

The *Block clients with 20 violations within 30 minutes* check box is introduced under the SQL Injection and Cross-site scripting pages. For more information, see [SQL injection and Cross-site scripting](#).

The CADS service logs malicious clients and you can view the details in the *Network Function* column of the *Action History* page. For more information, see [Action History](#).
June 16, 2022

Search box on Multi-Site Applications Dashboard

A search box is introduced on the Multi-site Applications dashboard that helps you search for a multi-site application within the list of multi-site applications.

For more information, see Multi-site application summary.

Cloud region recommendation for existing multi-site applications

The CADS service now supports getting site recommendations for existing multi-site applications. Enter user location, traffic expected from each user location, and the cloud service provider for an application and get its corresponding recommendations. You can choose to exclude the existing sites from the recommendation calculations.

For more information, see Cloud region recommendation engine.

Service Profiles

You can now define the core settings of a service, such as load balancing, back-end SSL, and health check configuration under a service profile. While creating a service, you can associate this service profile with the service and inherit the preferred configurations.

In the CADS service GUI application creation workflow, service profile settings are available while creating services under the Service Profiles tab.

For more information, see Create service profiles.

June 03, 2022

Domain name uniqueness check for a user-defined (Route 53) multi-site application

The CADS service checks the uniqueness of the domain name for a user-defined (Route 53) multi-site application on the Application Details page where you enter the domain name. If the entered domain name exists in the hosted DNS zone, an error message is displayed on the same screen. Previously, the uniqueness check was done during deployment which is at the end of the multi-site application creation workflow.

With this enhancement, if necessary, you are notified to change the domain name early in the workflow rather than at the end.
Handling unsupported commands while migrating a configuration

Commands that are not applicable, not supported, or contain missing entities are clearly listed when a Citrix ADC configuration is migrated to the Citrix App Delivery and Security service.

The CADS service also displays a suggested configuration after fixing the issues. You can choose to accept the suggested configuration or edit the commands manually.

New rules for content routes

The following rules are added while creating a content route for an endpoint:

Client TCP Address MSS - Identifies and returns the maximum segment size (MSS) in a TCP/IP packet.
Client TCP Address Source Port - Identifies and returns the source port in a TCP/IP packet.

View Audit Log messages

You can now track the configuration activities in the CADS service from the Audit Log dashboard. In the left navigation pane, navigate to Audit Log.

Using the audit log dashboard, you can:

- Track all events and activities for the Citrix environments.
- Manage and monitor the applications.
- Use the filters to search the audit log messages that enable you to narrow down and find the information in real-time.

For more information, see View audit log.

Data leak prevention

The CADS service now supports the data leak prevention feature that avoids the leak of sensitive information, such as credit card numbers and social security numbers, to unauthorized recipients.

If your application has access to database servers that store user-specific sensitive information, the CADS service identifies if the responses coming from the database server contain any user-specific sensitive information. It also allows you to define one of the following actions to perform to avoid leakage of such information when a match is found:

- Block: Based on the maximum match length configured, the CADS service blocks those many strings in the responses. For example, if the maximum length configured is 5 for credit cards, the CADS service blocks the last 5 strings of the credit card.
- Mask: The CADS service masks the safe object details with an X in the responses before processing it further. For example, if the maximum length configured is 5 for credit cards, the CADS service masks the last 5 strings of the credit card with an X.
None: No action is taken on the response. The CADS service processes the responses as is without any changes.
For more information on data leak prevention, see Data leak prevention.

Field format protection

The CADS service now supports the field format protection feature. This feature helps in reducing the risk of attacks caused by sending inappropriate data in web forms.

With this feature, the CADS service examines both the type and length of web form data and ensures that it is appropriate for the targeted field. If inappropriate web form data is found in a user request, you can configure the CADS service to block the request.

Support for role based access control in CADS service

CADS service provides role-based access control (RBAC) using which you can grant access permissions based on the roles of individual users within your organization. Only Citrix identity provider is supported in the CADS service currently. During the initial onboarding process, an administrator with full rights is created. This administrator can then invite other administrators to use the CADS service. The following custom roles are available:

**AppAdministrator** - This role has permissions to create and deploy applications.

**AppOperator** - This role has read-only permissions. The user can monitor an application, but not create or deploy an application.

**InfraAdministrator** - This role has permissions to create an environment and cloud access profiles in addition to creating and deploying applications.

Specify subnets to be used by the CADS service to reach your origin application servers

Typically, you configure your application servers security group to allow ingress traffic from all the IP addresses in the VPC. This works well by default because during environment creation in the CADS service, it creates new subnets in the VPC for provisioning the infra to reach your origin application servers. However, to increase security, you can restrict the IP addresses that the CADS service uses to connect to your application servers. You can do so during environment creation by specifying the subnets you created exclusively for the CADS service. Doing so, avoids creating default subnets, and the service provisions the infra in the specified subnets. Also, ensure that you change your application servers security group to allow ingress traffic from the subnets you have specified.
**Auto-upgrade dashboard**

The CADS service now supports the automatic upgrade of the Citrix environments. Navigate to Applications > Environments > Settings to view the Auto-upgrade dashboard. The dashboard displays the available upgrade slots for your environments and the one currently selected. Environment upgrade ensures that you retain access to the latest features and fixes offered by the service. For more information, see Manage an environment.

**Support for client authentication**

The SSL endpoints now support certificate-based client authentication in the Citrix App Delivery and Security service.

**Support for API definitions**

The CADS service now supports API definitions. You can create an API definition by navigating to API Definitions > Add API. After the API definition is created, you can use it while configuring a new application, and also in application settings, such as, content routes for an end point, content transform, and security protection. The API resource paths are available as a filter condition.

**View and track the Standalone entitlement consumption details**

You can now view and track your standalone Advanced and Premium entitlement consumption details in the Citrix App Delivery and Security service GUI. Navigate to the Usage dashboard to view the validity, capacity, and consumption details of the Premium and Advanced Entitlements. For more information, see Entitlements.

**May 16, 2022**

**Replace request URL**

The CADS service now supports replacing the request URL with the specified URL.

For example, consider that the HTTP client request is GET /pub/WWW/TheProject.html HTTP/1.1. If there is a requirement to redirect the client request to a different resource, you can replace the URL by configuring the Replace request URL action. This modifies the client request URL before sending it to the server as GET /pub/WWW/NewProject.html HTTP/1.1.

For more information, see Add content transform.
Fixes


April 28, 2022

**Check health status of classic apps**

You can now check the health status of deployed classic apps. The health status displays the real-time health of your deployed apps for each application service in an availability zone. To view the health status of a deployed app, click the three dots in the **Actions** column of the Application dashboard and then click Health Status. For more information, see [Deliver a classic application](#).

**SAML based authentication support**

Admins can now add SAML authentication to the apps. Only authenticated users are allowed to access specific services configured by the admin. For more information, see [Configure authentication for the endpoints](#).

Fixes

**ADSS-10117**: You cannot increase the number of rows using pagination to see the environments after the tenth environment.

April 20, 2022

**DNS fallback endpoint**

The CADS service now supports adding a DNS fallback endpoint. The DNS fallback endpoint acts as a backup endpoint and responds to DNS queries when all sites associated with a multi-site application are in DOWN state.

April 13, 2022

**Changes in the Add Site page of a multi-site application**

The **IPv4 Address or DNS Name** and **IPv6 Address or DNS Name** fields in the multi-site application **Add Site** page are now combined in the **DNS Name, IPv4, or IPv6** field.
Known issues

August 19, 2022

The Citrix App Delivery and Security Service – Citrix Managed has the following known issues:

You cannot edit the names of the multi-site application and the site in which the application is deployed.

Entitlements

August 18, 2022

The Citrix App Delivery and Security service license is based on flexible consumption-based metering, where your applications automatically consume capacity from available entitlements. This consumption-based method is a software as a service (SaaS) model, where you consume a service based on the entitlement that you've purchased. This flexibility helps you to reduce capacity wastage and avoid license-related performance limits. To use Citrix App Delivery and Security, you need a valid entitlement.

Entitlement types

You can use one of the following entitlements for Citrix App Delivery and Security.

- Standalone entitlements
- Trial entitlements

Standalone entitlements

The Citrix App Delivery and Security service standalone entitlements come in two editions: Advanced and Premium. Entitlements are yearly subscription, which means every entitlement has only one-year validity. The two editions have the following entitlement types:

Table 1. Entitlement types

<table>
<thead>
<tr>
<th>Edition type</th>
<th>Entitled to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced</td>
<td>300 TB bandwidth + 25 million DNS queries</td>
</tr>
<tr>
<td>Advanced</td>
<td>1200 TB bandwidth + 100 million DNS queries</td>
</tr>
</tbody>
</table>
Citrix App Delivery and Security service

<table>
<thead>
<tr>
<th>Edition type</th>
<th>Entitled to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced</td>
<td>4800 TB bandwidth + 480 million DNS queries</td>
</tr>
<tr>
<td>Advanced</td>
<td>20000 TB bandwidth + 2 billion DNS queries</td>
</tr>
<tr>
<td>Premium</td>
<td>300 TB bandwidth + 25 million DNS queries</td>
</tr>
<tr>
<td>Premium</td>
<td>1200 TB bandwidth + 100 million DNS queries.</td>
</tr>
<tr>
<td>Premium</td>
<td>4800 TB bandwidth + 480 million DNS queries</td>
</tr>
<tr>
<td>Premium</td>
<td>20000 TB bandwidth + 2 billion DNS queries</td>
</tr>
</tbody>
</table>

Citrix App Delivery and Security service uses the Citrix Intelligent Traffic Management (ITM) to monitor traffic. The Usage dashboard in the Citrix App Delivery and Security service GUI measures the number of DNS queries sent for an application.

Customers also have an option to buy a DNS pack for yearly subscription.

**Table 2. Subscription types**

<table>
<thead>
<tr>
<th>Subscription type</th>
<th>Entitled to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yearly</td>
<td>1 billion DNS queries</td>
</tr>
</tbody>
</table>

The following table shows the features that the two entitlement editions support.

**Table 3. Supported features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Citrix App Delivery and Security service Advanced</th>
<th>Citrix App Delivery and Security service premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL/Load balancing/content switching</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Content rules</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GSLB</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Caching and compression</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Analytics</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Lifecycle management</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Citrix App Delivery and Security service

<table>
<thead>
<tr>
<th>Feature</th>
<th>Citrix App Delivery and Security service Advanced</th>
<th>Citrix App Delivery and Security service premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITM based GSLB</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security (WAF, BOT management)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>ICA Proxy</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Gateway SSL VPN</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

You can buy multiple units of the entitlements listed in **Table 1. Entitlement types**, in any combination of editions or any combination of tiers with different or same start date and end date.

For example, you can buy:

1. Two units of 1200 TB pack of the same edition or different edition.
2. One unit of 300 TH pack of premium and One unit of 4800 TB advanced.

To know more about how to buy a Citrix App Delivery and Security entitlement, see [https://www.citrix.com/en-in/buy/licensing/product.html](https://www.citrix.com/en-in/buy/licensing/product.html)

When you create an application, select one of the available editions from the drop-down menu. Select the edition based on the feature that you want to see. To create an application, from the GUI navigate to **Applications > New Application**. Refer to **Table 3. Supported features** for features supported on each edition.

**Trial entitlement**

You can explore the Citrix App Delivery and Security service without buying an entitlement. The trial entitlement is valid for 60 days and comes with the following capacity:

Premium: 1 TB + 1 million DNS queries

To use the trial entitlement, create a Citrix Cloud account and log on to Citrix Cloud.

After the trial entitlement has expired or a trial quota (data processed in TB) is exhausted, the Citrix App Delivery and Security service stops processing the traffic. After 30 days from the trial expiry, all the resources created in the Citrix App Delivery and Security service get deleted. During these 30 days, you can opt to buy an entitlement and move your apps from trial to paid entitlements.

**View Usage dashboard**

You can view and track the Standalone entitlement consumption details (Advanced, Premium and DNS Queries) in the **Usage** dashboard.
Citrix App Delivery and Security service

Citrix App Delivery and Security service applies metering parameters to incoming and outgoing application traffic at the ADC instances provisioned by the service. Based on these meters, the Citrix App Delivery and Security service generates the dashboard report.

Navigate to the **Usage** dashboard to view the validity, capacity and the consumption details of all the Entitlements purchased.

- **Premium entitlements**

  Navigate to **Usage > Premium** to see the details of all the Premium entitlements.

  You can see a tabular view and a donut view of the validity, capacity and the consumption details of all the existing and expired Premium entitlements. You can also view the details of the purchase and expiry dates in a tabular view for all the existing and expired entitlements.

  Additionally, you can view the details of the entitlements that are in the Grace period.

  ![Premium Entitlement Example](image)

  You can also view the validity, capacity and the consumption details of the Trial Entitlements. Based on the available details you can make an informed decision to buy and move from trial to paid entitlements.

- **Advanced entitlements**

  Navigate to **Usage > Advanced** to see details of all the Advanced entitlement details.

  You can see a tabular view and a donut view of the validity, capacity and the consumption details of all the existing and expired Premium entitlements. You can also view the details of the purchase and expiry dates in a tabular view for all the existing and expired entitlements.

  Additionally, you can view the details of the entitlements that are in the Grace period.
DNS Queries

Navigate to **Usage > DNS Queries** to see DNS query details for the entitlements. You can see a tabular view and a donut view of the validity, capacity and the consumption details of all the existing and expired DNS Queries. You can also view the details of the purchase and expiry dates in a tabular view for all the existing and expired DNS Queries.
Citrix App Delivery and Security service behavior on reaching expiry or reaching end of quota

This section describes Citrix App Delivery and Security service behavior on reaching expiry or reaching the end of quota, in different scenarios.

**Scenario 1:** You have only one entitlement, and it has expired.

**Behavior:** After expiry, the grace period for 30 days starts. During this period, you get the edition of the expired entitlement; for example, 10 TB of data processing + 1 million DNS queries.

After the end of the grace period, the Citrix App Delivery and Security service stops processing the application traffic.

After 90 days from the end of the grace period, your account and data plane components will be deleted.

**Scenario 2:** You have multiple entitlements of the same edition with a different expiry date, and one of them expires:

**Behavior:** Citrix App Delivery and Security service continues with the active entitlement.

**Scenario 3:** You’ve multiple entitlements of different editions with different expiry dates, and one of them expires.

**Behavior:** Grace period starts for the expired entitlement.

**Scenario 4:** You’ve multiple entitlements, and the quota of one of the entitlements is consumed before the expiry date.

**Behavior:** Citrix App Delivery and Security service continues with the active entitlement.

**Scenario 5:** You have purchased annual entitlements for a multiyear.

**Behavior:** Customer-entitled quota is given yearly.

Example: If you have purchased Advanced: 300 TB + 25 million DNS queries entitlement for 2 years, then-

- In the first year, your quota is 300 TB + 25 million DNS queries
- In the second year, any remaining quota of the first year expires and you get a fresh quota of 300 TB + 25 million DNS queries, due for the second year.

**Data Governance**

March 30, 2022
Citrix App Delivery and Security (CADS) service is a part of Citrix Cloud services, and it uses Citrix Cloud as the platform for signup, onboarding, authentication, administration, and licensing. Citrix collects and stores data in Citrix Cloud as part of the CADS service. This document describes what data is collected and methods of data collection, storage, and transmission. The information supplements, Citrix Cloud Services Data Protection Overview.

This information is for Security Officers, Compliance Officers, Information Auditors, Network Infrastructure and Operations administrators, and line-of-business owners.

Customer Content

Configuration

CADS service stores the following data provided by you:

- User information (email, user name, and region).
- IAM roles, VPC networks, Zones, Route53 zones, and application servers.
- Application delivery configurations. It includes Origin Server IP addresses, SSL certificates, and keys.

Multi-site Applications

CADS service consumes data from the Citrix Intelligent Traffic Management (ITM) service using APIs. For more information about data collection, storage, and retention on ITM service, see Citrix Intelligent Traffic Management.

Analytics

CADS service collects L3-L7 details from the Citrix instances provisioned in your premises as follows:

- **Application Dashboard** - Applications’ URL, request method, response code, total bytes, web app server details, virtual server IP addresses, client details, browser, client OS, client device, SSL protocol, SSL cipher strength, SSL key strength, ADC instance IP address, timestamp of server flaps, response content type.
- **Application DNS** - FQDN, site IP or FQDN, client subnet or resolver details.
- **Web Insight** - Virtual server IP address, clients, URLs, browsers, operating systems, requests methods, response statuses, domains, Web app server IP address, SSL certificates, SSL cipher negotiated, SSL key strength, SSL protocol, SSL failure front end.
- **Security Insight** - Client IP, URL, security violations, attack geolocation, attack timestamp, transaction ID, WAF, and ADC security configuration status.
You can view and use this information to troubleshoot the applications that are delivered through the CADS service.

**Logs**

For troubleshooting Citrix instances that are provisioned by CADS service, the following data are periodically collected from Citrix instances:

- Tech-support bundle from Citrix instances.
- SNMP traps providing alerts on the state and performance of the Citrix instances.
- Syslog of Web transactions traversing through Citrix instances and network state information.
- SMTP server details for email configuration.
- SSL certificates, SSL key, SSL CSR, CA issuer, signature algorithms of the Web apps optimized by the CADS service.
- Data Tracking for Citrix ADC Configuration Audit changes pertaining to the ADC instances, which include Web app server IP address and Citrix ADC IP address details.
- Citrix ADC configurations stored as a template, which includes Web app server IP address details.
- IP address of the Citrix instances, instance type, config backup, critical events, number of apps associated, geolocation of the data center where the Citrix instances are deployed.
- Citrix Analytics logs. For more information, see Data Governance in Citrix Analytics.

**How do we collect, store, and transmit data?**

CADS service collects data from the Citrix instances (CADS ADC and agent instances). These instances are deployed in your virtual private cloud (VPC) and data is transmitted from the instances securely over an SSL channel encrypted using the TLS 1.2 protocol to the cloud service.

Data is stored in the Relational database and as files in an Elastic File System (EFS) hosted in the AWS cloud. For more information on the commercial regions that Citrix Cloud uses and the presence of the CADS service within each region, see Geographical Considerations.

Passwords, SNMP community strings, SSL certificates, and ADC config backup are encrypted using an AES 256 key.

**References**

- For more information on how we access the collected data, see Citrix Services Security Exhibit.
Citrix App Delivery and Security service

- For more information on how long the collected data is kept, see Citrix Cloud Services Data Protection Overview.
- Citrix Cloud Technical and organizational data security measures.

Citrix App Delivery and Security service support matrix

June 14, 2022

CADS service is a SaaS offering that deploys an auto-scaling app delivery infrastructure that scales on demand.

The following tables and sections list the supported browsers, clouds, regions, and services.

Table 1: Supported browsers

To access Citrix App Delivery and Security, your workstation must have a supported web browser.

The following browsers are supported:

<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Edge</td>
<td>&quot;Citrix ended support for IE11 in Citrix Cloud on March 31, 2022.&quot;</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Chrome 19 and later</td>
</tr>
<tr>
<td>Safari</td>
<td>Safari 5.1.1 and later</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Firefox 3.6.25 and later</td>
</tr>
</tbody>
</table>

Table 2: Supported workloads

Application workloads in the following clouds are supported.

<table>
<thead>
<tr>
<th>Application</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Delivery</td>
<td>Workloads deployed on AWS.</td>
</tr>
<tr>
<td>Multi-site app delivery</td>
<td>Workloads deployed on any public cloud, private cloud, or on-premises. For on-premises, the site must be publicly addressable using an IP address or FQDN.</td>
</tr>
</tbody>
</table>
Supported AWS regions

Application workloads in the following AWS regions are supported. The availability zones supported in each region depend on your AWS subscription.

- Asia Pacific (Hong Kong)
- Asia Pacific (Tokyo)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Africa (Cape Town)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- Europe (Milan)
- Middle East (Bahrain)
- South America (São Paulo)
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Canada (Central)

Supported deployments

The following deployments are supported:

- Application servers and the CADS service app delivery infrastructure are deployed in the same VPC.
- Application servers and the CADS service app delivery infrastructure are connected via a Transit Gateway.
- Application servers and the CADS service app delivery infrastructure are connected via VPC peering.

Supported features

For an updated list of supported features, see the Data sheet.
Configure role-based access control

August 12, 2022

Citrix App Delivery and Security Service – Citrix Managed provides fine-grained, role-based access control (RBAC) using which you can grant access permissions based on the roles of individual users or groups within your organization.

You can configure individual users as administrators using the Citrix Identity provider (IdP), and individual users and user groups as administrators using Azure AD. Individual users added using the Citrix IdP or Azure AD receive an email and must click the link and complete the steps to complete the registration process. User groups added using Azure AD are automatically added as administrators with the permissions specified at the time of adding the group. A user who is part of an Azure AD group can log in using the administrator sign-in URL and enter their user credentials to access the CADS service tile.

Add individual users using Citrix IdP

All users are added in Citrix Cloud. As the first user of your organization, you must create an account in Citrix Cloud and then log on using those credentials. You are granted the superadmin role, and by default, you have all access permissions in the Citrix CADS service. Later, you can add other users in your organization in Citrix Cloud with different permissions, based on their role.

Add an administrator

During the initial onboarding process, an administrator with full rights is created. This administrator can then invite other administrators to use the CADS service. Only Citrix Cloud administrators with full access can define permissions for other administrators.

When you add administrators to your Citrix Cloud account, you define the administrator permissions that are appropriate for their role in your organization. By default, new administrators are assigned full access permissions. If you want to limit access, you can define custom access permissions.

1. In the GUI, click the Hamburger icon at the top left, and select Identity and Access Management.
2. On the **Identity and Access Management** page, select **Administrators** tab.

   This tab lists the administrators for this service that are created in Citrix Cloud.

3. In the **Select an identity provider** list, select **Citrix Identity**. Type the email ID of the administrator that you want to add.

4. Select **Custom access** for the specified administrator. This administrator cannot invite other administrators to use the CADS service.

5. Select **App Delivery and Security** and click the right arrow. The available roles are listed.
6. Select from one of the following roles:

- **AppAdministrator** - This role has permissions to create and deploy applications and global applications, and also manage SSL certificates. For more information about creating an application, see Deliver a modern application. For more information about SSL certificates, see Manage SSL certificates.
- **AppOperator** - This role has read-only permissions. App operators can monitor an application. They cannot create or deploy an application or global application, or add SSL certificates.
- **InfraAdministrator** - This role has permissions to create an environment and cloud access profiles. An infra admin can create and deploy applications and global applications,
and also add SSL certificates. For more information about creating an environment, see Manage an environment. For information about creating cloud access profiles, see Create cloud access profiles. For more information about creating an application, see Deliver a modern application. For more information about SSL certificates, see Manage SSL certificates.

7. Click **Send Invite**.

The user receives an email invite from Citrix Cloud. The user must click the link provided in the email to complete the registration process by providing their full name and password. Later, log on to Citrix Cloud using these credentials, and select the **Citrix App Delivery and Security** service.

### Modify administrator permissions

When you add administrators to your Citrix Cloud account, you define the administrator permissions that are appropriate for their role in your organization. By default, new administrators are assigned full access permissions to all Citrix Cloud account functions and available services. If you want to limit access, you can define custom access permissions.

Only Citrix Cloud administrators with full access can define permissions for other administrators.

To change existing administrator permissions:

1. Click the Hamburger icon at the top left, and select **Identity and Access Management**.
2. On the **Identity and Access Management** page, select the **Administrators** tab.
3. In the **Select an identity provider** list, select **Citrix Identity**.
4. For the administrator you want to manage, click the three dots and select **Edit Access**.

5. Select **Custom access** for the specified administrator.
6. Select **App Delivery and Security** and click the right arrow.
7. Select a role and click **Send Invite**.
Import user groups using Azure Active Directory

Perform the following steps:

1. Connect Azure Active Directory to Citrix Cloud. Ensure that you have a Microsoft Azure account and global admin access in Azure AD. For detailed steps, see Connect Citrix Cloud to Azure AD.

2. Import a user group from Azure AD. For detailed steps, see Add Azure AD administrator groups to Citrix Cloud.

App Administrator view

As an app administrator, you see the following view in the CADS service. The environments tab is not available.

Infra Administrator view

As an infra admin you see the following view in the CADS service. The environments tab is available.
**Custom access administrators view**

As an app administrator, app operator, or infra administrator, you see the following view in the Cloud. You cannot add administrators.

![Diagram of Citrix App Delivery and Security service](image)
Get started with Citrix App Delivery and Security service – Citrix Managed

March 30, 2022

This document walks you through the onboarding and setting up Citrix App Delivery and Security Service – Citrix Managed for the first time. Perform the following steps to get started.

Sign up for Citrix Cloud

Create a Citrix Cloud company account or join an existing one that someone else in your company has created. For detailed instructions, see Sign up for Citrix Cloud.

Request the Citrix App Delivery and Security entitlement

After you log on to Citrix Cloud, do the following:

1. Go to the Available Services section.

2. On the App Delivery and Security tile, click Manage.
   The tile moves to the My Services section.
3. In **Citrix App Delivery and Security Service**, click **Request Trial** to start the initialization.

4. Choose a region.
Choose a region

Select a region that best suits your performance and business needs.

- North America
- EMEA
- Asia Pacific

I understand that I cannot change the region after set up.

5. Choose a role.

Welcome to Application Delivery and Security.
Select roles and use cases that apply to you

- Network Admin /ITOps: Manage, monitor and migrate applications
- App Admin/CloudOps: Deliver, manage, monitor and troubleshoot applications
- SecOps: Secure the applications
- DevOps: Automating application delivery and security

Initialization is in progress.
6. Select from one of the following options:

   • **Deliver an Application**: Specify the services that represent your origin application servers, and endpoints that users use to access the application. For more information, see [Deliver a modern application](#).

   • **Deliver a Multi-Site Application**: You can deploy your apps across multiple locations to improve application performance and availability, reduce latency, and optimize user experience. For more information, see [Deliver a multi-site application](#).
Overview of Citrix App Delivery and Security service – Citrix Managed

March 30, 2022

Citrix App Delivery and Security Service – Citrix Managed provides an outcome-focused model that allows you to specify the functional and business intent of your application deployment. Based on the specified functional intent, Citrix App Delivery and Security Service – Citrix Managed creates policies to configure functionalities, such as security protection, load balancing, SSL offloading, content rules, and multi-site applications. For example, you select A+ profile and the service configures the ciphers and other entities required to get an A+ rating from Qualys Labs for your applications.

The service continuously optimizes the deployment by auto-redirecting traffic to a better site, auto-removing a server, or autoscaling capacity dynamically to match the application’s needs.

Discovery-driven configuration paradigm aims to automate, speed-up, and simplify the laborious process of application delivery, by discovering origin application servers automatically using APIs. For example, when specifying the application servers, you can specify the application EC2 instances or an AWS application Autoscale group. The service continuously maps these IDs to their corresponding IP addresses and discovers new IP addresses used by the application, or IP addresses that are no longer part of your application. The service also manages the allocation of your application public IP addresses and registers them in AWS Route 53 with a user provided domain name.

Based on the business intent, Citrix App Delivery and Security Service – Citrix Managed auto-sizes the required infrastructure and adjusts it on demand. For example, the service auto-adjusts if there is a change in the number of the origin application servers due to scaling events, and changes stickiness
settings accordingly. After delivering the applications, you can use the rich analytics in Citrix App Delivery and Security Service – Citrix Managed to:

- Monitor application performance.
- Troubleshoot using the detected anomalies.
- Visualize the threat details associated with security and take corrective actions to secure the applications.

The following diagram depicts the workflow.

![Workflow Diagram](image.png)

Citrix App Delivery and Security provides the following benefits:

- **Intent based workflows**: Prepares your AWS VPC to make it ready for delivering your application based on the specified intent.
- **Elastic provisioning**: Provides on-demand provisioning and scaling of ADCs based on your application load. Your infrastructure is scaled up during heavy traffic and scaled down when there is less demand.
- **Simplified deployment**: Deliver your applications in minutes. The service can also seamlessly integrate with AWS cloud native services and systems. You save on installation and configuration time, and also avoid wasting time and resources on potential errors introduced by the manual process.
- **Operational efficiency**: Optimized and automated way to achieve higher operational productivity. Your operational costs are reduced by saving your time, money, and resources on maintaining and upgrading the traditional application delivery infrastructure. And you only pay for your actual consumption.
Citrix App Delivery and Security service

- **Analytics**: The service aggregates data across all the applications and identifies anomalies in performance and security.

**Architecture**

The following diagram illustrates the infrastructure of how Citrix App Delivery and Security is provisioned during delivery of applications on AWS.

---

**Important**

Do not make manual changes to the infrastructure managed by Citrix App Delivery and Security. Doing so might interfere with the functioning of the service.

Citrix App Delivery and Security provisions the following elements in your AWS VPC:

- Three subnets, one each for management network, client network, and server network.
- NAT gateway that routes management (control plane) traffic from both the ADC and the agent to the internet.
- Route table that contains entries for enabling management traffic to go to the internet through the NAT gateway.
- Citrix agent instance that is a proxy for the service. An agent enables the service to communicate with one or multiple ADCs deployed in your VPC.
- Security groups that are associated with the ADC instances and the agent. Security groups control inbound and outbound traffic.

**Note**

Only port 80 and port 443 are open.
Citrix App Delivery and Security service

- **ADC Autoscale cluster** - A set of ADC instances that provide the ADC functionality. ADC instances receive traffic and distribute traffic to your application servers.

**Notes**

- Citrix App Delivery and Security does not make any changes to the resources created by you in your VPC. It only provisions all the necessary infrastructure to deliver your applications. Provisioning includes cloud native infrastructure, such as network gateways, routing tables, subnets, security groups, ADC instances, and ADS service-agent instances. Provisioned ADC instance names start with the prefix “Citrix-“ for easy identification in your AWS console.

The following diagram illustrates the traffic flow in your environment. Application traffic is distributed across multiple availability zones depending on the deployment of your application servers. The ADC cluster processes the traffic and selects an origin application server to handle the request, based on the configured load balancing settings. The origin application server might be in the same or a different availability zone.
Create cloud access profiles

March 10, 2022

A cloud access profile is used by the Citrix App Delivery and Security service to acquire permissions on the customer’s AWS account for deploying application delivery infrastructure in customer owned VPCs. To create this profile, you must be the AWS account administrator that has the necessary permissions on the VPC that you intend to use for delivering your applications. Your AWS account must allow you to use AWS CloudFormation and IAM services.

As part of creating the cloud access profile, two IAM roles on AWS are created. One IAM role gives permissions to the service to provision infrastructure on your AWS account, such as networks, NAT Gateways, security groups, and ADC instances. The other IAM role is used by the ADC VPX instances deployed in your account. The role is used to enable support for back-end auto scaling, if your application servers are deployed as an AWS autoscaling group.

Citrix provides a ready-made CloudFormation template (CFT) to simplify the configuration of these two IAM roles. The template helps an administrator in creating these two IAM roles that are needed for the cloud access profile creation.

IAM role created for Citrix App Delivery and Security service

The IAM role gives permissions to the service’s AWS account to create and delete entities in AWS on your behalf.

The following high-level permissions are granted to the service:

- Provision instances using EC2.
- Create and delete security groups and subnets.
- Create and delete NAT gateway.
- Create and delete network load balancers.
- Create and delete DNS hosted zones and DNS records inside zones using AWS Route 53.
- Attach and remove IAM roles to and from instances.

These high level permissions are used by the service in the following scenarios:

1. When the first application is deployed in a VPC:
   - New ADC EC2 instances are assigned the second IAM role to enable back-end Autoscale support.
   - NAT gateway, subnets, and security groups are created.
   - Citrix agent and Citrix ADCs are provisioned.

2. When more applications are later deployed in the same VPC:
   - IP addresses are acquired in the ADCs for the application.
   - Network load balancing is configured with these application IP addresses.
Citrix App Delivery and Security service

- DNS entries are created with the domain specified for the application.

3. When autoscaling of ADCs is done to adjust to the traffic patterns. For example, a new ADC instance is created if the existing set of ADCs is operating at full capacity.

The IAM role is the mechanism in AWS by which you grant these permissions to the AWS account in which you run the service.

**IAM role created for Citrix ADC VPX instances**

During infrastructure provisioning when the first application is deployed in a VPC:

- The ADC VPX instances are created.
- The IAM role with the following set of permissions is assigned to the VPX instances by the service.

The high-level permissions are used for tasks such as:

- Change IP address on network interfaces.
- Listen to the Amazon simple queue service (SQS).
- Learn about changes to Autoscale groups.

The permissions are needed for the ADC in the following scenarios:

- During application delivery with origin application servers that are part of an Autoscale group. The ADC calls the AWS services to find the list of origin application servers that are part of the Autoscale group.
- If the ADC cluster head fails or if the cluster ADC head is not reachable, then the ADC selects a new cluster head. The ADC then shifts the cluster head IP address to the newly elected cluster head.

**Create a cloud access profile**

1. Click **Environments**.

2. In the **Cloud Access Profiles** tab, click **Create**.

3. Type a name for the profile and click **Generate Template**.

4. Follow the instructions to create a profile.

5. Click **Create**.

**Manage an environment**

July 26, 2022
An environment represents the infrastructure that is used for application delivery. The necessary infrastructure, such as gateways, agents, and ADCs, is prepared as part of the environment deployment. Once deployed, this environment can be used to deliver multiple applications.

The Citrix App Delivery and Security service provisions the following elements in the customer's AWS VPC as part of environment deployment:

- Deploy AWS CFT to create the following entities in the customer's AWS VPC:
  - Three subnets: One each for management network, client network, and server network. You can specify the server subnet details. For more information about how and when to do so, see How does the CADS service connect to the origin application servers.
  - NAT gateway that routes management/control plane traffic from both the ADC and the agent to the internet.
  - Route table that contains entries for enabling management traffic to go to the internet through the NAT gateway.
  - Security groups that are associated with the ADC instances and the agent. Security groups control inbound and outbound traffic.
- Citrix agent instance that is a proxy for the service. An agent enables the service to communicate with one or multiple ADCs deployed in the customer VPC.
- ADC Autoscale cluster (a set of ADC instances) that provide the ADC functionality. ADC instances receive traffic and distribute traffic to your application servers.

### Subnets

The service creates three subnets per availability zone for deploying the app delivery infrastructure. Each subnet has 255 addresses. That is, the service blocks 765 (3*255) IP addresses. Ensure that the following conditions are met for the VPC CIDR block size where the app delivery infrastructure is deployed:

- To deploy the environment in two availability zones, the VPC CIDR block size must be greater than the /21 netmask (2,048 IP addresses).
- To deploy the environment in one availability zone, the VPC CIDR block size must be greater than the /22 netmask (1,024 IP addresses). Since the infrastructure is deployed in one availability zone, Citrix recommends to not use it for a production environment. It is best suited for staging or POC.

### How does the CADS service connect to the origin application servers

The CADS service provisions the infra in different subnets in your VPC to connect to your origin application servers. Typically, you configure your application server's security group to allow ingress traffic from all the IP addresses in the VPC. This works well by default because during environment...
Citrix App Delivery and Security service

creation in the CADS service, it creates subnets in the VPC for provisioning the infra to reach your origin application servers. However, to increase security, you can restrict the IP addresses that the CADS service uses to connect to your application servers. You can do so during environment creation by specifying the subnets you created exclusively for the CADS service. Doing so, avoids creating default subnets, and the service provisions the infra in the specified subnets. Also, ensure that you change your application server's security group to allow ingress traffic from the subnets you have specified.

Specify a subnet

1. While creating an environment, select Specify subnets to be used by the CADS infra to reach the origin application servers.
2. Specify subnets for each of the availability zones.

Note

If your application servers are in different VPCs, ensure that Transit Gateway and VPC peering are configured for the customized subnets.

Connect to an application server in a different VPC

Deploying the app delivery infrastructure in the same VPC as the origin application servers saves cost and reduces management overhead. However, you might want to deploy both in different VPCs to isolate the infrastructure. For this deployment to work, the app delivery infrastructure in one VPC must be able to send traffic to the origin application servers in another VPC.
Citrix App Delivery and Security service

To establish communication between the VPC of the app delivery infrastructure and the VPC of the origin application servers, the following options are available:

- **VPC Peering**: Use for network connections between two VPCs.
- **Transit Gateway**: Use for network connections between many VPCs.

The terms app delivery infrastructure VPC and CADS VPC are used interchangeably in this document.

**Prerequisites**

Configure VPC peering or Transit Gateway in your AWS account so that you can select them in the CADS service GUI.

**Notes**

- The origin application server VPC cannot have overlapping CIDRs with the CADS VPC.
- To avoid latency between the CADS VPC and the origin application servers, both must be in the same region.

For VPC peering, perform the following steps in your AWS account:

1. Create a VPC peering connection between the CADS VPC and origin application server VPC. A peering ID is allocated as a result.
2. Add entries to the route table for application servers to respond to the CADS VPC using the peering ID. For a sample routing table entry, see Routing table for the VPC peering option.
   
   **Note**

   The CADS service configures the routes for the CADS VPC to send traffic to the origin application server VPC.

3. Add rules to the security group attached to the origin application server to allow traffic from the CADS VPC.

For Transit Gateway, perform the following steps in your AWS account:

1. Create a transit gateway.
2. Attach the VPC of the origin application servers to the transit gateway.
3. Add entries to the route table for the origin application servers to respond to the CADS VPC. For a sample routing table entry, see Routing table for the Transit Gateway option.
   
   **Note**

   The CADS service configures the routes for the CADS VPC to send traffic to the origin application server VPC.

4. Add rules to the security group attached to the origin application server to allow traffic from the CADS VPC.
For more information about VPC peering and Transit Gateway, see the AWS documentation.

Routing table for the VPC peering option

This section helps in adding entries to the route table for origin application servers to respond to the CADS VPC by using the peering ID.

For the preceding illustration, the routing table entry in the origin application server VPC must be defined as follows:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.2.0.0/16</td>
<td>peering ID</td>
</tr>
</tbody>
</table>

Routing table for the Transit Gateway option

This section helps in adding entries to the route table for origin application servers to respond to the CADS VPC by using a transit gateway.
For the preceding illustration, the routing table entry for each origin application server VPC must be defined as follows:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.2.0.0/16</td>
<td>TGW</td>
</tr>
</tbody>
</table>

**Create an environment**

1. In the left navigation pane, click **Environments**.
2. In the **Environments** tab, click **Create**.
3. Specify values for the following parameters:
   - Name
   - Cloud Access Profile
   - AWS Region
   - Availability Zones
   - AWS VPC - The VPC where the app delivery infrastructure is to be deployed.

   If the app delivery infrastructure and origin application servers are in different VPCs, speci-
ify the following parameters for the origin application servers.

- AWS VPC
- Subnet

Select how the CADS service connects to the origin application servers. Options are as follows:

- VPC Peering

- Transit Gateway
Auto-upgrade an environment

As a network administrator, you might manage many Citrix environments running on a CADS service release in Citrix App Delivery and Security. The CADS service upgrades a Citrix environment to the latest builds.

Benefits

The CADS service automatically creates maintenance jobs to upgrade your Citrix application environments. The auto-upgrade feature provides the following benefits.

- Seamless Upgrade of CADS service data plane (Citrix environments).
- Monitor the service to quickly react to alerts before the traffic impact.
- Service level agreement management.

Prerequisites

You have created an environment and a cloud access profile.
Introduction

The CADS service auto-upgrade is one of the major operational activities. To ease the process, CADS service upgrade helps you monitor your environment in the following ways:

- The CADS service UI indicates that it has scheduled an upgrade for the environment and creates the upgrade slot for these environments. With this upgrade, you get access to the advanced and latest features. You receive updates on new features and fixed issues.
- The CADS service provides three time slot options to pick from and upgrade the environment. If you do not choose a time slot from the suggested options, the CADS service automatically upgrades the environment in the default upgrade time slot.
- The CADS service provides infrastructure administration and configuration of the environment by upgrading to the latest builds.
- The CADS service offers security upgrades.

The upgrade advisory provides a link to the corresponding release notes. With this information, you can review the updates on new features and fixed issues. The CADS service creates a maintenance job to upgrade the Citrix environments. You can choose the required time slot for upgrade from the time slot options provided in the Upgrade Advisory page.

View upgrade advisory

Navigate to Applications> Environments> Settings to view the following information.

- The list of environments and their upgrade status.
- The environments on which the upgrade is scheduled.
- The environments on which the upgrade is in-progress.
   This view also shows the percentage of upgrade completed and the estimated time to complete the upgrade job in the pie chart. The pie chart representation of the in-progress upgrade is also shown in the Environments page.
- The Citrix environments in error state due to upgrade failure. Shows the red symbol for the errored state.
- The Citrix environments on which upgrade is completed show a green tick status.

The Upgrade Advisory page displays the available environments. The Release Notes link guides you to the specific CADS service release notes. You can review the new features, fixed, and known issues. As an administrator, you can choose an option from the available three time slot options for the upgrade job. Do the following to upgrade the environment in the required time slot:

1. In Environments, click Settings.
2. Select the Default schedule or the Select from system recommendation schedule.
3. Click Save.
Upgrade Citrix environments

In the Upgrade Advisory page, after your review, you can do the following:
Select one of the two options:

1. Default schedule – the CADS service automatically upgrades the environment.
2. Select from system recommendation – select the time slot from the three options provided by the CADS service.
   If the recommended time slot is not selected, the CADS service automatically upgrades the environment at the default upgrade time slot.

Default Schedule:

1. The system automatically schedules an upgrade and updates the time slot in the Status column.
2. Click Save.

Select from system recommendation:

1. Select the required time slot from the drop-down list, the selected time slot is shown in the Status column.
   The Status column also displays the upgrade status.
2. Click Save.

Notes:

- If an autoupgrade fails, the Citrix environment rolls back to the previous version and moves to the errored state. The upgrade will be scheduled in the next iteration.
- If the rollback also fails, contact Citrix support to resolve the issue. During this time the traffic is uninterrupted for the existing environment.

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Undeploy an environment

When you undeploy an environment that has one or more applications in the DEPLOYED state linked to it, all the applications linked to that environment are deleted after you confirm in the dialog box.

You can choose to cancel, undeploy the application first, and then come back to undeploy the environment.

Deliver a modern application

August 19, 2022

An application is the central component in Citrix App Delivery and Security and contains the application delivery and security information required to deliver the customer’s application. Two main components of an application are its services and endpoints. Services correspond to the customer’s application servers. Endpoints correspond to the FQDN and virtual IP addresses that users use to reach the application.

The configuration of an application is organized as a set of application delivery features. These features help in optimizing, securing, accelerating, and ensuring availability of customers applications. Each application delivery feature allows a user to configure a specific feature provided by Citrix App Delivery and Security. Together they constitute the overall application delivery configuration for your application.
Citrix App Delivery and Security service

Create services to represent your origin application servers. You can select a default service profile that contains the most commonly used settings for a service. Alternately, you can create your own service profile and specify the load balancing settings, back-end SSL settings, and health checks for your servers. For more information about services, see Create services. For more information about service profiles, see Create service profiles.

Using the authentication feature, admins can add SAML authentication to the apps. Once authentication is enabled, only authenticated users are allowed to access specific services configured by the admin. For more information, see Authentication.

Using content rules, you can evaluate an incoming request and apply one or more actions based on the evaluation. For example, you can drop a connection if DDoS attack is suspected or manipulate the data in HTTP requests and responses. Citrix App Delivery and Security supports both rewrite and responder content rules. For more information, see Content Transform.

The security protection feature of Citrix App Delivery and Security protects your applications from security threats. Create security protection to configure features, such as allow or block requests, add exceptions, define rules to examine the traffic, geo blocking, rate limiting, and cookie consistency. Exceptions can be added for cross-site scripting protection and buffer overflow protection. Exceptions help avoid false positives and bypass the traffic. For more information, see Security protection.

Also, you no longer have to guess where to host the application servers. Based on the traffic insights, such as latency, availability, and throughout, Citrix App Delivery and Security recommends the best locations for hosting your applications. For more information, see Multi-site application.

Before you can create an application, you must create at least one cloud access profile and one application environment.

A classic application in the Citrix App Delivery and Security Service – Citrix Managed (CADS) service offers granular control over the configuration as compared to a modern application and is recommended for advanced Citrix ADC users. For more information, see Deliver a classic application.

Create an application

Follow these steps to create an application:

1. Specify application details.
2. Create services.
3. Add endpoints.
4. Configure authentication for the endpoints.
5. Add Content transform.
Specify application details

You must have at least one environment before you can proceed with application creation.

1. Navigate to Applications > New Application.
2. Type a name for the application.
3. (Optional) Select an API Definition from the list. For information about creating API definitions, see API definitions in the Citrix App Delivery and Security service.
4. Select an environment.
5. Click Next.

Manage an application

In the Applications page, click one of the following options in the Actions column to manage your deployed apps. Redeploy the application after making changes.

- Edit
- Redeploy
- Undeploy
- Health Status
Modify and redeploy an application

You can edit the application details, services, endpoints, load balancing, content rules, and security protection settings for an application.

1. Navigate to the Applications page.
2. For applications whose status is Deployed, click the three dots in the Actions column.
3. Click Edit.
4. Click any of the tabs to change the configured values and click Deploy.

You have completed the steps to modify and redeploy an application.

Check the health status of an application

The health status displays the real-time health of your deployed applications for each application service in an availability zone.

1. Navigate to the Applications page.
2. For applications whose status is Deployed, click the three dots in the Actions column.
3. Click Health Status.

The following status indicates that the application is healthy.
The following status indicates that the application is partially up because some of the services are
down.

Application Status

State: Partially UP

Details:
us-east-1c:
- svc301: UP
- svc302: DOWN

us-east-1a:
- svc301: UP
- svc302: DOWN
If all the services are down, the following status is displayed.

**Application Status**

**State:** DOWN

**Details:**
- us-east-1c:
  - svc101 : DOWN
- us-east-1a:
  - svc101 : DOWN

**Done**
Create services

July 7, 2022

The services tab comprises services and service profiles. Services represent the back-end servers in your VPC. These servers are the origin servers of your application. Service profiles contain the load balancing and SSL settings for these services. Two service profiles are available by default: Default HTTP Profile and Default HTTPS Profile. While creating a service, if you select one of these default profiles then creating a service profile is not mandatory. However, if you create a service profile, you must create a load balancer.

1. Click Create Service.
2. Specify values for the following parameters:
   - Name
   - Protocol: Select HTTPS to create an SSL service. For more information, see Configure an SSL profile.
   - Port
   - Service Profile: Select an existing profile or create a service profile. For information about creating a service profile, see Create service profiles.
   - App Server Type: Select from Auto Scaling Group, EC2 Instances, or Servers. Select an auto-scaling group, EC2 instance, or server type respectively. Only app servers from the selected environment are displayed.
     - Server type includes two options: IP address and FQDN. Select an option.
     - Specify an IP address or FQDN, and click Add Server. The details appear in the List of Servers table.
3. Click **Create**.
4. Click **Next**.

### Self-heal slow application servers

A poorly performing server can affect the performance of your applications. If an Autoscale group, or EC2 instances with IP address in AWS is configured, the self-healing capability of the CADS service can detect a slow server and take remedial action accordingly.

For example, if the response time of one of the servers is consistently poor, the CADS service identifies this server, and gracefully replaces it with a healthy server.

The service considers the following conditions while replacing a faulty server:

- All persistent connections are honored.
- Existing connections are completed.
- New connections aren’t accepted for the faulty server.

Related actions taken by the CADS service are logged and admins can view them in the Action History. For more information, see [Monitor self-healing](#).

### Configure detecting and auto-replacing a slow server

1. Navigate to **Applications > New Application**.
2. Type a name for the application, and select an environment.
3. Click Next.
4. Click Create Service.
5. In the Create Service page, type values for the following parameters:
   - Name
   - Protocol
   - Port
   - Service Profile
   - App Server Type - Select either Auto Scaling Group, or Servers
     You can auto-replace a slow server, if the server is added using an IP address and hosted as an EC2 instance in AWS.
     If you select Servers, select the IPAdress in the Address Type drop-down, and enter the required IP address in the IP Address field. FQDN is not supported.
   - Select a group from the list.
6. Slide the following toggles to enable the functionality:
   - Detect slow server
   - Auto-replace slow server
Create service profiles

June 10, 2022

A service profile is a predefined set of the service-related configuration that includes load balancing, back-end SSL, and health check settings. Every service must have a service profile associated with it.

The CADS service provides you two default service profiles, Default HTTP Profile and Default HTTPS Profile. While creating a service, you can associate one of these default profiles or create a profile according to your preference. If you select one of these default profiles then creating a service profile is not mandatory. If you create a service profile, you must create a load balancer. You can define other service-related settings as per your preference.

Configure load balancing

In a real-world scenario with a limited number of servers providing service to many clients, a server can become overloaded and degrade the performance of the server farm. Using load balancing algorithms, you can evenly distribute network traffic to avoid overloading any resource. The result is a better experience for end users in terms of improved performance and availability of your apps.

The load balancing module of the Citrix App Delivery and Security distributes client requests across multiple app servers, such as EC2 instances, FQDN/IP address-based servers, and Autoscale groups.

When the Citrix App Delivery and Security receives a client request, it selects a target server based on the specified rules or routes all traffic to the default server. It uses load balancing criteria to prevent bottlenecks by forwarding each client request to the server best suited to handle the request when it arrives.

Specifying the maximum number of requests per server ensures that a server is not overloaded. You can also specify a URL to redirect traffic, to avoid dropping requests if a server is not reachable.

Prerequisites

1. You have created an environment and a cloud access profile.
2. You have specified the basic details, such as the name of the application and environment by navigating to Applications > New Application. For more information, see Deliver an application.

Before you begin

Decide which algorithm and stickiness you plan to use for your load balancer. The following algorithms and stickiness are supported.
Algorithm

Algorithm is the method used to direct the client request to the server. In the HASH methods, the Citrix App Delivery and Security extracts a predetermined portion of the request, creates a hash of the portion, and uses that value to select the server.

The following methods are supported:

- **Round Robin**: Requests are distributed across the servers sequentially regardless of the load.
- **Least Connection**: Request is assigned to the server with the least number of active connections depending on the relative compute capacity of the server. This method is the most used method and is also the default method.
- **Least Response Time**: Request is assigned to the server with the lowest average response time.
- **SOURCEIPHASH**: Create a hash of the source IP address.
- **DOMAINHASH**: Create a hash of the domain name, or part of the domain name if it exceeds 80 characters, in the request. The domain name is taken from either the URL or the host header. If the domain name appears in both, the URL is preferred. If the request does not contain a domain name, the algorithm defaults to LEASTCONNECTION.
- **URLHASH**: Create a hash of the request URL, or part of the URL if it exceeds 80 characters.

Stickiness

The Citrix App Delivery and Security uses the configured load balancing method for the initial selection of a server. It forwards all subsequent requests from the same client to that same server during a session. This setting is especially helpful in shopping cart and banking transactions. However, a server can become overloaded if it has too many open sessions or a specific session requires more resources.

The following stickiness types are supported:

- **NONE**: No stickiness is configured. Successive requests from the same client are directed to any server. This option is the preferred one for stateless applications. This value is the default value.
- **SESSION COOKIE**: The Citrix App Delivery and Security inserts an HTTP cookie that is used to direct all requests to the same server during a session. This cookie uniquely identifies the session when a client accesses the application for the first time. It then refers to the cookie for subsequent requests from the same client. The HTTP cookie inserted by the service is a temporary cookie and is erased when the browser is closed. This type of stickiness is typically selected when the stickiness must be valid only until the browser is open.
- **STICKY COOKIE**: The Citrix App Delivery and Security inserts an HTTP cookie that is valid for the configured duration. Default duration = 2 mins.
- **SOURCEIP**: Connections from the same IP address belong to the same stickiness session. That is, all requests from the same source IP address are forwarded to the same server for the configured duration. Default duration = 2 mins.
• **SSLSESSION** - Connections with the same SSL session ID belong to the same stickiness session. The back-end app server assigns an SSL session ID to each session. All requests with the same SSL session ID are forwarded to the same server for the duration configured. For example, use SSL session ID if you cannot use source IP stickiness because the device is behind a NAT gateway. As a result, the requests might not have the same source IP address. Default timeout= 2 mins.

**Create a load balancer**

A default load balancer is bound to all services through the service profile. If you create a service profile, you must create a load balancer.

1. Navigate to **Applications > New Application**.
2. Type a name for the application, and select an environment.
3. Click **Next**.
4. Click the **Service Profiles** tab.
5. Click **Create**.
6. In the **Create Service Profile** page, type a name for the profile and click **Create**.
7. In the **Create Load Balancer** page, specify values for the following parameters.
   - Name* - Name for the load balancer.
   - Algorithm*
• Stickiness
  • Stickiness Timeout - Time period, in minutes, for which stickiness is in effect. After the timeout expires, the request is treated as a new request and can be directed to any server depending on the configured load balancing algorithm.
• Max Connections to Server - Maximum number of permissible simultaneous open connections per server. This number ensures that the server is not overloaded.
• Redirect URL - If the server is DOWN or not reachable due to any reason, the requests are dropped. To avoid such a situation, you can specify a URL to redirect traffic to, if none of the servers are reachable. For example, the redirect might be to a page that simply states that “The servers are not reachable. Try after some time.”
* Indicates a required parameter

8. Click Create.
9. Click Create.
10. Click Next.

Configure back-end SSL settings

SSL settings on the CADS service contain settings related to SNI, server authentication, cipher suites, and protocol versions configured on a back-end SSL application server.
Support for SNI on the back-end application servers

The CADS service supports dynamic SNI on the back-end TLS connections. SNI helps to enable SSL encryption on multiple domains if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net.

If the back-end server is configured for multiple domains, the server can respond with the correct certificate based on the SNI received in the Client Hello message. The service learns the SNI in the client connection and uses it in the server-side connection. In other words, the common name received in the SNI extension of the Client Hello message is forwarded to the back-end SSL connection.

When server authentication is enabled, the server certificate is verified by the CA certificate and the common name/SAN entries in the server certificate are matched with the SNI. Therefore, the CA certificate must be bound to the service.

1. Navigate to Applications > New Application.
2. Type a name for the application, and select an environment.
3. Click Next.
4. Click the Service Profiles tab.
5. Click Create.
6. In the Create Service Profile page, type a name for the profile and click Backend SSL.
7. Click Configure SSL Settings.
8. In the Create SSL Policy page, type a name for the policy, select SNI, and click Create.
The policy is listed on the Backend SSL tab in the Create Service Profile page.

9. Click Create.

10. Click Next.

**Configure server authentication**

Since the CADS service performs SSL offload and acceleration on behalf of an application server, the service does not usually authenticate the origin application server’s certificate. However, you can authenticate the server in deployments that require end-to-end SSL authentication.

In such a situation, the service becomes the SSL client and carries out a secure transaction with the back-end application server. It verifies that a CA whose certificate is bound to the service has signed the server certificate, and checks the validity of the server certificate.

To authenticate the server, enable server authentication and select the certificate of the CA that signed the server’s certificate to the SSL service.

1. Navigate to Applications > New Application.

2. Type a name for the application, and select an environment.

3. Click Next.
4. Click the Service Profiles tab.

5. Click Create.

6. In the Create Service Profile page, type a name for the profile and click Backend SSL.

7. Click Configure SSL Settings.

8. In the Create SSL Policy page, type a name for the policy, select Server Authentication, and click Create.

The policy is listed on the Backend SSL tab in the Create Service Profile page.

9. Click Bind CA Certificates.

10. Click Create SSL Certificate.

11. Specify a name for the certificate and choose a certificate file. CA certificates don’t need a key.
12. Click **Create**. The certificate is listed on the SSL certificates page.

13. Click **Create**.
14. Click Next.

**Configure SSL cipher suites and protocol**

SSL cipher suites help to establish a secure connection between your app servers and the client. Select the cipher suites to use in your setup.

Protocol version is used during an SSL handshake. Select one or more protocol versions that your app servers support. By default, the highest protocol version that both peers support is selected.

1. Navigate to Applications > New Application.
2. Type a name for the application, and select an environment.
3. Click Next.
4. Click the Service Profiles tab.
5. Click Create.
6. In the Create Service Profile page, type a name for the profile and click Backend SSL.
7. Click Configure SSL Settings.
8. In the Create SSL Policy page, type a name for the policy.
9. Click Select All Cipher or select individual cipher suites from the list. You can expand each group to view the ciphers that are part of the group and, select or unselect individual ciphers.
10. Select the Protocol Version.
11. Click Create.
The policy is listed in the **Backend SSL** tab on the **Create Service Profile** page.

12. Click **Create**.

13. Click **Next**.

**Configure health checks**

Health checks monitor the health of servers by sending probes to the back-end app servers. If the server responds within the specified time interval, the state of the server is set to UP. That is, the server can accept traffic. If the server does not respond to the designated number of probes within the specified time period, the server is set to DOWN. No requests are forwarded to this server until its state changes to UP. Traffic is distributed only among healthy servers.
1. In the **Create Service Profile** page, click **Health Checks**.

2. Click **Add Health Check**.

3. Specify values for the following parameters:
   - **Name** - Name for the health check.
   - **Protocol** - Protocol of the health check and port number used by the server in your EC2 instance.
   - **Port** - Destination port where the health checks are sent. If this parameter is not configured, the health checks are sent to the same port as regular traffic.
   - **Interval** - Time interval, in seconds, between two successive health checks to the server. Must be greater than the “Response Timeout” value.
   - **Response Timeout** - The time, in seconds, within which a response must be received from the server. Must be less than the “Interval” value.
   - **Unhealthy Time Interval** - Time interval, in seconds, between two successive health checks to an unhealthy server.
   - **Failed Check Count** - Number of failed health checks after which a server is marked unhealthy.
   - **Request URL Path** - HTTP request URL path to which health checks are sent. Applicable only to HTTP/HTTPS health checks. A “/” specifies that the monitor checks the server. To check a specific endpoint, specify the URL for the endpoint. For example, if the server is “example.com” then a specific endpoint might be “/example.com/comments.html”.
   - **Request Header** - HTTP header to be sent in the health checks. Applicable only to HTTP/HTTPS health checks.
   - **ResponseType** - Expected HTTP response code or text to be present in the HTTP response body to mark the server as healthy. Applicable only to HTTP/HTTPS health checks.

* Indicates a required parameter
4. Click **Add**.
   The configured health checks are displayed in a tabular format.

5. Click **Create**.

6. Click **Next**.

**Add endpoints**

June 2, 2022

Endpoints represent the FQDN or the IP address that clients connect to. It can be internal, that is within the VPC. Clients can access the application only within the internal network. If an external endpoint is selected, any client can access the application over the internet.
The FQDN can be auto allocated or user-defined. Auto-allocated lets you use a DNS provider other than AWS Route 53. The FQDN is displayed after you deploy the application. You must add this FQDN as a CNAME in your authoritative DNS zone configuration. User-defined lets you use AWS Route 53 as a DNS provider to host your application's FQDN. You must have bought and registered a domain with Route 53. That is, the zone must be properly acquired from AWS or delegated to AWS. For more information, see https://docs.aws.amazon.com/acm/latest/userguide/setup-domain.html. For example, if the registered zone is example.net and the domain is app1, then app1.example.net is the FQDN that clients connect to access your app.

An endpoint must have a default content route associated with it. The route includes the conditions and a target service. If the traffic matches the condition, the request is directed to the specified service.

Choose the clients who can access your application. Select Internal to deliver your application privately within the VPC. Only clients within the data center or VPC can access the application. Select External to deliver your application publicly. Any client on the internet can access the application.

Also specify the FQDN generation mode. Select Auto-allocated if you want to use a DNS provider other than Route 53 to host your application's FQDN. The auto-allocated application FQDN is displayed in the Application dashboard after the application is deployed. Configure your application FQDN in your DNS provider as a CNAME record by using the auto-allocated FQDN. Select User-defined if you want to use Route 53 as a DNS provider to host your application's FQDN. The application FQDN's DNS zone must already be hosted in Route 53. Define an FQDN for the application. It is auto-configured in Route 53 during application deployment.

You can create or select an endpoint.

Follow these steps to select an endpoint.

1. Navigate to Applications > New Application.
2. Specify basic details, such as name of the application, environment, and services. For more information, see Deliver an application.
3. Click Select.
4. In the Select Endpoint page, select an endpoint from the list and click Add.

Follow these steps to create an endpoint.

1. Navigate to Applications > New Application.
2. Specify basic details, such as name of the application, environment, and services. For more information, see Deliver an application.
3. Click Create.
4. Specify values for the following parameters:
   - Name
   - Access: Specify Internal or External.
Citrix App Delivery and Security service

- FQDN: Specify **Auto allocated** or **User defined**.
- Protocol: Specify **HTTP** or **HTTPS**. If you select HTTPS, you must add a certificate and optionally, add an SSL policy to get an A+ rating for your applications. For more information, see Add an SSL certificate. You can select one or more certificates, if present, from the list. Select **Auto Redirect HTTP traffic to HTTPS** to ensure that the clients communicate over secure SSL.
- Port

5. Click **Create**.

6. (Optional) To add a route based on some conditions click **Add**. Specify a name, condition, and a target service. Click **Add**.
Conditions and their corresponding operators and values are listed in the following table:
<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
<th>Operators</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Request URL</td>
<td>Identifies an element in the URL portion of an HTTP request.</td>
<td>Contains, Equals,</td>
<td>URL Path</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Startswith, Endswith,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not contains, Not equals,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not startswith, Not</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>endswith</td>
<td></td>
</tr>
<tr>
<td>HTTP Request URL Suffix</td>
<td>Identifies an element in the URL suffix of an HTTP request.</td>
<td>Contains, Equals,</td>
<td>URL Suffix Value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Startswith, Endswith,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not contains, Not equals,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not startswith, Not</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>endswith</td>
<td></td>
</tr>
<tr>
<td>HTTP Request Method</td>
<td>Identifies an element in the HTTP request or response by using a method in the HTTP request to evaluate HTTP request data.</td>
<td>Equals, Not equals</td>
<td>GET, PUT, POST, DELETE</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>Identifies and returns the client IP address in a TCP/IP packet.</td>
<td>Between, Equals,</td>
<td>IP Addresses, Subnet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Insubnet, Not between,</td>
<td>IP Addresses, Range</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not equals, Not insubnet</td>
<td>Start, Range End</td>
</tr>
<tr>
<td>Client TCP Address</td>
<td>Identifies and returns the source port in a TCP/IP packet.</td>
<td>Equals</td>
<td>TCP Source Ports</td>
</tr>
<tr>
<td>Source Port</td>
<td></td>
<td></td>
<td>TCP MSS</td>
</tr>
<tr>
<td>Client TCP Address</td>
<td>Identifies and returns the maximum segment size (MSS) in a TCP/IP packet.</td>
<td>Greater than</td>
<td>TCP MSS</td>
</tr>
<tr>
<td>MSS</td>
<td></td>
<td></td>
<td>TCP MSS</td>
</tr>
<tr>
<td>HTTP Request Header</td>
<td>Identifies the HTTP request data to determine if the data contains a specific header.</td>
<td>Contains, Exists, Not</td>
<td>Header Names, Header Value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>contains, Not exists</td>
<td></td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
<td>Operators</td>
<td>Values</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>HTTP Request</td>
<td>Identifies the HTTP request data to determine if the data contains a specific host name.</td>
<td>Contains, Equals, Startswith, Endswith, Not contains, Not equals, Not startswith, Not endswith</td>
<td>Hostname Values</td>
</tr>
<tr>
<td>Hostname</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP API Resource</td>
<td>Identifies the URL portion in an HTTP-based API request.</td>
<td>Equals, Not equals, Startwith</td>
<td>URL Path</td>
</tr>
<tr>
<td>Path</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. To add a default route, select a service from the Default Content route list. Click Add Default Content route. Requests that do match any condition are forwarded to this service.

You have completed the steps to create an endpoint. Select from one of the following options:

- Click **Next** to configure a load balancer, content rules, and security protection.
- Click **Deploy** to start application delivery.
Add an SSL certificate

Add an SSL certificate if you select the HTTPS protocol. You can add an SSL certificate in the endpoint workflow or using the SSL Certificate Manager. For more information about the SSL Certificate Manager, see Manage SSL certificates.

Add an SSL certificate while adding an endpoint

1. Click Add SSL Certificate.
2. In the Select SSL Certificates page, click Create SSL Certificate.
3. In the Create SSL Certificate page, type a certificate name.
4. Browse to the location of the certificate and key file on your computer.
5. If the key is encrypted, add a password.
6. To add the certificate in the certificate chain, select Add certificate in certificate chain.
7. Click Create.

Get an A+ rating from Qualys Labs

Perform the following actions to get an A+ rating from Qualys Labs for your applications.

1. Click Add SSL Policy.
2. In the Create SSL Policy page, type a name for the policy.
4. Click Create.

Configure client authentication or mutual TLS (mTLS)

In a typical SSL transaction, the client that is connecting to a server over a secure connection checks the validity of the server. To do so, it checks the server’s certificate before initiating the SSL transaction. Sometimes, however, you might want to configure the server to authenticate the client that is connecting to it.

With client authentication enabled, the CADS service asks for the client certificate during the SSL handshake. The service checks the certificate presented by the client for normal constraints, such as the issuer signature and expiration date.

If the certificate is valid, the service allows the client to access all secure resources. But if the certificate is invalid, the service drops the client request during the SSL handshake.

You can add an SSL certificate at the time of enabling client authentication, or select from an existing certificate in the certificate store.

1. Click Configure SSL Settings.
2. In the Select SSL Settings page, click Create.

3. In the Create SSL Policy page, select Client Authentication and click Create.

4. Select the SSL policy and click Add.

5. Add a CA certificate, and then click Create.
   
   **Note:** An SSL certificate is required if the HTTPS protocol is selected.
Configure authentication for the endpoints

April 25, 2022

Authentication provides security for a distributed internet environment by allowing any client with the proper credentials to connect securely to protected application servers from anywhere on the Internet.

The Citrix App Delivery and Security service supports SAML based authentication. Also, authentication is only supported for user defined FQDNs and HTTPS applications.

How it works

The SAML IdP (Identity Provider) is a SAML entity that is deployed on the public internet. The IdP receives requests from the SAML SP and redirects users to a logon page, where they must enter their credentials. The IdP authenticates these credentials with the active directory (external authentication server, such as LDAP) and then generates a SAML assertion that is sent to the SP. The SP validates the token, and the user is then granted access to the requested protected application.

Prerequisites

1. You have created an environment and a cloud access profile.
2. You have specified the basic details, such as the name of the application, environment, services, and endpoints by navigating to Applications > New Application. For more information, see Deliver a modern application.
3. You have configured the required services and endpoints.
4. You have set up the FQDN type to User defined and Protocol to HTTPS in the endpoint configuration.

To set up authentication for the endpoints (FQDNs/IP addresses)

1. Navigate to Applications > Authentication.
2. In the Deliver an Application page, click Create.
3. In the Create SAML Identity Provider page, specify values for the following parameters:
   - Name – Name for the SAML IdP.
   - Metadata URL – URL of the XML document that contains information about the SAML server.
   - Issuer Name – The name to be used in requests sent from Citrix ADS to IdP to uniquely identify Citrix ADS.
• **User field** – User name. SAML user ID, as provided in the SAML assertion.

4. Click **Create**. The IdP you created appears in the Authentication page.

**Note:**
You can add only one IdP per application.

**Bind a service to the IdP**

1. In the Deliver an Application page, select the preferred services in the **Services** list to bind to the IdP.
   You can bind the IdP to one or more services as per the requirement. If you select **Select All**, all the services that are available in the application are authenticated. This is the default option.
2. Select from one of the following options:
   - Click **Next** to configure content rules and security protection.
   - Click **Deploy** to start application delivery.

After you have enabled SAML authentication, only authenticated users are allowed to access specific services configured by the admin.

**Content Transform**

April 27, 2022

Do you want to take a specific action on HTTP requests based on the criteria, such as user location, header, and IP address?

Citrix App Delivery and Security Service – Citrix Managed enables you to respond to HTTP requests depending on the following criteria:

- Render a different page based on:
  - User’s geographical location.
  - Browser specification.
  - Languages the browser accepts.
  - Order of preference.

Content Transform also helps you to do the following:

- Drop the connection if the request is from an IP range that can be a suspected DDoS attack or hack attempt.
Citrix App Delivery and Security service

- Redirect traffic, respond with custom messages, or manipulate data on HTTP requests or responses.

- Remove unnecessary HTTP headers, mask internal URLs, redirect webpages, queries, or keywords.

Use content transform in the CADS service to examine the request from the client or response from the server and forward the request depending on the applicable rule. The content transform feature evaluates the data and applies one or more actions based on the evaluation.

Benefits

With content transform, you can do the following:

- Evaluate any part of the header or body of an HTTP or HTTPS request or response and take the configured action based on evaluation. The content transform enables you to configure more actions. For example, transforming the value of an HTTP header in the request or response.

- Redirect the request to a secure webpage. For example, while handling sensitive financial data, ensure that the client uses a secure connection to browse a site by redirecting the request to a secure connection. That is, use https:// instead of http://.

- Show a custom error page instead of the default 404 error page. For example, if you show the home page or site map of the website instead of an error page, the visitor remains on the site instead of moving away from the website.

- Append the default page name to the URL of a website. For example, if the default page of a company's website is http://www.abc.com/index.php, when the user types abc.com in the address bar of the browser, you can rewrite the URL to abc.com/index.php.

- Evaluate basic characteristics of traffic and data. For example, content transform can identify whether an HTTP request or response contains a particular type of header or URL. You can drop a connection or reset a connection at the request level based on the configured rule.

Prerequisites

1. You have created an environment and a cloud access profile.
2. You have specified the basic details, such as the name of the application, environment, services, and endpoints by navigating to Applications > New Application. For more information, see Deliver a modern application.

Types of content transform

Citrix App Delivery and Security service supports the following types of content transform:
Citrix App Delivery and Security service

- **Rewrite**
- **Responder**

You can select a condition for rewrite and responder. CADS service converts the condition into the rules and binds it to the application. CADS service acts based on the configured condition. For more information, see Create or Select a content transform section.

**Rewrite**

Rewrite refers to the rewriting of required information in the requests or responses handled by the CADS service. Rewriting can help in providing access to the requested content without exposing unwanted details about the website's actual configuration.

Rewrite rule is used to identify the HTTP data that you want to modify before serving. The rules are provided for modifying the data.

For example, you can modify the data to mask server information in a response for security purposes.

Actions are the steps CADS service takes, depending on the condition configured in the rule.

For example, if a condition in a rule matches a particular source IP address in a request, the action that is associated with this rule determines whether the connection is permitted.

**Rewrite action**

A rewrite action indicates changes made to a request or response prior to sending it to a server or client. The type of actions that the CADS service takes are feature specific.

For example, in rewrite, actions can replace text in a request.

In CADS service, actions are configurable. After enabling the rewrite feature, you need to configure one or more actions.

For example, you can add a local Client-IP header to incoming requests. If you want to insert the client IP from which a request is sent. The rewrite action inserts the HTTP header you specify into the HTTP request or response.

**Responder**

The responder helps in content filtering functions. The responder rule helps to select the requests to which the CADS service responds. The responder rule is associated with an action, which is performed if a request matches the rule.

Responder supports protocols such as TCP, DNS (UDP), and HTTP. With responder enabled in your application, server responses can be based on who sends the request, where it is sent from, and other criteria with security and system management implications.
Citrix App Delivery and Security service

For example, when users request a webpage, you can provide a different page based on the situation. You can drop the connection if the request is coming from an IP range that has been generating DDoS attacks or initiating hacking attempts.

**Responder action**

CADS service substitutes for and acts as a web server. You must configure one or more responder actions for handling requests. The responder action is used to manually define responses such as, simple HTML-based response, designated error response, and designated HTML page. For example, you can configure the text for a respond action with a web server error code and brief HTML page. You can configure a custom header for a respond action.

The responder redirects the request to a different webpage or web server. For example, A Redirect action can redirect requests originally sent to a “dummy” website that exists in DNS, to an actual website. It can also redirect search requests to an appropriate URL. The redirect action consists of a complete URL.

**Conditions**

Conditions evaluate the traffic based on the rules, settings, or string match operation that is defined in the rewrite and responder.

The following are the conditions and their corresponding operators and values:

- **HTTP headers:** A common method of evaluating the HTTP traffic is to examine the headers in a request or a response.

  A header performs the following functions:

  - Provide cookies that contain data about the sender.
  - Identify the type of data that is being transmitted.
  - Identify the route that the data has traveled (through header).

  - **Valid HTTP Request** - Identifies the validity of the incoming HTTP request.
  - **Valid HTTP Response** - Identifies the validity of the generated HTTP response.
  - **HTTP Request Method** - Identifies an element in the HTTP request or response by using a method in the HTTP request to evaluate HTTP request data.

    - Valid operators: **Equals, Not equals.**
    - Value: **GET, PUT, POST, DELETE.**
  - **HTTP Request Header** - Identifies the HTTP request data to determine if the data contains a specific header.
Valid operators: **Contains, Exists, Not contains, Not exists.**

Value: **Header Names, Header Value.**

- **HTTP Response Header** - Identifies the HTTP response data to determine if the data contains a specific header.
  
  Valid operators: **Contains, Exists, Not contains, Not exists.**
  
  Value: **Header Names, Header Value.**

- **HTTP Request Hostname** - Identifies the HTTP request data to determine if the data contains a specific host name.
  
  Valid operators: **Contains, Equals, Startswith, Endswith, Not contains, Not equals, Not startswith, Not endswith.**
  
  Value: **Hostname Values.**

- **HTTP Request URL** - Identifies an element in the URL portion of an HTTP request.
  
  Valid operators: **Contains, Equals, Startswith, Endswith, Not contains, Not equals, Not startswith, Not endswith.**
  
  Value: **URL Path.**

- **HTTP Request URL Query** - Identifies an element in the URL query of an HTTP request.
  
  Valid operators: **Contains, Equals, Startswith, Endswith, Not contains, Not equals, Not startswith, Not endswith.**
  
  Value: **URL Path.**

- **HTTP Request URL Suffix** - Identifies an element in the URL suffix of an HTTP request.
  
  Valid operators: **Contains, Equals, Startswith, Endswith, Not contains, Not equals, Not startswith, Not endswith.**
  
  Value: **URL Suffix Value.**

- **Client IP Address** - Identifies the client IP address. Identify and return a client IP address in a TCP/IP packet.
  
  Valid operators: **Between, Equals, Insubnet, Not between, Not equals, Not insubnet.**
  
  Value: **IP Addresses, Subnet IP Addresses, Range Start, Range End.**

- **HTTP Request Cookie** - Identifies the HTTP request based on its cookie. Identifies almost any type of information in a cookie header Returns the contents of the HTTP Cookie header.
  
  Valid operators: **Contains, Not contains.**
  
  Value: **Cookie Name, Cookie Value.**

- **HTTP Response Status Code** - Identifies the response status code from the server. Returns the response status code.
Valid operators: **Equals, Notequals, Between, Not between.**

**Value:** **Response Status Codes, Range Start, Range End.**

**Operators for HTTP Headers** – Operators represent actions that match text and HTTP header values with a collection of static strings in the value.

- **Equals** - An operation that evaluates whether the condition (target) matches the value (static strings).
- **Contains** - An operation that identifies if the string argument appears in any instance of the header value. Evaluates whether the target contains any of the strings that are bound to the value.
- **Startswith** - An operation that evaluates whether the target starts with any of the strings that are bound to the value.
- **Endswith** - An operation that evaluates whether the target ends with any of the strings that are bound to the value.
- **Exists** – An operation that evaluates if a request or response contains a particular object.
- **Between** – An operation that matches the individual strings and sets of strings with any portion of a header value. The header value can be an entire string, the start of a string, or any portion of text in between the start and the end of the string.
- **Not between** - An operation that evaluates the header value that can be an entire string, the start of a string, or any portion of text that is not between the start and the end of the string.
- **Is valid** - An operation that evaluates if a request or response is valid.
- **Ins subnet** - An operation that evaluates if a request or response is from a particular subnet.
- **Not ins subnet** - An operation that evaluates if a request or response is not from a particular subnet.
- **Not startswith** - An operation that evaluates whether the request or response does not start with any of the strings that are bound to the value.
- **Not endswith** - An operation that evaluates whether the request or response does not end with any of the strings that are bound to the value.
- **Not contains** - An operation that evaluates if the string argument appears in any instance of the header value. Evaluates whether the request or response contains any of the strings that are not bound to the value.
- **Not equals** - An operation that evaluates whether the request or response does not match the value.
- **Not exists** - An operation that evaluates if a request or response does not contain a particular object.

**Value** - Value is a parameter specific to an HTTP request or response. Evaluate specific data that the HTTP response or request contains.

- **GET** - Retrieves information from the server.
- **PUT** - Sends the data to a server to create/update a resource.
- **POST** - Submits an entity to the specified resource that causes a change in state or effects on the server.
- **DELETE** – Deletes a resource from the server.
- **Query Name** - Identifies a specific name that the HTTP request or response contains.
- **URL Path** - Identifies a specific segment of a URL that the HTTP request contains.
- **Query Value** - Identifies a specific value that the HTTP request or response contains.
- **URL Suffix Value** - Identifies a specific suffix value of a URL that the HTTP request contains.
- **Range End** - Option to set the highest value of its range.
- **Range Start** - Option to set the lowest value of its range.
- **Subnet IP Address** - Identifies the specific subnet address.
- **IP Address** - Identifies the specific IP address.
- **Header Names** - Identifies a specific header name.
- **HeaderValue** - Identifies a specific header value.
- **Hostname Values** - Identifies a specific host name value.
- **Response Status Code** - Identifies the status code generated by servers.
- **Cookie Values** - Identifies a specific cookie header that the HTTP request or response contains.
- **Cookie Name** - Identifies a specific cookie name that the HTTP request or response contains.

**Create or Select a content transform**

The content transform feature of the CADS service examines the request from the client or response from the server, performs action according to the specified rules, and forwards the traffic to the client or the server.

You can create a content transform or select the existing content transform for your service.

Follow these steps to create a content transform.

1. Navigate to **Applications > Content Transform**.
2. In the **Deliver an Application** page, click **Create**.
3. In the **Create Content Transform** page, type a name in **Content Transform Name**, create a rewrite rule or a responder rule and click **Create**.

Follow these steps to select an existing content transform.

1. Navigate to **Applications > Content Transform**.
2. In the **Deliver an Application** page, click **Select**.
3. In the **Select Content Transform** page, select the required content transform in the list by selecting the check box and click **Add**.
In a content transform you can create:

- A rewrite rule.
- A responder rule.
- Combination of rewrite and responder rules.

**Note:**
You can add only one content transform for an application.

### Add a rewrite rule

The rewrite feature helps you to rewrite the required information in the requests or responses handled by the CADS service.

Follow these steps to create a content transform using the rewrite:

1. In Create Content Transform page, select the Rewrite tab.
2. Click Add Rewrite Transform.
3. In the Add Rewrite Transform page, enter the following parameters:
   - **Rule Name** – Type a unique name for the rewrite rule. The unique name for the rewrite rule. Must begin with a letter, number, or the underscore character (_). Must contain only letters, numbers, and the hyphen (-), period (.), hash (#), at (@), equals (=), colon (:), and underscore characters.
   - **If the following condition is met** – Evaluates the traffic based on condition, settings, or string match operation. This tab corresponds to the rewrite rule. Only if the conditions are met, the rewrite actions are performed. For more information, see Types of content transform section.

Select the required condition and select or type the corresponding values and operators from the drop-down list. For more information on conditions, operators, and values, see Conditions section.

Click **AND Condition** to add more than one condition to the same rule, and configure the required parameters according to the required specification. To remove the added conditions, click the **Minimize** icon.

- **Then do the following** - If the condition is met, then the following configured rewrite actions should be done. For more information on rewrite action, see Types of content transform section. Select the required action and select or type the corresponding value fields such as header value, header name.
  - **Forward Client IP with header name X-Forwarded-For** - Forwards the HTTP header X-Forwarded-For in an HTTP request with the client's IP address as its value.
- **Forward Port with header name X-Forwarded-Port** - Forwards the HTTP header X-Forwarded-Port in an HTTP request with the client’s port as its value.

- **Forward Protocol with header name X-Forwarded-Proto** - Forwards the HTTP header X-Forwarded-Protocol in an HTTP request with the client’s protocol as its value.

- **Insert Custom HTTP Header in Request** - A rewrite action to insert a user defined custom HTTP header in a request.
  - Valid Fields: **Custom Header Name, Header Value**

- **Insert Custom HTTP Header in Response** - A rewrite action to insert a user defined custom HTTP Header in a response.
  - Valid Fields: **Custom Header Name, Header Value**

- **Replace an HTTP Header in Request** - A rewrite action to replace an HTTP header in a request.
  - Valid fields: **Header Name, Header Value**

- **Replace an HTTP Header in Response** - A rewrite action to replace an HTTP header in a response.
  - Valid fields: **Header Name, Header Value**

- **Remove an HTTP Header in Request** - A rewrite action to remove an HTTP header in a request.
  - Valid fields: **Header Name**

- **Remove an HTTP Header in Response** - A rewrite action to remove an HTTP header in a response.
  - Valid fields: **Header Name**

- **Custom Header Name** - A string, customized name for the HTTP request or response header.

- **Header Value** - Custom header string for HTTP request or response header. For example, for a header name “Strict-Transport-Security”, the value is “max-age=31536000”.

- **Header Name** - A string, name for the HTTP request or response header.

- **Replace request URL** - A rewrite action to replace the request URL with the specified URL. The CADS service enables you to convert the URL available in the client request to another URL that the backend server can understand. You can achieve the following benefits by using this rewrite feature:
  - Enhances the security by hiding the actual URL to the resource, which is requested by the client.
Citrix App Delivery and Security service

* Prevents the unauthorized user access from gaining access to the network resources.

* Valid fields: **Enter URL you like to replace**
  
  - **Enter URL you like to replace** - The URL that has to be replaced with the request URL. For example, you can change the URLs in the client request temporarily when the website is under maintenance. If the request URL is `http://www.example.com` in the web browser. You can configure the CADS service to replace the URL in the client request by giving the replacing URL input as `http://www.example.com/resource/inventory/s?t=112`.

When you select the required condition, the corresponding applicable actions are highlighted in the Rewrite Actions drop-down list, and the not applicable actions are grayed out.

1. In the **Add Rewrite Rule** page, after entering the required parameters, click **Add**.

   The rewrite rule is listed in the **Create Content Transform** page and displays the following information:

   - **Content Transform Name** - The content transform name is a unique name for the content transform. Must begin with a letter, number, or the underscore character (_). Must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

2. Click **Create**.

   The rewrite rule is listed in the **Deliver an Application** page.

   You have completed the steps to create a content transform using the rewrite.
Add a responder rule

The responder helps in content filtering functions. CADS service examines the request from the client, takes action according to the applicable responder rule, sends the response to the client, and closes the connection with the client.

Follow these steps to create a content transform using the responder:

1. In the Create Content Transform page, select the Responder tab.
2. Click Add Responder Rule.
3. In the Add Responder Rule page, enter the following parameters:

   - **Rule Name** – Type a unique name for the responder rule. The unique name for the responder rule. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

   - **If the following condition is met** – Evaluates the traffic based on condition, settings, or string match operation. This tab corresponds to the rewrite rule. Only if the conditions are met, the rewrite actions are performed. For more information, see Types of content transform section.

   Select the required condition and select or type the corresponding values and operators from the drop-down list. For more information on conditions, operators, and values, see Conditions section.

   Click **AND Condition** to add more than one condition to the same rule, and configure the required parameters according to the required specification. To remove the added conditions, click the **Minimize** icon.

   **Note:**

   HTTP Response Header is not applicable to the responder rule.

   - **Then do the following** - If the condition is met, then the following configured rewrite actions are done. For more information on rewrite action, see Types of content transform section. Select the required action and select or type the corresponding value fields such as header value, header name.

     - **Redirect to URL** - Modify a URL to redirect traffic from URL A to URL B.

       - Valid fields - **URL value**.

       The **URL value** can be an absolute value or a relative value. For example, https://www.example.com, modifies the server to which the request is redirected. /index.html, redirects the request to the resource index.html on the existing server that is configured.
– **Drop the request** - Drop a connection based on the HTTP request-based parameter.

– **Reset the request** - Reset a connection based on the HTTP request or response parameter.

– **Respond with Error** - Sends the chosen error response.
  
  * Valid Fields: **Choose the Error**. You can choose **DEFAULT** or **CUSTOM**.
  * If you choose **DEFAULT** error, valid fields: **Custom Error Message**.
  * If you choose **CUSTOM** error, valid fields: **Error Code**, **Custom Error Message**.

– **Choose an Error** - Select the error codes provided in the drop-down list to respond with that error code. You can select from the list of **DEFAULT** errors or select **CUSTOM** to provide a custom error.
  
  * **Error Code** - Provide an appropriate error code for your custom error.
  * **Custom Error Message** - Send the custom error message by providing an appropriate error message.

– **Respond with an HTML page** - Choose an HTML file to respond with a custom message. You can upload the required HTML page. Use this type of action to send the desired HTML page as the response.
  
  * **HTML File** - You can upload an HTML page with a custom message during responder run time. Click **Upload File** to choose the required HTML file.

When you select the required condition, the corresponding applicable actions are highlighted in the **Responder Actions** drop-down list and the not applicable actions are grayed out.

1. In the **Add Responder Rule** page, after entering the required parameters, click **Add**.

   The responder rule is listed in the **Create Content Transform** page and displays the following information:

   - **Content Transform Name** - The content transform name is a unique name for the content transform. Must begin with a letter, number, or the underscore character (_). Must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.
2. In the **Create Content Transform** page, click **Create**.

The responder rule is listed in the **Deliver and Application** page. You have completed the steps to create a content transform using the responder.

**Bind a service**

CADS service enables you to bind the required services to the content transform.

- In the **Deliver an Application** page, select the preferred services in the **SERVICES** drop-down list by selecting the check box.

You can view the selected services in the drop-down list under the **Services** tab.

Click **Next** to configure the **Security Protection** feature. Otherwise, click **Deploy**.
Edit a content transform

You can edit the characteristics of an HTTP request or response of a content transform such as host name, URL. You can modify the conditions, actions, and corresponding fields.

The Deliver an Application page lists the created content transform with the following details:

- **NAME** - Unique name of the content transform.
- **RULES** - The rule enables the CADS service to evaluate a piece of traffic or data. For example, a rule can enable the CADS service to determine whether an HTTP request originated from a particular IP address.
- **SERVICES** - Denotes the services that are associated with the configured content transform.
- **ACTIONS** - Denotes the edit and delete action that is configured for that specific content transform.

Follow these steps to edit a content transform:

1. In the Deliver an Application page, click Select.

   The Select Content Transform page lists the following details:

   - **NAME** - Unique name of the content transform.
   - **RULES** - The rule enables the CADS service to evaluate a piece of traffic or data. For example, a rule can enable the CADS service to determine whether an HTTP request originated from a particular IP address.
   - **ACTIONS** - Denotes the Edit and Delete actions.

1. Click the Edit icon in the Actions column.

2. In the Update Content Transform-<rule name> page, click the Edit icon.

   You can enable or disable the rewrite rule (in the Rewrite tab) or the responder rule (in the
Responder tab) by toggling the STATUS field.
3. Click Update to save the updates.

Edit a rewrite rule

1. In the Update Content Transform- <rule name> page, Rewrite tab, select the required rewrite rule. Click the Edit icon to edit the rewrite condition and rewrite action.
2. In the Add Rewrite Rule page, modify the required condition, rewrite action, and corresponding fields.
3. Click Update to save the updates.
4. Click Update in the Update Content Transform- <rule name> page.

Edit a responder rule

1. In the Update Content Transform - <rule name> page, Responder tab, select the required responder rule. Click the Edit icon to edit the responder condition and responder action.
2. In the Add Responder Rule, modify the required condition, responder action, and corresponding fields.
3. Click Update to save the updates.
4. Click Update in the Update Content Transform- <rule name> page.
Delete a content transform

Follow these steps to delete a content transform:

1. Select the required content transform in the Deliver an Application page, and then click the Delete icon in the Actions column.

2. Click Remove.

   The selected content transform is removed from the application.

In the Select Content Transform page, click the Delete icon under the ACTIONS column to delete the content transform.
Delete a rewrite rule

1. In the Update Content Transform - `<rule name>` page, select the required rewrite rule in the Rewrite tab and click the Delete icon in the Actions column.
2. Click Yes, Delete.
   Verify that the rewrite rule is removed from the list.

Delete a responder rule

1. In the Update Content Transform - `<rule name>` page, select the required responder rule in the Responder tab and click the Delete icon in the Actions column.
2. Click Yes, Delete.
   Verify that the responder rule is removed from the list.
Add security protection

July 26, 2022

CADS edition, provides an intent-based security protection for your web applications and APIs from OWASP Top-10 attacks and exploits. With CADS security protection, you can define your desired business intent without having to understand the complexities of OWASP Top-10, network, policies, and other application security configuration that the traffic passes through. In addition to the web application firewall and bot management, the service also provides visibility into security insights that provide real-time monitoring of traffic violations and vulnerabilities.

Benefits

1. Automatically assigns the business intent to security policies.
2. Translates high-level security requests into relevant configuration changes.
3. Simplify deployment and management of security for applications.
4. Get valuable insights and visibility into security events and automate remediation actions.
5. Get continuous protection with auto-update of WAF or bot signature and IP reputation feed.

Prerequisites

Complete the following prerequisites before you add security protection to your application. By default, security protection is disabled.

1. Sign up for Citrix Cloud.
2. Request for Citrix App Delivery and Security Service – Citrix Managed entitlement.
3. Set up application environment.

For more information, see Get started with Citrix App Delivery and Security service topic.

How Citrix App Delivery and Security Service – Citrix Managed security protection works

The Citrix App Delivery and Security Service – Citrix Managed security protection has a collection of security checks that protect your application from malicious attacks, software vulnerabilities, SQL database vulnerabilities, errors in the code design, and failures to secure websites that host or can access sensitive information. You can enable and configure security checks to protect your application from various security attacks.
**Security check**

A security check is a check that inspects malicious or unknown attacks on your web applications. The security check use heuristics, positive security, and other detection techniques to identify attacks. You can configure a security check by first enabling it and then configuring it to block requests, log request details, add exceptions, or define rules to examine traffic.

The CADS security checks are classified into the following categories:

- **Basic security check.** Web security protection applicable to any content type.
- **HTML security check.** Web security protection applicable only to HTML-based websites and to HTML portions of Web 2.0 sites that contain both HTML and XML content.
- **JSON security check.** Web security protection applicable only to JSON-based websites and to JSON content type in Web 2.0 sites.

**Signatures**

Signatures are configurable rules to simplify the task of protecting your websites from attacks. A signature represents a pattern of a component attack on an operating system, web server, website, or other resources.

The CADS Security Protection has a built-in default signature object consisting of more than 1,300 signature rules. The CADS Security Protection and Bot signatures can be customized by adding new rules. A signature rule can have multiple patterns and can flag a violation only when all the patterns are matched to avoid false positives.

**Actions**

All security checks have a set of configurable actions which control how CADS Security Protection can handle a request or response.

- **Block action**
  The block action prevents vulnerabilities from attacking your application. By default, security checks have the block action disabled. You must enable if you want to block a request that contains a malicious attack. If block action is not enabled, the CADS service only logs the request data.

- **Log action**
  The log action enables you to collect request details that have a malicious attack. The log details can be further investigated for monitoring and analytics purposes. When you enable a security check that the log-only action is auto-enabled for the feature.
Exception (rule)

For security check, an exception is a rule written to allow access to specific data and block the rest. Exceptions are applicable only for a few security checks such as SQL injection, cross-site scripting, Cross-Site Request Forgery (CSRF), Field Consistency, and Cookie Consistency. These rules are written to bypass security validation for false-positive scenarios.

You can configure an exception to bypass security checks for legitimate requests. A security check is performed on the incoming traffic payload and malicious requests, patterns are identified even if they are spread across multiple lines. When examining the traffic, you can apply exceptions to bypass the security check for the following criteria:

- Incoming traffic with SQL injection attacks that are malicious.
- Incoming traffic with cross-site scripting attacks that are vulnerable to your web applications.
- Incoming traffic with cookie consistency attacks to gain access to a legitimate session of the target user.
- Incoming traffic with field consistency attacks that send unauthorized web from data.
- Incoming traffic with CSRF attacks induces a user to perform actions that are not intended to perform.

The ADS security protection not only enables you to create an exception but also manages exceptions for the security check through the ADS GUI or API interface.

Example use case 1: Exception for Cross-Site Scripting protection:

Consider a form field `dpasswd` in the URL, `https://adcsvc.example.com/login.php` not prone to cross site scripting. The corresponding field can be exempted from the cross-site scripting protection. To configure this exception, you can add a rule in which the URL pattern must be defined as `https://adcsvc.example.com/login.php(regex)`, field type must be `Form Field`, and form field name must be `"^dpasswd\$(regex)"`.

<table>
<thead>
<tr>
<th>Sample payload</th>
<th>URL</th>
<th>Field type</th>
<th>Form field</th>
</tr>
</thead>
</table>

Example use case 2: Exception for cookie consistency validation:

False positives occur when a cookie mismatch is incorrectly flagged as a vulnerability by a scanning
Citrix App Delivery and Security service

tool. To handle such scenarios, you can add an exception for the header cookie that can be exempted from cookie validation. Consider a client sending a login request to the server. On successful login, the server response includes the set-header cookie that contains the JSESSIONID and its value.

```
1  Set-Cookie: JSESSIONID=abc123; Path=/; HttpOnly
2  <!--NeedCopy-->  
```

The client sends the cookie ID in its subsequent request to the server. To handle a false positive or legitimate request, you can add an exception to bypass cookie validation for JSESSIONID for any request coming from the client.

**Conditions**

Conditions are characteristics that you want to examine in an incoming request. Following are some conditions for which a Citrix App Delivery and Security Service – Citrix Managed evaluates the traffic.

1. Malicious scripts embedded in a request.
2. IP addresses or address ranges that requests originate from.
3. Country or geographical location that requests originate from.
4. Length of a specified portion of the request, such as the query string.

**Get started with CADS service security checks**

The CADS service security protection features are classified into three categories, General, WAF, and Bot.

**General**

- **Allow and block list**—Inspects the incoming traffic with rules defined to Allow or Block a client’s access to web application resources, based on parameters such as IP address, subnet, or HTTP request headers.
- **Geo blocking**—Restricts unauthorized access based on user’s geographical location.
- **IP reputation**—Blocks traffic coming from an IP address with a bad reputation score
- **Rate Limit**—Limits the amount of network traffic. For example, if the feature limits the number of incoming requests to 100, then more requests to the web application are blocked. Rate limiting controls traffic flow based on client IP address, client subnet, URL, or URL pattern, and HTTP headers.
Citrix App Delivery and Security service

WAF

- **SQL injection**—Examines HTTP or HTTPS requests and blocks HTML-based, and JSON-based SQL attacks that can affect your web applications.
- **Buffer overflow**—Examines if an incoming traffic can cause a buffer overflow on the web server. If the service detects a URL, a cookie, or a header longer than the specified maximum length in a request, it blocks a JSON-based request or HTML based requests to prevent a buffer overflow attack.
- **Cookie Consistency**—Examines the cookie sent by the browser and blocks the request if the cookie does not match the cookie in the web application. To resolve a false positive and bypass the security check, you can add an exception.
- **Cross-site scripting**—Examines if an attacker inserts malicious code into an incoming request that can have huge implications, such as compromising website security or user authentication. To resolve a false positive and bypass the security check, you can add an exception.
- **Command Injection**—Examines if an incoming request has any vulnerable commands. To resolve a false positive and bypass the security check, you can add an exception.
- **CSRF**—Inspect HTTP or HTTPS requests and blocks HTML-based, or JSON-based CSRF attacks that can affect your web applications.
- **Field Consistency**—Examines web forms returned by users for your application and verifies that web forms were not modified inappropriately by the client. The security check is only for HTML requests that contain a web form, with or without data.
- **WAF Signatures**—A list of signature rules is available under different categories to protect your web application against security attacks. The Citrix ADC security protection examines the traffic and blocks the request if it matches a signature pattern. By default, all signatures are enabled.
- **HTTP Security Headers**—HTTP response headers can be used to prevent security attacks on the web application by controlling the browser behavior during application access.
- **Data Leak Prevention**—Identifies if the responses coming from the webserver contain any user-specific sensitive information. When a match is found, the CADS service takes the configured action to avoid leakage of such information.

Bot

- **Bot Signatures**—A list of bot signature rules is available under different categories to protect your web application against security attacks. The Citrix ADC security protection examines the traffic and blocks the request if it matches a signature pattern. By default, all bot signatures are enabled.

Before you enable a security check, you must create a security protection profile or use an existing security profile.
Add a security protection profile

If you already have a security protection profile, you can select and add the profile for your application, otherwise you can create a profile.

Complete the following steps to add a security protection by using the GUI:

1. Navigate to **Applications > New Application > Security Protection**.
2. Click **Select**.
3. In the **Add Security Protection** slide, select a security protection profile and click **Add**.
4. The profile is added to security protection summary table.
5. Select and bind the profile to a service.

**Note:**

You can add only one security profile to an application service.
The security protection profile is now added to the application before it is ready to be deployed in the cloud. If you do not see an existing profile in the list, you can create a one.

**Create a security protection profile**

As a first-time user, you can create a profile for your application. Complete the following steps by using the GUI.

1. Navigate to **Applications > New Application > Security Protection.**
2. Click **Create**.
3. In the **Create Security Protection** page, enter a name and configure one or more of the following security features:
   a) Allow and Block list
   b) Geo Blocking
   c) IP Reputation
   d) Rate Limit
   e) SQL Injection
   f) Buffer overflow
   g) Cross-site scripting
   h) Cookie Consistency
   i) CSRF
   j) Field consistency
   k) Signatures
   l) HTTP Security Headers
   m) Data Leak Prevention
   n) Bot signatures
1. Click **Create**.

   You can view the newly created security protection profile.

2. Select and bind the profile to a service.

   **Note:**

   You can add only one security profile to an application.
The profile is added to your application.

**Edit a security protection profile**

If you already have a security protection profile and you prefer to update its details, you can use the edit functionality.

Complete the following steps to update a security protection profile by using the GUI:

1. Navigate to Applications > Security Protection.
2. Click Select.
3. In the Add Security Protection slide, select a security protection profile and click the pencil icon to update.
4. In the Update Security Protection page, modify details and click Update.
5. The Add Security Protection page displays the updated profile.
6. Select the profile and click Add.
7. The profile is added to security protection summary table.
8. Select and bind the profile to a service.
Allow and block list

The Allow and block list functionality enables you to create a security rule to allow or block requests based on user parameters such as IP address, subnet address, or HTTP header.

Allow list. A rule that allows user requests to access internal resources if all conditions configured for the rule match the request.

Block list. A rule that blocks user request to internal resources if all conditions configured for the rule match the request.

Enable allow and block list protection

Before you create a security rule, as a first step, you must enable the security check toggle. If you disable the toggle, the Citrix App Delivery and Security Service – Citrix Managed does not inspect the traffic.
Create a rule

As a first-time user, if you do not see a security rule for allow or block list, you can create one. Complete the following steps to create a rule by using the GUI.

1. Navigate to Applications > Security Protection.
2. In the Create > Allow and Block list tab page, enable the Enable Allow and Block list protection toggle and click Add Rule.
3. In the Allow and Block list page, set the following parameters:
   a) Rule name. Name of the rule for an allow list or a block list.
   b) If the following conditions are met. The conditions to define based on user parameters such as IP address, subnet address, or HTTP header. You can add multiple conditions for a rule using either AND Condition or OR Condition. A combination of AND Condition and OR Condition is not supported. The Citrix App Delivery and Security Service – Citrix Managed security evaluates traffic based on the conditions that you define.
      i. HTTP Request Method. Request method for create, read, update, or delete operations.
         A. Operator. Logical condition to evaluate the HTTP request method.
         B. Value. HTTP request method operation.
      ii. HTTP Request Header. Header used in an HTTP request to provide information about the request.
         A. Operator. Logical condition to evaluate the value of specific headers.
         B. Name. Name of the HTTP request header field.
         C. Value. Request header field value.
      iii. HTTP Request host name. HTTP host header that has the host name of the client request.
         A. Operator. Logical condition to evaluate the request host name.
         B. Value. Host name value.
      iv. HTTP Request URL. HTTP request made by a client to a named host located on the back-end server.
A. Operator. Logical condition to evaluate the request URL.
B. Path. Request URL path.

v. IP Allow and Block list.
   A. Operator. Logical condition to evaluate the IP address of the client request.
   B. Value. IP address or subnet address.

c) Then do the following Action. Action to apply based on evaluation. Action types are as follows:
   i. Allow. Allow user request to access internal resources.
   ii. Drop. Drop user request without sending a response.
   iii. Reset. Reset client connection by closing it.

d) Click Add Rule.

You can view the newly created rule on the Create new Security Protection page.
Click the pencil icon to modify rule details.

**Edit an allow or block rule**

Complete the following steps to update a rule by using the GUI:

1. Navigate to **Applications > Security Protection**.
2. Click **Add Security Protection**.
3. In the **Add Security Protection** slide, select a rule and click the pencil icon to edit.
4. In the **Allow and Block list** page, edit details and click **Update Rule**.
5. You can view the updated rule on the **Create Security Protection** page.

**Geo blocking**

The geo blocking security check enables you to allow or block requests based on a geographical location from where the request originates from. The filter works based on a geo match condition that has a list of countries in an allow list and a block list. If a request matches a geo match condition, then the request is either allowed or blocked based on the location the request originates from.

**Enable geo blocking protection**

Before you configure geo-blocking, you must enable the security check. When disabled, the Citrix App Delivery and Security Service – Citrix Managed does not allow, or block requests based on the client's geo location.

**Classify geo locations**

Complete the following steps to classify geo locations under an allowed or blocked country list:

1. Navigate to **Applications > Security Protection > Create > Geo Blocking**.
2. In the **Geo Blocking** tab section, classify countries under allowed list and blocked list.
**IP reputation**

IP reputation security check blocks unwanted requests coming from an IP address that has a bad reputation score. The security check enables you to classify IP address threat categories as an allowed list and blocked list. If a request matches a condition, the request is either allowed or blocked based on its IP address and its threat category. Some of the key threat categories are spam sources, Windows exploits, botnets, scanners, and so forth.

**Enable IP reputation protection**

Enable the IP reputation security check to examine traffic for the IP reputation. When disabled, the Citrix App Delivery and Security Service – Citrix Managed does not inspect the traffic for its IP address and threat category.

**Classify IP address threat category**

Complete the following steps to classify the threat categories as an allowed list or a block list:

1. Navigate to **Applications > Security Protection > Create > IP Reputation**.
2. In the **IP Reputation** tab section, classify the threat categories under allowed list and blocked list.

![IP Reputation](Image)

**Rate limit**

The Rate Limit security check limits network traffic and protects your application from security vulnerabilities and bot attacks. The filter limits traffic by restricting the number of user requests that an
Citrix App Delivery and Security service

application can receive within a timeframe.

The filter uses a rate limit condition that measures the number of requests received within a timeframe. If there are too many requests within a timeframe, the check blocks requests exceed the threshold limit. By doing this, the Citrix App Delivery and Security Service – Citrix Managed protects your application from excess traffic.

**Example use case: Rate limiting requests per URL for a ticket booking website**

Consider a ticket booking website www.adcsvc.example.com that receives huge traffic every 2 minutes. To limit traffic to the website, you can limit the number of requests per URL to 200 for 120 seconds. If there are more than 200 requests received per URL within 120 seconds, then the rate limit security check validation fails, and the check blocks the excess requests per URL.

**Enable rate limit protection**

Before you configure the rate limit policy you must enable the security check. When disabled, the CADS service does not rate limit traffic to your application.

**Configure rate limit policy**

Complete the following steps to configure the rate limit policy for enhanced application security.

1. Navigate to *Applications > Security Protection > Create > Rate Limit*.
2. In the *Rate Limit* tab section, click *New Policy*.
3. In the *Configure Rate Limit Policy* page, set the following parameters:
   a) Policy Name. Name of the rate limit policy.
   b) Limit Requests. Logical condition to rate limit traffic.
      i. Server
         A. For overall app. Logical condition to rate limit traffic on the server-side.
         B. Per URL. Logical condition to rate-limit traffic if it matches the pre-defined URL on the server-side.
         C. Per URL matching the pattern. Logical condition to rate-limit traffic only if the incoming request URL exactly matches the pre-defined URL on the server-side.
         D. Matching the URL pattern. Logical condition to rate-limit traffic only if the incoming request URL matches the URL syntax pattern on the server-side.
      ii. Client
         A. Per client IP. Logical condition to rate limit traffic based on client IP address.
         B. Per client matching the following client pattern. Logical condition to rate-limit traffic if the response URL matches the predefined URL on the client side.
C. Matching the client pattern. Logical condition to rate-limit traffic if the response URL matches the predefined client or subnet address.

D. Per client identified by a specified HTTP header. Logical condition to rate-limit traffic per client identified by a specific HTTP header.

E. Per client identified by values in an HTTP header. Logical condition to rate-limit traffic per client identified by a specific HTTP header value.

F. Per client identified by a cookie. Logical condition to rate-limit traffic per client identified by a cookie.

G. Per client identified by a user agent. Logical condition to rate-limit traffic per client identified by a user agent.

iii. Server and Client

A. Per client matching the specific URL. Logical condition to rate-limit traffic per client matching exactly the URL.

c) Maximum requests. Maximum number of requests that is allowed within a time frame.

d) Timeframe. Maximum time (in seconds) to rate limit traffic.

e) Subsequent requests are. Action to apply.

f) Status. Enable or disable rate limit policy configuration.

4. Click Add Policy.

You can view the policy in the Rate Limit summary section.
SQL injection

The SQL injection filter examines the incoming request for SQL Injection attacks. If an SQL attack is detected in the payloads, the security check blocks the request. Use the SQL protection check to secure your web application and prevent SQL injection attacks.

Enable SQL injection protection

Before you configure the SQL injection exception, you must first enable security protection for HTML or JSON content type requests. When disabled, the CADS service does not inspect the traffic for SQL injection attacks. Also, you must toggle the Block action to block requests that contain malicious SQL attacks. When the block action is not selected, CADS service only logs the data.

Intent based auto blocking

The **Block clients with 20 violations within 30 minutes** option allows you to define the intent of auto blocking malicious clients that are attempting SQL injection attacks.

If the number of requests violating the security check received from a client increases to 20 or more in a 30-minute duration, the client is considered malicious. Select **Block clients with 20 violations within 30 minutes** to block such clients for a 30-minute duration.
Create an SQL injection exception

An SQL injection attack can occur in several parts of a request. The variants of an SQL injection attack are:

- **Form fields.** A basic SQL injection attack can be through a login page where the user provides input. The web application accepts inputs through the page, which pass the user input to the database for processing. If the web application accepts inputs without sanitizing them, an attacker can inject SQL statements through the form fields that can delete, copy, or modify contents in the database.

- **Header.** Server variables such HTTP headers can also be vulnerable for SQL injection. If a web application accepts inputs from HTTP headers, fake headers containing arbitrary SQL can inject code into the database.

- **Cookie.** Cookies are another vulnerability for SQL injection. This is done by modifying cookies to affect the database queries. Web applications often load cookies and use the data for database operations. A malicious user, or malware deployed on a user’s device, can modify cookies, to inject SQL in an unexpected way into the back-end database.

To avoid false positives and bypass a security check, you can add an SQL injection exception for form fields, header, or cookie values.

Complete the following steps to add an exception.

1. Navigate to **Security Protection > SQL Injection > New exception.**
2. Set the following parameters to add an exception for SQL injection protection:
   - a) URL Pattern. The URL for which the exception is required. It can be a regular expression. For any URL enter ‘.*’.
   - b) Field type. The field type for which the exception is required.
   - c) Form field names. The form field in which the exception is required. It can be a regular expression.
   - d) Status. Enable or disable the SQL injection exception.
3. Click **Add Exception.**
You can view the exception on the **SQL Injection** tab section.

**Edit an SQL injection exception**

Complete the following steps to update an SQL injection exception:
1. Navigate to Applications > Security Protection > SQL Injection.
2. In the SQL Injection tab section, select an exception and click the pencil icon to edit.
3. In the Configure SQL injection exception page, edit details and click Update Exception.
4. You can view the updated exception in the SQL Injection summary section.
5. Click Update Security Protection.

Buffer overflow

The buffer overflow security check detects if your application receives more input than expected that can cause a buffer overflow on the application server. For example, let us consider the origin server is set to handle a URL length of maximum of 500 characters but if an incoming URL length is 700 characters, the buffer overflow security check validation fails, and it blocks the request.

To prevent buffer overflows, the Citrix App Delivery and Security Service – Citrix Managed security check enables you to set the maximum length for request parameters such as URL, cookie, or header value. If the input value for these parameters is longer than the profiled length, then the check blocks the request because it can cause an overflow.

Enable buffer overflow protection

Before you configure the buffer overflow limit, you must enable the security check. When disabled, the Citrix App Delivery and Security Service – Citrix Managed does not inspect the traffic for buffer overflows. Also, you must enable the Block toggle to block requests that can cause a buffer overflow.

When the block toggle is not selected, the Citrix App Delivery and Security Service – Citrix Managed only logs the data.

Configure buffer overflow limit

You can prevent the buffer overflow vulnerability by configuring the maximum length for parameters such as URL, cookie, or header length.

1. Navigate to Applications > Security Protection > Create > Buffer Overflow.
2. In the Buffer Overflow tab section, set the following parameters:
   a) Maximum Container Depth. Enter the maximum allowed nested depth for a JSON element. Requests with container depth greater than the configured value are blocked. Default: 5, minLength: 0, maxLength: 127.
   b) Maximum Document Length. Enter the maximum allowed document length in a JSON request. Requests with document size greater than the configured value are blocked. Default: 20000000, minLength: 0, maxLength: 2147483647.
c) Maximum Object Key Count. Enter the maximum allowed object key count in a JSON request. Requests with object key count greater than the configured value are blocked. Default: 10000, minLength: 0, maxLength: 2147483647.

d) Maximum Object Key Length. Enter the maximum allowed length for an object key in a JSON request. Requests with object keys of length greater than the configured value are blocked. Default: 128, minLength: 0, maxLength: 2147483647.

e) Maximum Array Length. Enter the maximum length for an array in a JSON request. Requests with array length greater than the configured value are blocked. Default: 10000, minLength: 0, maxLength: 2147483647.

f) Maximum String Length. Enter the maximum allowed length for a string in a JSON request. Requests with json string length greater than the configured value are blocked. Default: 1000000, minLength: 0, maxLength: 2147483647.

---

**Cookie consistency**

The cookie consistency filter examines if the cookie returned by the user matches the cookies set by the website. If a modified value is found, the cookie is stripped from the request before forwarding it to the application server.

**Enable cookie consistency**

Before configuring the cookie consistency security check, you must first enable the feature. When disabled, CADS does not inspect the traffic for cookie consistency attacks. Also, you must toggle the Block action to block requests that contain malicious SQL attacks. If the block action is not selected, CADS only logs the data.
Create a cookie consistency exception

You can create an exception to prevent blocking legitimate requests or resolve false positives and bypass the security check. Complete the following steps to add an exception.

1. Navigate to Applications > Security Protection > Cookie consistency > Manage Cookie Consistency.

2. Set the following parameters to add an exception for cookie consistency:
   a) Cookie Name. Name of the cookie set by the server.
   b) Status. Enable or disable cookie consistency exception.

3. Click Add Exception.
You can view the exception in the cookie consistency summary section.

**Edit a cookie consistency exception**

Complete the following steps to update a cookie consistency exception:

1. Navigate to **Applications > Security Protection > Cookie Consistency**.
2. In the **Cookie Consistency** tab section, select an exception and click the pencil icon to edit.
3. In the **Manage Cookie Consistency** page, edit details and click **Update Exception**.
4. You can view the updated exception on the **Cookie Consistency** tab section.

**Cross-site Scripting**

In a Cross-Site Scripting (cross-site scripting) attack, an attacker inserts malicious code into an incoming request that can have huge implications, such as compromising website security or user authentication. Use the cross-site scripting feature to secure your web application and prevent cross-site scripting attacks.

**Enable Cross-site Scripting protection**

Before you configure the Cross-site Scripting exception, you must first enable the security check for HTML or JSON content type requests. When disabled, the CADS service does not inspect the traffic. Also, you must enable the Block toggle to block requests that contain malicious Cross-site scripting attacks. When the block is not selected, CADS service only logs the data.

**Intent based auto blocking**

The **Block clients with 20 violations within 30 minutes** option allows you to define the intent of auto blocking malicious clients that are attempting cross-site scripting attacks.

If the number of requests violating the security check received from a client increases to 20 or more in a 30-minute duration, the client is considered malicious. Select **Block clients with 20 violations within 30 minutes** to block such clients for a 30-minute duration.

**Create a Cross-site Scripting exception**

You can add a Cross-site Scripting exception for form field, header, and cookie values to prevent blocking legitimate requests or resolve false positives, and bypass the security check. Complete the following steps to add an exception.

1. Navigate to **Security Protection > Cross-site Scripting > New exception**.
2. Set the following parameters to add the cross-site scripting exception:
a) URL Pattern. The URL for which the exception is required. It can be a regular expression.
   For any URL enter `. *`.

b) Field type. The field type for which the exception is required.

c) Form field names. The form field in which the exception is required. It can be a regular
   expression.

d) Status. Enable or disable the cross-site scripting exception.

3. Click **Add Exception**.

You can view the exception on the cross-site scripting summary section.
Edit a Cross-site scripting exception

Complete the following steps to update a Cross-site scripting exception:

1. Navigate to **Applications > Security Protection**.
2. Click **Add Security Protection**.
3. In the **Add Security Protection slide**, select an exception and click the pencil icon to edit.
4. In the **Configure Cross-site Scripting Exception** page, edit details and click **Update Exception**.
5. You can view the updated exception on the **Create new Security Protection** page.

Command Injection

The command injection security check examines if an incoming request has unauthorized commands that can break the system security or modify the system. If the request has malicious commands, the CADS service blocks the request.

Enable command injection

Before configuring the command injection security check, enable the feature for HTML and JSON content type requests. When disabled, CADS service does not inspect the traffic for command injection attacks. Also, you must toggle the Block action to block requests that contain unauthorized command attacks. If the block action is not selected, CADS service only logs the data.
Create a command injection exception

You can add an exception for legitimate requests or resolve false positives, and bypass command injection check. Complete the following steps to add an exception.

1. Navigate to **Security Protection > Command Injection > New exception**.

2. Set the following parameters to add a command injection exception:
   a) Exception type. Select a content type to add an exception for command injection check.
   b) URL Pattern. The URL for which the exception is required. Only for JSON content type, the URL is applicable. It can be a regular expression. For any URL enter ‘. *’. 
   c) Field Type. Vulnerable field that can be excluded from security check input validation.
      i. Form Field. If the vulnerable field type is selected as form field, then enter the field name.
      ii. Header. If the vulnerable field type is selected as header, then enter the header name.
      iii. Cookie. If the vulnerable field type is selected as cookie, then enter the cookie name.
   d) Status. Toggle command injection exception status.

3. Click **Add Exception**.
You can view the exception in the command injection summary section.

Configure Command Injection Exception

- **Exception Type**: HTML
- **URL Pattern**: /login.index.html
- **Field Type**: Form Field
- **Form Field Name**: password
- **Status**: On

Add Exception  Cancel
**Edit a command injection exception**

Complete the following steps to update a command injection exception:

1. Navigate to **Applications > Security Protection**.
2. Click **Add Security Protection**.
3. In the **Add Security Protection** slide, select an exception and click the pencil icon to edit.
4. In the **Configure command injection exception** page, edit details, and click **Update Exception**.
5. You can view the updated exception on the **Command Injection** tab page.

**Cross Site Request Forgery (CSRF)**

The Cross Site Request Forgery (CSRF) security check tags each web form sent by a protected website to users with a unique and unpredictable Form ID. When there is an incoming request from the user, the security filter examines the web form to ensure that the supplied Form ID is correct. The security check is applicable only to HTML requests that contain a web form, with or without data.

**Enable CSRF**

Before configuring the CSRF security check, you must first enable the feature. When disabled, CADS does not inspect the traffic for CSRF attacks. Also, you must toggle the Block action to block requests that contain malicious CSRF attacks. If the block action is not selected, CADS only logs the data.

**Create a CSRF exception**

You can create a CSRF exception to prevent blocking legitimate requests or resolve false positives and bypass the security check. Complete the following steps to add an exception.

1. Navigate to **Applications > Create > CSRF > New Exception**.
2. Set the following parameters to add an exception for CSRF:
   a) **URL Pattern.** The URL for which the exception is required. It can be a regular expression. For any URL enter ‘*’.
   b) **Status.** Toggle command injection exception status.
3. Click **Add Exception**.
Edit a CSRF exception

Complete the following steps to update a CSRF exception:

1. Navigate to Applications > Create > CSRF.
In the CSRF tab section, select an exception and click the pencil icon to edit.

3. In the Configure CSRF Exception page, edit details and click Update Exception.
4. You can view the updated exception on the CSRF tab section.

Field format protection

With the field format protection feature of the CADS service, you can examine both the length and type of web form data to ensure that it is appropriate for the field. If inappropriate web form data is found in a user request, you can configure the CADS service to block the request.

The CADS service supports examining the different field formats such as numeric, alphabetic, and alphanumeric. For example, if a particular field expects the user to enter a phone number, the field format protection feature examines the user-submitted input to ensure that the data matches the format of a phone number. If a field expects the first name, this feature ensures that the data in that field is of a type and length appropriate for a first name. It does the same thing for each form field that you configure it to protect.

Enable field format protection

Before configuring the field format protection feature, you must first enable the feature. When disabled, the CADS service does not inspect the field formats of web form data. You must enable the Block Requests toggle to block the requests that violate the field formats. If the block action is disabled, the CADS service only logs the malicious data.

In addition to enabling the feature, you can add one or more enforcement rules to configure field format protection for an individual field of a specific form.

Add a field format enforcement

Complete the following steps to add field format protection for a specific field:

1. Navigate to Applications > Security Protection > Create > Field Format.
2. Click **New Enforcement** and set the following parameters:

   a) **URL Pattern**: The client URL for which field format protection is applied.
   
   b) **Field name**: The name of the field that is validated for the data entered.
   
   c) **Field Format**: The type of data that is allowed for the field. The following types of data are supported:
      
      i. **Integer**
      
      ii. **Alphabets**
      
      iii. **Alphanumeric**
      
      iv. **No HTML**
      
      v. **Any**
      
      vi. **SSN**
      
      vii. **Credit card**
      
      viii. **Custom Format**
   
   d) **Minimum Length**: The minimum length of data allowed in the field.
   
   e) **Maximum Length**: The maximum length of data allowed in the field.
   
   f) **Status**: Select the check box to enable the enforcement.

3. Click **Add Enforcement**.
**Edit a field format enforcement**

Complete the following steps to modify a field format enforcement:

1. Navigate to **Applications > Security Protection**.
2. Click the pencil icon under the **Actions** column corresponding to the security protection that you want to edit.
3. Select **Field Format** on the left navigation menu.
4. Click the pencil icon under the **Actions** column corresponding to the enforcement that you want to edit.
5. Edit the values (or enforcement) and click **Update Enforcement**.

---

**Field consistency**

The field consistency security check examines web forms returned by a user to a website and verifies if the web forms were modified inappropriately by the client. The security check applies only to HTML requests that contain web forms, with or without data.

**Enable field consistency**

Before configuring field consistency security check, you must first enable the feature. When disabled, CADS does not inspect the traffic for form field attacks. Also, you must toggle the Block action to block requests that contain malicious attacks. If the block action is not selected, CADS only logs the data.
Create field consistency exception

You can create a field consistency exception to prevent blocking legitimate requests or resolve false positives and bypass the security check. Complete the following steps to add an exception.

1. Navigate to Applications > Security Protection > Field Consistency > New Exception.

2. Set the following parameters to add an exception for CSRF:
   a) URL Pattern. The URL for which the exception is required. It can be a regular expression. For any URL enter ‘*’.
   b) Status. Toggle command injection exception status.

3. Click Add Exception.
You can view the exception on the **Field Consistency** section.

![Field Consistency](image)

**Edit field consistency exception**

Complete the following steps to update a Cross-site scripting exception:

1. Navigate to **Applications > Security Protection**.
2. Click **Add Security Protection**.
3. In the **Add Security Protection** slide, select an exception and click the pencil icon to edit.
4. In the **Configure Field Consistency Exception** page, edit details, and click **Update Exception**.

**WAF Signatures**

A signature represents a pattern that is a component of a known attack on an operating system, web server, website, XML-based web service, or any other resource. A set of configurable rules offers an easy-to-use security service, applying the power of pattern matching to detect attacks and protect your application against common vulnerabilities and exposures.

**Enable WAF signature protection**

Before you customize a signature rule, you must enable the security check. When disabled, the Citrix App Delivery and Security Service – Citrix Managed does not inspect the traffic for common vulnerability attacks. Also, enable the Block toggle to block requests with a common vulnerability attack. When the block toggle is not selected, the Citrix App Delivery and Security Service – Citrix Managed only logs data for the selected signature rule.

**Manage WAF signatures**

The **Signature** tab section displays a preconfigured list of signatures with new rules added periodically or updates added to old rules. As a user, you might want to customize a signature or list of signatures under a category. To filter signatures, you can select a category and use the search functionality to narrow-down your search.
Categories. Signatures are classified under various categories. You can select a category to view the list of signatures classified under it. For example, selecting web-cgi reduces the table to display signatures that reference web-cgi attack type.

Search. The search functionality enables you to locate a signature based on the category that you have selected. For example, selecting web-cgi as the signature category, you can use the signature attributes to filter signatures that reference this category. Following are the signature attributes and its search operators to filter your search:

- ID. Unique identifier for a signature. Use the search operator to sort rules based on signature ID.
- Log string. Log message for a signature. Use the search operator to sort rules based on log string value.
- Year. The year when the rule was newly added. Use a search operator to sort rules based on a year value.
- Reference. External references to a signature. Use a search operator to sort rules based on reference.
- Block. Block toggle to block traffic. Use a search operator to sort rules based on block toggle status.
- Log. Log toggle to only log data. Use a search operator to sort rules based on log toggle status.

Customize a WAF signature

Complete the following steps to customize a signature:

1. Navigate to Applications > Security Protection > Create > Signatures.
2. In the Signature tab section, select signatures and set the following parameters:
   a) Log. Enable log toggle to only log signature violation.
   b) Block. Enable block toggle to block traffic.
HTTP response headers are used to prevent security attacks on your web application by controlling the browser behavior during application access. In addition to the default headers, the security check enables you to add a security header or delete the Server: Apache/2.4.1 (UNIX) header in the HTTP responder headers for enhanced security protection.

Enable HTTP security header protection

Before you configure the HTTP headers, you must enable the security check. When disabled, the Citrix App Delivery and Security Service – Citrix Managed does not inspect the traffic for HTTP security headers.

Configure default HTTP security header

Complete the following steps to insert a default HTTP header:


2. In the HTTP Security Headers tab section, set the following recommended default headers.

   a) X-Frame-Options. Specifies the browser how to behave when rendering a page in <frame>, <iframe>, <embed> or, <object> format. The security header protects the website from clickjacking attacks. There are two directives for X-Frame options – DENY and SAMEORIGIN. If you specify DENY attempts to load frames from both the same sites and other sites will FAIL. If you specify SAMEORIGIN, page loading works from the same website and fails for other websites.

      i. Value. Select directive type as DENY and SAMEORIGIN.
      ii. Status. Select the toggle to insert the header when examining the traffic.
      iii. Actions. Click the pencil icon to edit a directive.

   b) Content-Security-Policy. Enables administrators to mitigate Cross site script and clickjacking attacks by controlling how the browser loads JavaScript’s images, CSS from different sources. For example, Content-Security-policy: script-src ‘self’ js.example.com. Indicates how JavaScript can be loaded from js.example.com and not from anything else.

      i. Value. Set the source directive value.
      ii. Status. Select the toggle to insert the header when examining the traffic
      iii. Actions. Click the pencil icon to edit.

   c) X-Content-Type-Options. Specifies the browser that only the MIME types advertised by the original web server in the Content-Type headers must be used. This header protects the website against MIME sniffing vulnerabilities.
d) Referrer-Policy. Specifies the browser how much referrer information must be included with requests. There are two directives for referrer-policy security header – no-referrer and no-referrer-when-downgrade (default).

i. Referrer-policy security header – no-referrer. If you specify the no-referrer directive, the Referrer header is omitted, and no referrer information is sent along with the requests.

ii. No-referrer-when-downgrade (default). If you specify the no-referrer-when-downgrade (default) directive, the origin, path, and query string of the URL are sent as a referrer when the protocol security level stays the same (HTTP -> TTP, HTTPS->HTTPS) or improves (HTTP -> HTTPS), but not sent to less secure destinations (HTTPS->HTTP). For “origin” derivative, only the origin of the document is sent as referrer.

A. Value. Directives type for referrer-policy security header.
B. Status. Select the toggle to insert the header when examining the traffic
C. Actions. Click the pencil icon to select a directive.

Add an HTTP security header

The Citrix App Delivery and Security Service – Citrix Managed, security protection enables you to add an extra HTTP security header for enhanced security protection. Complete the following steps to add a new HTTP header:

2. In the HTTP Security Headers tab section, click Insert Additional Headers.
3. In the Insert Additional Headers page, set the following parameters.
   a) Header Name. Name of the HTTP security header.
   b) Value. Directive for the security header.
   c) Status. Select the toggle to insert the header when examining the traffic.
4. Click Add Header.
The Citrix App Delivery and Security Service – Citrix Managed, security protection enables you to delete a server header from the HTTP server-side response. Complete the following steps to delete a header:

2. In the HTTP Security Headers tab section, click Delete Headers.
3. In the Delete Headers page, set the following parameters.
   a) Header Name. Name of the server header to be removed in the HTTP response.
4. Click Delete Header.
You can view the header on the **Delete Headers summary** section.

---

### Data leak prevention

Your websites can have access to database servers that store user-specific sensitive information such as Credit Card numbers and Social Security Numbers. The leakage of such information might pose a security risk. The Data Leak Prevention feature of the CADS service helps to avoid the leak of such sensitive information.
With this feature, the CADS service identifies if the responses coming from the webserver contain any user-specific sensitive information. When a match is found, the CADS service takes configured action to avoid leakage of such information.

The data leak prevention feature allows you to create safe objects that define the rules to prevent attacks. These safe objects contain regular expressions to match the sensitive information in the responses and the action to perform when there is a match.

If the responses from the webserver match the regular expression defined in the safe object, you can configure the CADS service to perform one of the following actions:

- **Block**: Block the response.
- **Mask**: Mask the sensitive information with an X in the responses before processing it further.
- **None**: Take no action. The CADS service processes the responses as is without any changes.

The safe objects for Credit Card and Social Security Number (SSN) are created by default. You can enable or disable these default safe objects and change the action associated with them. You cannot change the name or regular expression of these default safe objects.

You can configure actions at the global level. Configuring the global level action changes the action associated with all the individual safe objects. For example, if you configure the global action as block, the action associated with all the safe objects gets changed to block. You can also change the action specific to individual safe objects.

**Enable data leak prevention**

Before you configure the data leak prevention, you must first Enable Data Leak Prevention. By default, the Credit Card and SSN safe objects are created, disabled, and the action is set to block. If necessary, you can edit the status or safe object action for the default safe objects. You can also create new safe objects by clicking Add Safe Object Rule.

**Note:**

If the data leak prevention feature is disabled, the default safe objects for Credit Card and Social Security Number (SSN) are not effective even if their status is enabled.
Add a safe object

Complete the following steps to create a safe object:

1. Navigate to Applications > Security Protection > Create > Data leak prevention.
2. Select Enable Leak Prevention and click Add Safe Object Rule.
3. On the Configure Safe Object Rule page, enter the following parameters:
   - Safe Object Name: Name for the safe object.
   - Safe Objection Action: The action to perform when the server response matches the configured regular expression. You can choose Block, Mask, or None.
   - Maximum Match Length: The numerical value representing the maximum length of the string that you want to match.
   - Regular expression: A Perl compatible regular expression that is used for matching the response from the server.
   - Comments: Any remarks about the safe object.
4. Select the Status check box to enable the safe object rule.
5. Click Add.
You can view the newly added safe object on the Data Leak Prevention page.
Edit the safe object

Complete the following steps to edit a safe object:

1. Navigate to Applications > Security Protection > Select > Data leak prevention.
2. Select Enable Leak Prevention.
3. Click the edit icon under the Actions column corresponding to the safe object that you want to edit.
4. Perform the required changes and click Update.

You can also delete the safe object by clicking the trash icon under the Actions column corresponding to the desired safe object.
Configure global actions for safe objects

Using the Global Actions option, you can change the safe object action for all the existing safe objects at once.

1. Navigate to Applications > Security Protection > Select > Data leak prevention.
2. Select Enable Leak Prevention.
3. Choose an action from the Global Actions drop-down list.
4. Click Yes, Proceed.

Bot signatures

The bot signature security check protects your web application against bot attacks. Bot signatures help in identifying good and bad bots based on request parameters such as user-agent in the incoming request.

Enable bot signature protection

Before you customize a bot signature rule, you must enable the security check. When disabled, the Citrix App Delivery and Security Service – Citrix Managed does not inspect the traffic for bot attacks. Also, enable the Block toggle to block requests with a bot attack. When the block toggle is not selected, the Citrix App Delivery and Security Service – Citrix Managed only logs data for the selected bot rule.

Manage bot signatures

The list of bot signatures is huge and new rules get added and stale ones are removed periodically. As a user, you might want to search for a specific bot signature or list of signatures under a category. To filter signatures easily, the bot signature page provides an enhanced search capability. The search
Citrix App Delivery and Security service

function enables you to find bot rules and customize its property based on one or more bot signature attributes.

**Categories.** Bot signatures are classified under different categories. You can select a category to view the list of bot signatures classified under it. For example, selecting “Crawler” reduces the table to bot rules that reference Crawler, and it is an easy way to locate Crawler type bot attacks.

**Search.** The search functionality enables you to locate a bot signature based on the category that is selected. For example, selecting “Crawler” as the bot signature category, you can use the bot signature attributes and its search operators to filter a signature that reference the selected bot category. Following are the bot signature attributes and its search operators to filter your search.

- Id. Sort bot signatures based on bot rule ID.
- Name. Sort bot signatures based on rule name.
- Developer. Sort bot signatures based on the host company publisher.
- Type. Sort bot signatures based on signature type.
- Action. Sort bot signatures based on bot action.
- Log. Sort bot signatures that have logging enabled.
- Block. Sort bot signatures that have blocking enabled.

**Customize a bot signature**

Complete the following steps to customize a bot signature:

1. Navigate to **Applications > Security Protection > Create > Bot Signatures**.
2. In the **Signature** tab section, select signatures and set the following parameters:
   a) Log. Enable or disable log to only log data.
   b) Block. Enable or disable block toggle to block traffic.
   c) Action. Action to apply on bot evaluation. Action types are as follows:
      i. Drop. Drop user request without sending a response.
      ii. Reset. Reset client connection by closing it.
3. Once you customize a bot signature rule, click **Create New Security Protection**.

4. You can view the security protection profile in the Add Security Protection summary section.

5. Select the profile and click **Add Security Protection**.

In the **Deliver an Application** page, bind the security profile to a service and click **Deploy**. This step completes the procedure for application delivery.

**Bot trap**

The bot trap is an effective technique to block attacks from bots. This technique detects and blocks automated bots by inserting a random trap URL in the server response. The trap URL is an alphanumeric URL auto-generated by the CADS service and is invisible to human users. However, if the client is an automated bot and if the trap URL is accessed, the CADS service can block the request from the client.
Enable bot trap

Before you configure the bot trap, you must first enable the feature. When disabled the CADS service does not insert the trap URL in the server response. You must toggle the **Block Requests** to block requests from an automated bot. If the block action is not selected, CADS only logs the data.

Configure bot trap enforcement

To prevent bot attacks with specific webpages, add the application URLs for which the bot trap URL must be inserted.

1. Navigate to **Applications > Security Protection > Create > Bot Trap**.
2. Select **Enabled** and **Block Requests**.
3. Click **Add Enforcement** and enter the URL for which the bot trap URL is inserted in the server response. The entity can be a regular expression.
4. Select the **Status** check box to enable the enforcement.
5. Click **Add Enforcement**.
Complete the following steps to update a bot trap enforcement:

1. Navigate to **Applications > Security Protection**.
2. Click the pencil icon under the **Actions** column corresponding to the security protection that you want to edit.
3. Select **Bot Trap** on the left navigation menu.
4. Click the pencil icon under the **Actions** column corresponding to the enforcement that you want to edit.
5. Edit the values (or enforcement) and click **Update Enforcement**.
Deliver a classic application

July 26, 2022

A classic application in the Citrix App Delivery and Security Service – Citrix Managed (CADS) service offers granular control over the configuration as compared to a modern application and is recommended for advanced Citrix ADC users.

Use the classic application workflow in the CADS service if:

• You are an existing Citrix ADC on-premises customer with a substantial investment in existing ADC configurations.
• Interested to move to the Cloud but prefer to have the familiar configuration experience as the Citrix ADC on-premises product.

The CADS service offers two options:

• Create an application from scratch using the ADC config model. Recommended if you are familiar with ADC configurations and want to create similar configurations in the Cloud.
• Migrate an existing ADC configuration to the Cloud. Recommended if you have a stable configuration that has been working well for a long time and you want to move the configuration as is to the CADS service.

To create an application from scratch, see Create a classic application.

To migrate an ADC configuration, see Migrate the ADC configuration to the CADS service.

For a simplified, streamlined experience and when you don’t have an ADC configuration, use the modern application. For more information, see Deliver a modern application.

Supported Citrix ADC features

The following ADC features are supported in the classic application workflow in the CADS service:

• Audit Logging
• Content Switching
• DNS
• Load Balancing
• Monitoring
• Rate limiting
• Rewrite
• Responder
• SSL Offloading
• URL Transform
• Web application firewall (WAF)

Manage a classic application

In the **Applications** page, click one of the following options in the **Actions** column to manage your deployed classic apps. Redeploy the application after making changes.

- Edit
- Redeploy
- Undeploy
- Health Status

Modify and redeploy a classic application

You can edit the application details, services, endpoints, load balancing, content rules, and security protection settings for an application.

1. Navigate to the **Applications** page.
2. For applications whose status is **Deployed**, click the three dots in the **Actions** column.
3. Click **Edit**.
4. Update the configured values and click **Deploy**.

You have completed the steps to modify and redeploy an application.
Check the health status of an application

The health status displays the real-time health of your deployed applications for each application service in an availability zone.

1. Navigate to the Applications page.
2. For applications whose status is Deployed, click the three dots in the Actions column.
3. Click **Health Status**.

The following status indicates that the application is healthy.
The following status indicates that the application is partially up because some of the services are
down.

**Application Status**

**State**: Partially UP 🟢

**Details**:
- `us-east-1c`:
  - `svc301`: UP 🟢
  - `svc302`: DOWN 🔴
- `us-east-1a`:
  - `svc301`: UP 🟢
  - `svc302`: DOWN 🔴

Done
If all the services are down, the following status is displayed.

**Application Status**

**State**: DOWN

**Details**:
- us-east-1c:
  - svc101: DOWN
- us-east-1a:
  - svc101: DOWN

[Done button]
Create a classic application

March 10, 2022

The classic application workflow mirrors the ADC configuration model. It uses the same structure and the same names, such as load balancing virtual server, service and service group, and bindings.

Note
Classic apps are disabled by default. To use classic apps, contact Citrix support to enable it for your account.

Sample configuration for a classic application

You are a Citrix ADC customer interested in using load balancing to evenly distribute network traffic and avoid overloading any back-end server. You also want to ensure that requests from a client are sent to the same back-end server.

Create the following entities:

- Load balancing virtual server. Configure persistency settings on the virtual server.
- HTTP service to bind to the virtual server.

Perform the following steps:

1. Navigate to **Applications > New Application**.

2. Click **Switch to Classic Application**.

3. Type a name for the application and select an environment. Select **Load Balancing**.
4. Add a server. Click Add and specify a server name and the IP address of your back-end application server. Click Create.
The server appears in the list of servers for the load balancing virtual server.
5. Add a service. Click **Add**.

6. Specify a service name. Click **Server Settings**. Specify the server name that you created earlier and port as 80. Click **Create**.
The service appears in the list of services for the load balancing virtual server.
7. Add a load balancing virtual server.

8. Specify values for the following parameters:
   a) Name for the virtual server.
   b) Set Yes for **Frontend VServer**.
   c) Set **Vserver Port** to 80.
   d) Set **Service Type** to HTTP.
   e) Set **Persistence Type** to SOURCEIP.
9. In **Service Bindings**, click **Add**.
10. Type the name for the service that you created earlier and click **Create**.
Service Bindings

Service Name *

demo-service

Weight

Weight

Create  Cancel
The service appears in the list of services bound to the load balancing virtual server.

11. Click **Create**. You have successfully created a virtual server. Click **Submit**.
The application is listed on the Applications page.

12. In the **Actions** column, click the three dots and select **Deploy**.

You have successfully deployed a classic application.

**Migrate the Citrix ADC configuration to the CADS service**

May 30, 2022

In Citrix App Delivery and Security Service – Citrix Managed, you can either create an application or migrate an application from an existing Citrix ADC appliance using the **Migrate Application** feature. With this feature, you can recreate an application configuration in Citrix App Delivery and Security Service – Citrix Managed that exists on a Citrix ADC appliance.

To migrate an application, you require a set of CLI commands as a starting point. For example, you can use the Citrix ADC configuration file (*ns.conf*). Citrix App Delivery and Security Service – Citrix Managed analyzes the CLI commands and identifies the list of distinct applications embedded in the configuration. You can then select one application configuration that you want to migrate. Citrix App Delivery and Security Service – Citrix Managed extracts the corresponding CLI commands, which you
can review before the migration process starts. You can also view and change any of the following values:

- **IP Address/ports** - The IP address and port of the services and service group members from the original application configuration.
- **Configuration Files/Secrets** - Resource files or secrets specified in the application configuration. For example, password and certificate files.

You’re ready to start migrating the application configuration. Migration creates an application. Deploy this application on the target Citrix App Delivery and Security Service – Citrix Managed environment.

**Citrix ADC features supported in the CADS service**

For a list of supported Citrix ADC features in the CADS service, see [Supported Citrix ADC features](#).

**How to migrate a Citrix ADC configuration to the CADS service**

Follow these steps to migrate a Citrix ADC configuration as applications to the CADS service.

1. Click **Applications** and select **Migrate ADC Configuration**.
2. Add the CLI commands, or paste the commands copied from the configuration file (`ns.conf`) of a source Citrix ADC appliance.
3. Select the target application environment where you want to deploy the application. Click **OK** and then click **Next**.
The service starts discovering the applications from the configuration. Click **OK**.
4. Specify the following parameters and then click Next.

- Application Name
- Access Type: Select Internal or External.
- FQDN Type: Select Auto allocated or User defined.
- **Auto Redirect HTTP traffic to HTTPS** Select to ensure that the clients communicate over secure SSL. (Applicable only if the virtual server is of type SSL.)
- Select the virtual servers that form the application endpoint.
The service starts parsing the commands and extracting the application configuration. Click **OK**.
5. Click **Next**. The service validates the CLI commands. Click **OK**.

The commands are displayed in three sections, as applicable. The first section lists the commands that are not applicable to the CADS service.
The second section lists the commands for features that are currently not supported in the CADS service.

The third section lists the commands that contain references to entities that do not exist in your configuration.
6. Click **Next**. Any issues found in the configuration are highlighted in red color. The suggested configuration, after fixing the issues, is also listed.

```
1 add ssi certKey obssupport-20 -cert obssupport.pem -key obssupport.pem -expiryMonitor DISABLED
2 add transform profile obssupportrewrite
3 add transform policy obssupportrewrite transform true obssupportrewrite
4 add sslflow collector af_collector_192.168.93.130 -port 4799
5 add sslflow action af_action_cl-pilot_192.168.93.130 -collectors af_collector_192.168.93.130
6 add sslflow policy af_policy_cl-pilot_192.168.93.130 true af_action_cl-pilot_192.168.93.130
7 add sslflow "debug-web voyager prod-src-sipprofile" -ssProfileType BackEnd -ssl3 DISABLED -denystrongssl NONSECURE
8 set ssl service "debug-web voyager prod-src-sipprofile" debug-web voyager prod-src-sipprofile
9 add server 192.168.93.223 192.168.93.223
10 add service debug-web voyager prod 192.168.93.223 SSL 443 -ssl3 NONE -maxReq 0 -ci=p DisABLED -usip NO -uswebproxyport YES -sp OFF
11 add ssl profile "cl-pilot-vs-sipprofile" -ssl3 DISABLED -tsti DISABLED -denystrongssl NONSECURE
12 add ssl sserver "cl-pilot" -sipprofile "cl-pilot-vs-sipprofile"
13 add authentication vsserver authsv1 http
14 add lb vsserver cl-pilot SSL 0.0.0.0 0 -persistenceType SOURCEIP -timeout 30 -cITimeout 180 authvsname authsv1
15 SSLsecurity profile 0.0.0.0 0 -persistenceType SOURCEIP

Below is the equivalent configuration after fixing up (removing) the highlighted issues. Please review before proceeding further. If the suggested fixup is unsatisfactory, the configuration to migrate can still be modified by going back to Application Configuration step and making appropriate edits.
```

```
1 add ssi certKey obssupport-20 -cert obssupport.pem -key obssupport.pem -expiryMonitor DISABLED
2 add transform profile obssupportrewrite
3 add transform policy obssupportrewrite transform true obssupportrewrite
4 add sslflow collector af_collector_192.168.93.130 -port 4799
5 add sslflow action af_action_cl-pilot_192.168.93.130 -collectors af_collector_192.168.93.130
6 add sslflow policy af_policy_cl-pilot_192.168.93.130 true af_action_cl-pilot_192.168.93.130
7 add sslflow "debug-web voyager prod-src-sipprofile" -ssProfileType BackEnd -ssl3 DISABLED -denystrongssl NONSECURE
8 set ssl service "debug-web voyager prod-src-sipprofile" debug-web voyager prod-src-sipprofile
9 add server 192.168.93.223 192.168.93.223
10 add service debug-web voyager prod 192.168.93.223 SSL 443 -ssl3 NONE -maxReq 0 -ci=p DisABLED -usip NO -uswebproxyport YES -sp OFF
11 add ssl profile "cl-pilot-vs-sipprofile" -ssl3 DISABLED -tsti DISABLED -denystrongssl NONSECURE
12 add ssl sserver "cl-pilot" -sipprofile "cl-pilot-vs-sipprofile"
13 add authentication vsserver authsv1 http
14 add lb vsserver cl-pilot SSL 0.0.0.0 0 -persistenceType SOURCEIP -timeout 30 -cITimeout 180 authvsname authsv1
15 add transform profile ctrans45uat_profile2obsupp
7. Do one of the following:
   
   - Click **Next** to accept the fix.
   - Click **Application Configuration** to edit the configuration. You are taken to the **Application Configuration** page where you can edit the commands.

8. (Optional) Change the IP address and port values for the application servers by clicking the pencil icon. Click **Next**.

9. (Optional) Click the upload icon to upload any SSL certificates required by the application and specify their passwords. You are taken to the SSL certificate store. Select a certificate from the list and click **Select**. Then, click **Next**.
10. Review the configuration summary and click **Migrate**. After successful migration, an application is created with the specified configuration. The following page appears. Click **Close**.

You are taken to the applications landing page.

11. Navigate to your application using the pagination at the bottom of the page. Click the three dots in the **Actions** column and select **Deploy**.

The application summary page appears.
After successful deployment, the application status is updated on the Applications page.

In case of any issues, you can contact Citrix Support at https://www.citrix.com/support/.

Deliver a multi-site application

July 27, 2022

Thinking about providing an optimal user experience for your business applications that are delivered in multiple locations? Doing so can help you to enhance customer satisfaction, brand perception, productivity, and revenue. With the Citrix App Delivery and Security Service – Citrix Managed multi-site application feature, you can configure, deliver, and manage applications across multiple cloud environments for high availability and reliability.

A multi-site application provides global load balancing, site failover, and web traffic management across multiple data centers, cloud, or CDNs. It also plays a key role in business use cases, such as disaster recovery, application performance, application availability, and regulatory compliance.

A multi-site application routes network traffic intelligently across an organization’s data centers and public cloud provider networks. To perform this function, a multi-site application monitors the health, availability, and latency for each site. It applies any other policies that have been configured around regulatory requirements.

Benefits

A multi-site application provides the following benefits:
• **Ensures multi-site resiliency and disaster recovery** - Disaster recovery capability is critical to your business because downtime is costly. With a multi-site application, you have continuous monitoring for your data center’s availability, health, and responsiveness. A multi-site application redirects the traffic to the closest or best performing data center, or to healthy data centers if there is an outage.

• **Improves application performance and availability** - If web traffic isn’t distributed appropriately across data centers, one site might become oversubscribed while another is underutilized. This can result in poor service for some users and the risk of a service disruption because of overflow. Also, the proximity of the user to the server can impact network latency, making site selection a key element of service quality. By providing intelligent web traffic management, a multi-site application ensures that the load is balanced more evenly across sites while also routing content to each user from the nearest available server to ensure an optimal experience.

• **Increases scalability and agility** - A multi-site application solves the problem of limitation of sites and exponential growth of traffic with a greater number of sites. With scalability, you can add, upgrade, and deprovision sites transparently.

• **Reduces latency** - High amount of traffic to a website can significantly increase latency. Multi-site application plays a key role in distributing network traffic across several data centers to ensure that no single data center is overloaded with too many requests. It finds the site with the fastest response time (that is, the best network conditions) for each different client through distributed and crowd-sourced round trip time (RTT) measurements, allowing users to be connected to the optimal site.

• **Optimizes user experience** - A multi-site application allows you to globally load balance all the traffic, dynamically optimize the user experience, and lower service costs. It routes client requests to the nearest data center. It improves user experience by accelerating application response time. Network latency is minimized by delivering content from a data center, which is closer to the requesting user.

• **Meets regulatory and security requirements** - A multi-site application enables you to service a global user base in a manner that complies with government regulations for highly regulated industries such as telecommunications, defense, and healthcare.

**Prerequisites**

Before you deliver a multi-site application, you must complete the following preliminary steps:

• Create a Citrix cloud account profile.
• Create an application environment.

For more information, see Create cloud access profiles and Create an environment.
How a multi-site application works

A multi-site application routes traffic across multiple data centers. DNS infrastructure is used to connect the client to the data center. When a client sends a DNS request, the GSLB DNS server identifies the server that best meets the set criteria. The criteria can be one or more of the following:

- Availability (health) of data center.
- Response time of the data center.
- Geofencing rules that might limit certain data centers to specific geographic locations.
- GSLB distribution algorithm selected.

After the connection is established, the traffic is routed directly between the client and the application.

**Example:**

Let’s consider the following example to understand how a multi-site application distributes traffic based on the optimal round-trip time (optimal RTT) algorithm. For more information about supported algorithms, see Algorithms:

There are two sites or data centers, one in Bengaluru and another in New York.

1. A user in Austin requests the DNS services hosted by the GSLB to get the IP address of the server hosting the multi-site application.
2. The GSLB DNS server gives the IP address to direct the user to the site that would work best for the user according to the criteria. Typically, based on the optimal RTT algorithm, the user is directed to the New York data center. For more information on the optimal RTT algorithm.
3. The user connects to the New York data center.
4. Traffic is established directly between the multi-site application and the user in Austin.

**Deployment types**

The following deployment types are supported for multi-site applications:
• **Active-active** - The multi-site application is deployed in multiple active sites or data centers. If a data center is unreachable, application instances running in the remaining data centers take over the user traffic. This deployment type is ideal when you have a need for global distribution of traffic in a distributed environment, optimize user experience, and reduces latency.

• **Active-passive** - The multi-site application is deployed in an active and one or more passive data centers. This deployment type is ideal for disaster recovery. The active location is used to serve a client request. Traffic is routed to the passive data center only when the active data center goes DOWN.

### Algorithms

An algorithm controls how a multi-site application directs a client request across distributed sites or data centers. The CADS service supports the following load balancing algorithms:

• **Failover** - The failover algorithm supports a simple routing logic where a site is chosen based on its place in line, and its availability. It helps prevent disruption of access to applications delivered across multiple sites. Select the failover algorithm and specify the priority for each site to configure GSLB sites for high availability. This gives you the flexibility to shift traffic to a backup data center and fail over an entire site. You can create a failover chain that decides which site to select first, second, and so on.

  - For example, add primary and standby sites. If the primary site goes DOWN, the traffic is automatically diverted to the standby site. There can be multiple standby sites. Assign a priority of 1 to the primary site and an increasing priority of 2 and above to the standby sites. If the site with priority 1 is DOWN, requests are directed to the site with priority 2. If both the sites are DOWN, the traffic is directed to the site with priority 3, and so on.

• **Round robin** - The round robin algorithm distributes the client requests across the sites or data centers sequentially regardless of the load. Select the round robin algorithm and assign different weights to each site. GSLB performs the weighted round robin distribution of incoming connections. It does this by skipping the lower-weighted services at appropriate intervals. Weights are proportional. You can have three sites with a weight of 2:1:1, 50:25:25, or 90:45:45. In all cases the effect is the same. You can assign weights for the prioritization and selection of each site globally.

  - You can globally assign weights for the prioritization and selection of each site. For example, you have three sites selected for your multi-site application: site A, site B, and site C. You have assigned them the weights: 60, 50, and 10, respectively. The round robin algorithm converts these values into percentages, such as site A=50%, site B=42%, and site 3=8% (which adds up to a 100%). This means that 50% of the time, user requests are routed through site A; 42% of the time through site B; and 8% of the time through site C. If all the sites are given the same weight, traffic will be evenly distributed across them over time. If
you have only one site, then that site will be used 100% of the time, regardless of the weight you give it. Weights are only used for sites that are available. Unavailable sites cause the distribution to not match the configured weights. For example, if site A is weighted 100 and site B is weighted 1, and if site A is unavailable, all traffic is sent to site B.

• **Optimal RTT** - The optimal RTT algorithm measures network proximity. Select the optimal RTT algorithm and specify a penalty to choose the closest healthy data center from a latency perspective. When you specify penalty to a site, you add an extra latency. The additional latency is added to the one calculated by real user measurement (RUM). Penalty is a percentage value that can be applied to a site to modify the RTT, that is, artificially increase the response time (in milliseconds). Increasing or decreasing RTT brings down the performance of the site, such that the likelihood of it being picked is lower.

  - For example, a site might be expensive (hosted in a country where bandwidth or infrastructure cost is higher), and you want to reduce the likelihood of it being picked when an equivalent provider is close enough in terms of performance. So, you put in a penalty value (in percentage) that acts as a multiplier to increase the value of response time, as a result, lowering the probability of that site being picked. Let’s assume that RTT without penalty for site A is 50 milliseconds and for site B is 60 milliseconds. Specify a penalty of two (2) to site A and zero (0) to site B. The RTT for site A would be calculated as follows:

    Site A RTT with penalty applied = RTT (Round Trip Time in milliseconds) x (1 + Penalty)  
    = 50 milliseconds

    Thus, site A that now has an RTT of 150 milliseconds is not selected over site B that continues to have an RTT of 60 milliseconds.

• **Static Proximity**: The static proximity algorithm sends client requests to a site that is geographically nearest to the user location. The algorithm looks up the built-in GeoIP database and determines the client location based on the IP address derived by the DNS query. After identifying the location, the algorithm checks if the site is healthy and in the active state to process client requests. The healthy, active site that is geographically nearest to the user location responds to client requests.

  For example, consider a multi-site application having a healthy, active site in United States of America and in Singapore. With static proximity, client requests coming from India are sent to the Singapore site as it is geographically nearer.

**Monitors (Site health check)**

Monitors determine if a site is healthy by sending a health probe to a site. If the site responds, the monitor marks the state of the site as UP. If the site doesn’t respond to the designated number of probes within the specified time, the monitor marks the site as DOWN. No requests are forwarded to this site until its state changes to UP.
You can configure an HTTP, HTTPS, or TCP type monitor, specify a port for the health check, and add a URL path for the HTTP or HTTPS health probes to determine if the site is healthy. Health probes are by default sent to http(s)://hostname/path. You can enter a custom FQDN and path, such as hostname1/path/test, if you want to override the health probes URL to http://hostname1/path/test or https://hostname1/path/test.

**Note:**
The custom FQDN only overrides the URL related attributes (HTTPS server name indicator and HTTP(S) host header) and not the target IP of the health probe.

**Stickiness**

Some applications require stickiness between a client and a data center. All requests in a long-lived transaction from a client must be sent to the same data center; otherwise, the application session may be broken, with a negative impact on the client.

Stickiness is accomplished by enabling site persistence. Enabling stickiness ensures that a series of client requests for the multi-site application is sent to the same back end site instead of being load balanced if this site remains healthy. This enables the clients to remain sticky to a back-end site, even in the face of changing network conditions (for optimal RTT), site health (site with higher priority became healthy again), and round robin decisions.

For example, in an e-commerce website that uses a shopping cart, the server needs to maintain the state of the connection to track the transaction. With stickiness enabled, the client requests are forwarded to the same IP address of the selected data center for all subsequent DNS requests.

If a stickiness session points to a data center that is DOWN, then the configured GSLB method is used to select a new data center.

**DNS**

Domain Name System (DNS) translates human-readable domain names to machine-readable IP addresses, and vice versa.

The response from a DNS server typically has the IP address of the requested domain. If the IP address of the requested domain is unknown, the same is conveyed in the response.

**DNS time to live**

The DNS time to live (TTL) indicates how long the DNS response is cached by clients for the multi-site application. The default TTL is 20 seconds. Citrix recommends keeping the default value. Lowering
the TTL increases the number of DNS queries, leading to added cost and reduced performance. Increasing the TTL results in clients caching the DNS response for a longer time and a data center might become unhealthy during this time. Therefore, it is best not to change the default value of TTL.

**DNS fallback endpoint**

You can add an endpoint that acts as a backup endpoint and responds to DNS queries when all sites associated with a multi-site application are in DOWN state. If the DNS fallback endpoint is left blank, an empty DNS response is sent back to such DNS queries.

**Empty DNS responses**

When all sites associated with a multi-site application are in DOWN state, and there is no DNS fallback endpoint configured, the application sends empty DNS responses to clients trying to connect to the server. The responses do not have any IP address record in it. However the response code is successful. Sending empty DNS responses to clients, prevents clients from reconnecting to the multi-site application that has all sites in DOWN state.

The application checks the status of sites every 20 seconds and if any of them is back in the UP state, then the responses have IP addresses of the requested domain.

To check if a multi-site application is sending an empty DNS response, run the following command at the command prompt:

```
1  dig <FQDN of the multi-site application>
2  <!--NeedCopy-->
```

In the output you can see that the DNS response does not contain any IP address record.

Example:

```
1  dig 003e.16ed0.itms.appdeliverysecurity.com
2  <!--NeedCopy-->
```
Maintenance mode

Sites require periodic maintenance. The maintenance mode feature in multi-site applications enables you to plan for a scheduled maintenance or anticipate downtime for performing an upgrade, testing network connectivity, diagnosing an underlying hardware issue, and so on. Once your scheduled maintenance is completed, you can disable the maintenance mode.

Note:
For sites in the maintenance mode, the multi-site application in the analytics dashboard will be marked as under maintenance.

Geofencing

Regulatory compliance differs from country to country. This aspect must be kept in mind when delivering applications across multiple geographical locations and data flows across borders. Many organizations face mandates regarding the geographic location of data storage and processing. For example, the general data protection regulation (GDPR) dictates that EU-based users must be served by local servers for certain application requirements.

The Citrix App Delivery and Security Service – Citrix Managed multi-site application feature helps you to adhere to regulatory compliance. With the geofencing feature, a multi-site application can be configured to use specific data centers to serve users in specific regions, simplifying compliance with this
rule. Based on the countries configured in the Geo IP database, the requests are forwarded to the servers that host content customized for the regions.

**Cloud region recommendation engine**

The location of a site is an important factor in the performance of a multi-site application. The cloud region recommendation engine in the CADS service recommends you the best locations to deploy new sites for a multi-site application. These recommendations help you boost the overall performance of your application.

The recommendations provided are based on the user location, traffic (in percentage) expected from each user location, and the cloud service provider. You can use the recommended site location information while adding sites for a multi-site application.

The cloud region recommendation engine provides recommendations for single site, dual site, and triple site scenarios. The recommendations contain the location information, global latency, and benefit percentage. Global latency is based on real time measurements and the site location recommendations are arranged according to the best performing combination of cloud providers’ sites. Benefit displays the advantage of choosing dual-site or triple-site in comparison with the single site.

You can get recommendations for new applications and also existing applications. For existing applications, already configured sites are also displayed and included for calculating the recommendations. You can choose to exclude the existing sites from the recommendation calculations.

The recommendations are specific to the application you select. Enter user location, traffic expected from each user location, and the cloud service provider for an application and get the corresponding recommendations.

**Note:**

The cloud region recommendation engine only provides insights on the latency that the user experiences and the benefit of deploying additional sites to reduce the latency. Based on your network needs and preferences, you can decide if the lower latency outweighs the cost incurred for deploying the application in a second or third location.

To get the cloud region recommendations:

1. Navigate to **Multi-Site Applications > Recommendations** tab.
2. Select **New Application** or an existing application from **Select your application**.
3. Click **+ Location**. Select the user location from the list and add the expected traffic percentage.
   You can add a maximum of six user locations.

   **Note:**

   For the United States, apart from the country level selection, you can also choose one of
4. Toggle the **Existing Locations**. When enabled, for existing multi-site applications, the existing sites are included for recommendation calculations. This toggle does not impact recommendation calculations for new applications.

5. Optionally, select the preferred cloud provider from the **Cloud Provider** list and click **Recommend**.

6. The recommendations are listed under the **Recommended Site Locations** section. Click the recommendation list to view the geographic location of the site on the map.

Initially, the best recommended sites are listed under the **Recommended Site Locations** section. Clicking the next recommendation icon lists the next best recommendation. As you move on with the next set of recommendations, the global latency increases. You can also view the **Next 10 recommendations**.
Deliver a multi-site application

The Citrix App Delivery and Security Service – Citrix Managed multi-site application feature enables you to create, configure, and deliver an application in multiple sites.

**Step 1: Create a multi-site application**

Follow the steps to create a multi-site application and define the application endpoints.

1. Navigate to Multi-Site Applications > New Multi-Site Application.
2. In the Create a Multi-Site Application page, type the application name in Application Name.
3. Select an Application FQDN Type:
   - Select Auto-allocated if you want to use a DNS provider other than AWS Route 53.
   - The Citrix App Delivery and Security Service – Citrix Managed multi-site feature handles the creation of FQDN. It displays the FQDN details in the Multi-Site Applications summary.
page after the application delivery. You can configure the FQDN as a CNAME record in your DNS provider.

- **Select User Defined (Route 53)** if you want AWS Route 53 as the DNS provider to host the application FQDN and do the following:
  
  a) Select a **Cloud Access Profile** that is already configured.
  
  b) Type the domain name for the application in **Domain of Application FQDN**.
  
  c) Select the hosted DNS zone from the **Hosted DNS Zone** list. The Citrix App Delivery and Security Service – Citrix Managed multi-site feature handles the creation of FQDN. A CNAME for this FQDN is automatically created in your AWS Route 53 hosted zone.
4. Type a value in **DNS Time to Live**. The value indicates how long the DNS response is cached for the application.

5. Type an IP address or a host name in **DNS Fallback Endpoint**. This endpoint acts as a backup endpoint and responds to DNS queries when there are no healthy sites available for the multi-site application. If the field is left blank, the multi-site application sends an empty DNS response.

You have completed the steps to define the endpoint details for the multi-site application.

Click **Next**, to add a site.

**Step 2: Add a site**

Sites are locations that are load balanced by GSLB. You can either create a **User Defined** or a **Managed** site. Follow these steps to add and configure a site.

1. Click **Add Site**.

2. In the **Add a New Site** page, do one of the following:
   - Select **User Defined** if you want your site to be an on-premises data center, cloud, CDN, or any external platform not managed by the Citrix App Delivery and Security Service – Citrix Managed edition. Do the following:
     a) Type the name of the site in **Site Name**.
     b) Type an IPv4 address (32-bit), a DNS name, or an IPv6 address (128-bit hexadecimal) in the **DNS Name, IPv4, or IPv6** field for the application hosted on the user-defined site.
Note:
A combination of sites configured with IPv4 address (or DNS name) and IPv6 address is not supported. This combination might lead to inconsistent behavior of the multi-site application.

- Select Managed if you want the Citrix App Delivery and Security Service – Citrix Managed edition to manage the site in the AWS cloud. Do the following:
  a) Type the name of the site in Site Name.
  b) Select an application that is delivered. The FQDN and the AWS location of the delivered application is automatically populated.

3. Configure a monitor to send health probes to the site to verify if they are healthy. Do the following:
   a) Select a protocol. You can select HTTP, HTTPS, or TCP.
      If you select HTTP or HTTPS, the port number gets populated automatically. If needed, you can change the port number. Enter the Host and Path.
      You can select TCP only for user-defined sites. If you select TCP, enter the port number manually.

       Note:
The protocol type is automatically populated for the managed site.

   b) Type a TCP port number in Port, which is used by the application hosted on the site.

       Note:
The port number is automatically populated for the managed site.

   c) FQDN is automatically populated in Host. Optionally, you can type a custom FQDN and path in Host. For example, type hostname1/path/test if you want to override the health probes URL to http://hostname1/path/test or https://hostname1/path/test instead. Modifying the monitor's FQDN is necessary if there is HTTPS endpoints, since the installed certificate might result in SSL failures (that is, if there is a user-defined site with an IP address 1.1.1.1, https://1.1.1.1/ would fail, whereas https://hostname1/ would succeed) and mark the site as unhealthy.

4. Select the location type of the user-defined site. You can host your site either in a public cloud provider network or in your private data center. Choose one of the following:
   - **AWS/Azure/GCP**: Select AWS/Azure/GCP if you are hosting the site in a Point of Presence (POP) belonging to AWS, Azure, or Google Cloud Platform. Select the POP or Availability Zone (AZ).
   - **CDN**: Select CDN if you are hosting the site in a Content Delivery Network (CDN). A CDN has a globally distributed set of servers that proxies and caches web data at edge locations...
Citrix App Delivery and Security service

closest to the users. Select the CDN.

- **Private Data Center**: Select **Private Data Center** if you are hosting the site in your private data center. Type the geographical location where the site is hosted. This field is integrated with Google maps.

**Note:**

The location is automatically populated for managed sites and user-defined sites hosted in a public cloud or a CDN.

5. **Toggle to enable Configure Radar** if you have chosen **Private Data Center** as the site location type. Type the URL path to retrieve the radar object to measure the RTT of the site. For example, type `http(s)://<ip-or-dns-name>/path/to/`.

**Note:**

- The extension, `r20.png` is automatically appended to the given URL.
- If you don’t select the **Configure Radar** option and successfully complete the radar object configuration, the Optimal RTT algorithm is disabled while configuring GSLB methods.
- For successful multi-site application delivery, the radar probe URL must be reachable.
- For managed sites and public cloud provider site location types, radar measurements are automatically collected.
- Radar must be activated for the selected private data center. For more information, see [Activate radar for a private data center](#).

6. **Select continents and countries in Geo Fencing** that can access your site. By default, all the continents are selected. For example, to select a particular continent, deselect **Select All** and select **Asia**. Only users from the Asia continent are serviced from this site. You can also search for a location.
7. Select the **Perform Site Maintenance** check-box to mark your site in the maintenance mode.

**Note:**
For sites in the maintenance mode, the multi-site application in the **Analytics** dashboard is marked as under maintenance.

8. Click **Add Site**. The site is added, and its details are displayed.
9. Click **Add Site** and repeat steps 1–8 if you want to add another site.

You have completed the steps to add and configure sites.

Click the **Edit** or **Delete** icon in the **ACTIONS** column to edit the site details or delete a site, respectively.

**Note:**

After you create a site, you can’t edit the **Site Type**.

To configure GSLB and deliver the multi-site application, click **Next**.

**Step 3: Configure GSLB and deliver the multi-site application**

Follow these steps to configure the GSLB algorithm to route the network traffic intelligently across sites, configure stickiness, and deliver the multi-site application.

1. Select an algorithm to route the client traffic to sites. For more information about supported algorithms, see **Algorithms**.

   - Select **Failover** and type a value in **PRIORITY** for each site. For example, assign a priority of 1 to site A and an increasing priority of 2 and above to the standby sites.
   - Select **Round Robin** and type a value in **WEIGHT** to distribute the traffic to each GSLB site. For example, assign a weight nine (9) to site A and weight one (1) to site B.
   - Select **Optimal RTT** and type a value in **PENALTY**.
   - Select **Static Proximity**.

2. Select **Enabled** in **Stickiness** to enable stickiness if necessary. If not required, continue to step 5.

**Note**

The FQDN for multi-site applications is auto-generated under the itms.appdeliverysecurity.com top level domain (TLD) for sticky applications, rather than the default itms.appdeliverysecurity.com.
Changing stickiness for existing multi-site applications takes some time to propagate. The time taken to propagate depends on the TTL of the CNAME record pointing to the itm(s).appdeliverysecurity.com autogenerated record. The TTL for a multi-site application with user-defined FQDN is 10 minutes and therefore the change propagation takes around 10 minutes. The TTL for multisite applications with auto-allocated FQDN depends on the TTL duration configured by the application admin for the respective CNAME record.

The previously auto-generated FQDN remains active while the CNAME change propagates. Users hitting a cached CNAME record before propagation completion can still access the multisite application with the previous stickiness settings.

3. Type a value in **Stickiness Time To Live**. If stickiness is enabled, its TTL controls the time duration within which subsequent client requests for the multi-site application are sent to the same site.

4. Enter **Stickiness IPv4 Mask**. If stickiness is enabled, the client requests coming to the multi-site application are identified using this IPv4 subnet mask and sent to the same site.

5. Click **Deploy**.

The multi-site application is deployed successfully.

To view the summary and manage the multi-site applications, click **Manage Multi-Site Applications**.

**Multi-site application summary**

The **Multi-Site Applications** summary page lists the total number of created multi-site applications and lists the following details about each application:

- **MULTI-SITE APPLICATION NAME** - Name of the multi-site application.
- **FQDN** - Fully qualified domain name (FQDN) of the multi-site application.
Citrix App Delivery and Security service

- **STATUS** - The current deployment status of the multi-site application. One of the following values is displayed:
  - **INDRAFT** — The multi-site application is created, but the back-end resources are not deployed.
  - **ERROR** — The multi-site application deployment failed.
  - **DEPLOYED** — The multi-site application is successfully deployed.
  - **IN PROGRESS** — The multi-site application deployment is in progress.

- **ALGORITHM** - GSLB method such as failover, round robin, and optimal RTT used to configure the multi-site application. The method specified is used to determine the site that is selected (DNS response) for client requests.

- **ACTIONS** - Enables you to either modify, redeploy, undeploy, or delete a multi-site application. For more information, see Manage multi-site applications.

### Manage multi-site applications

In the **Multi-Site Applications** summary page, click the three dots in the **ACTIONS** column to manage your delivered multi-site applications.
Modify and redeploy a multi-site application

Follow these steps to edit the application details, site configuration, or GSLB configuration and redeploy the multi-site application.

1. In the Multi-Site Applications summary page, click … in the ACTIONS column and click Edit.

2. In the Edit Multi-Site Application page, click the Application Details, Location, or GSLB tab to make the required changes. For example, click GSLB and edit the algorithm.

3. Click Modify.

4. Click Redeploy.

You have completed the steps to modify and redeploy a multi-site application.
Undeploy a multi-site application

Follow these steps to undeploy a multi-site application.

1. In the Multi-Site Applications summary page, click … in the ACTIONS column. Click Undeploy.

2. In the Undeploy Multi-Site Application page, click Yes, Undeploy.

You have completed the steps to undeploy a multi-site application. Undeployed applications are in the INDRAFT status. You can either edit and redeploy, or delete them.

Delete a multi-site application

Follow these steps to delete a multi-site application.

Note:

You can delete a multi-site application only if it is undeployed.

1. In the Multi-Site Applications summary page, click … in the ACTIONS column. Click Delete.
2. In the **Delete Multi-Site Application** page, click **Yes, Delete**.

You have completed the steps to delete a multi-site application.

**Related topics**

*Activating radar for a private data center*

**Activate radar for a private data center**

March 31, 2022

Today’s business environment demands the ability to run an application that is both globally connected and consistently high performing. To achieve this, you need a tool that measures real-time internet performance across all major clouds and CDNs, and across a global network.

Radar uses a JavaScript script embedded within an application provider’s pages to collect information about the performance and availability of a multi-site application. Radar takes measurements from about 900 million users across 50,000 ISP networks, resulting in 10 billion data points every day, which enables you to ensure that the content and applications are always available, and the users receive the best experience.
Real user measurements (RUMs) on such a significant scale are achieved through Radar. RUMs can be achieved through radar tags and objects. A radar tag is a JavaScript tag integrated with the application provider’s pages you want to measure. The radar object can be deployed on the site using a responder policy and action. Responder action and policy serve a 43 bytes single pixel image whenever a URL with the extension r20.png is requested by the user’s browser.

When users access an application provider’s page, the radar tag runs and instructs the browser to retrieve radar objects, collect the metrics and send the telemetry to Radar.

The public cloud site locations have radar configured by default. If you are using a private data center, you must manually configure the Radar. The CADS service provides its application providers the ability to deploy the radar objects and measure the performance of their private data centers. Radar collects the following metrics:

- **Availability**: Specifies whether the radar object loads or not.
- **Response Time**: Specifies how long it takes for the server to respond to a subsequent request, once all of the noise of establishing a connection is completed. This is a relatively close approximation of TCP round-trip time (RTT) from the browser to the provider.
- **Throughput**: Throughput is the data rate of the connection, in kilobits per second, as measured from the retrieval of a 100 KB object.

These metrics allow the customer to effectively evaluate an existing content delivery strategy and take advantage of the Optimal RTT GSLB algorithm for hybrid multi-cloud applications. The information collected remains available only to the application provider. After configuring radar, the application provider can choose to become a radar member. Radar members are the application providers who have radar configured on their sites and also share their metrics with the radar community. Contact Citrix support to understand the benefits of collecting community measurements.

**Note:**
You do not get to see metrics collected from radar configuration in the CADS service UI. You can only view the healthiness of sites under **Analytics > Multi-site applications**.

To summarize, the radar RTT measurement process follows these steps:

1. Users visit the application (webpage) with a radar tag and when they download a webpage, they receive the radar tag.
2. When the page has finished loading, the radar tag initiates a request to each site.
3. The radar tag retrieves the small radar objects to determine the HTTP response time.
4. The data is collated and sent to the radar community. Based on the data, perform an optimal RTT and route the traffic to the site with the lowest RTT.

Activating radar for a private data center is a two-step process:

1. Integrate radar tag in application webpages.
2. Deploy radar objects on a site in a private data center.
Integrate radar tag in customer webpages

Prerequisite: To integrate the radar tag, you must know your customer id. Contact Citrix support to know your customer id. For more information on contacting Citrix support, see https://support.citrix.com/article/CTX128597.

Based on your need, you can choose one of the following methods to integrate the radar tag:

Note:
Do not change the JavaScript snippet. The code includes important information which if changed can create unexpected or unreliable behavior.

- Default tag: The default tag is the recommended version of the radar tag. The default radar tag waits until the load event is complete before downloading and running the radar client, ensuring that the load event is uninterrupted.

```html
<script>
if (typeof window.addEventListener === "function") {
    window.addEventListener("load", function() {
        if (window.cedexis === undefined) {
            var radar = document.createElement("script");
            radar.src = "//radar.cedexis.com/1/<cid>/radar.js"; // replace with user specific value
            document.body.appendChild(radar);
        }
    });
}
</script>
<!--NeedCopy-->
```

Replace `<cid>` with your customer id in the radar tag and place it in the HTML of the webpages just before the closing BODY tag.

- Pre-loading Radar Tag: If you are using Content Security Policy settings preventing the use of inline JavaScript, use pre-loading radar tag. This radar tag keeps the download of the radar client from blocking further parsing of the page, but runs it before the load event has fired.
Replace `<cid>` with your customer id in the radar tag and place it in the HTML of the webpages you want to measure.

- **Radar Native SDKs**: The Radar SDKs include client libraries that you can easily incorporate into any iOS or Android mobile app. The SDKs allow you to embed the Radar tag functionality, to take periodic measurements from the native application, without having to manually load and manage a web view.
  - iOS: https://github.com/cedexis/RadarKit
  - Android: https://github.com/cedexis/AndroidRadar
  - Headless: https://github.com/cedexis/radar-runner
  - Web Services: https://github.com/cedexis/webservices

**Deploy radar objects**

You can deploy radar objects in one of the following ways:

- Deploy Radar Objects on a host in a private DC.
- Integrate with Citrix ADC.

**Deploy radar objects on a site in a private data center**

**Prerequisite**: To serve the radar objects using TLS, ensure that the following certificates are available in the corresponding paths:

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public TLS certificate</td>
<td>/etc/ssl/public.crt</td>
</tr>
<tr>
<td>Private TLS key</td>
<td>/etc/ssl/private.key</td>
</tr>
<tr>
<td>Certificate chain</td>
<td>/etc/ssl/ca-certs.pem</td>
</tr>
</tbody>
</table>

Radar objects can be served by any modern operating system and webserver. The following instructions are tested against Ubuntu20 in Apache.

1. Install Apache2 and git packages.
Citrix App Delivery and Security service

1. `sudo apt-get install apache2 git
2. <!--NeedCopy-->`

2. Create and populate the Apache2 directory.

```
1. sudo mkdir -p /var/www/radar-objects
2. sudo git clone https://github.com/cedexis/testobjects /var/www/radar-objects/
3. <!--NeedCopy-->`

3. Disable the default Apache2 virtual host.

```
1. sudo rm /etc/apache2/sites-enabled/000-default.conf
2. <!--NeedCopy-->`

4. Enable the Apache2 mods as follows:

```
1. sudo a2enmod headers
2. sudo a2enmod rewrite
3. sudo a2enmod ssl
4. sudo systemctl restart apache2
5. <!--NeedCopy-->`

5. Add the Apache2 site configuration.

```
1. cat > /etc/apache2/sites-available/radar-objects.conf << 'EOF'
2. ErrorLog ${APACHE_LOG_DIR}/error.log
3. CustomLog ${APACHE_LOG_DIR}/access.log combined
4. DocumentRoot /var/www/radar-objects
5. Header add "Timing-Allow-Origin" "*"
6. RewriteEngine on
7. RedirectMatch 404 /\.git
8. EOF
"
6. Enable the new Apache site and restart Apache2.

```
sudo ln -s /etc/apache2/sites-available/radar-objects.conf /etc/apache2/sites-enabled/radar-objects.conf
sudo systemctl restart apache2
```

7. Verify if the radar objects are being served.

```
curl https://<FQDN>/img/r20.png
```
Integrate with Citrix ADC

You can deploy the radar object using Citrix ADC. You can either use the command line or the Citrix ADC Configuration Utility. For more information, see https://docs.citrix.com/en-us/citrix-intelligent-traffic-management/radar.html#integration-with-citrix-adc.

Application analytics

March 30, 2022

Citrix App Delivery and Security Analytics feature provides an easy and scalable way to view various insights to analyze and improve the application performance. You can use the following analytics features simultaneously in Citrix App Delivery and Security service:

<table>
<thead>
<tr>
<th>Analytics feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application analytics</td>
<td>Application analytics enable you to monitor the overall performance of the applications configured from the Citrix App Delivery and Security service.</td>
</tr>
<tr>
<td>Web Insight</td>
<td>Web Insight enables you to evaluate and visualize the complete application from the perspectives of performance and usage together. You can view Web Insight for an application and for all applications together.</td>
</tr>
<tr>
<td>Security</td>
<td>Security insight provides a single-pane solution to help you assess your application security status and take corrective actions to secure your applications from WAF and Bot violations.</td>
</tr>
<tr>
<td>Multi-site applications</td>
<td>Multi-site application analytics provide a single-pane solution to visualize the overall performance of multi-site applications configured from the Citrix App Delivery and Security service.</td>
</tr>
</tbody>
</table>
The application analytics feature of Citrix App Delivery and Security service enables you to monitor and help you to:

- Check the score and analyze the overall performance of the applications.
- Check for any issues that persist with server or client.
- Detect anomalies in the application traffic flows and take corrective actions.

**Note:**
Applications refer to one or more virtual servers that are configured on the Citrix App Delivery and Security service.

**Application dashboard overview**

After you deliver an application, the application dashboard enables you to view application details such as app name, app status, issues, and so on. For more information, see [Deliver an application](#).

All applications are displayed in the dashboard only after the applications start to generate data. From the dashboard, click an application to view detailed information about the application performance.

Navigate to **Analytics > Applications** to view the app dashboard.

The carousel slider offers ease of access to all options available in the **Filters** section.

From the **Filters**, you can:

- Select to view applications based on the following application scores:
  - **Critical** – Application score is between 0 and < 40.
  - **Fair** – Application score is between 40 and < 75.
  - **Good** – Application score is greater than or equal to 75.
  - **Not Applicable** – No virtual servers are configured.

- Select to view applications based on the application status such as **Up, Down, and Out of Service**.

- Select to view applications based on their issues and issue categories.

- Drag or select the histogram on the various metrics and view applications.

You can apply filters on the following:

- **Application score** – View applications based on **Critical, Review, Good**, and **Not Applicable**.
Note:
By default, you can view applications that are in Critical, Review, and Good status. To view applications that are in N/A status, you must select the Not Applicable option.

- **State** – View application based on the application status such as Up, Down, and Out Of Service.
- **Issue categories** – Provides a list of applications impacted with a specific issue, by choosing the issue type such as Performance and Config.
- **Current Issues** – Provides a list of applications with current issues that impact the app score.
- **Response Time** – A histogram that displays the average response time received by the applications.
- **Total Requests** – A histogram that displays the total number of requests received by the applications.
- **Throughput** – A histogram that displays the total network throughput processed by the applications.
- **Data Volume** – A histogram that displays the total data processed by the applications. Data volume is calculated by the total request bytes and response bytes for the applications.
- **Client Connections** – A histogram that displays the average client connections established by the applications.
- **Server Connections** – A histogram that displays the average server connections established by the applications.

**View applications**

By default, the dashboard displays all applications. Depending upon your requirement, you can use the filter option to view applications. You can view applications either by selecting the graph view or the table view.

The dashboard displays the following application details:

- **App name** – The application name.
- **App Score** – The application score and the status such as Critical, Good, Fair, and Not Applicable.
- **State** – The current availability of the application, such as Up, Down, Out of Service, and NA.
  - **Up** – All virtual servers associated with the application are Up.
  - **Down** – All virtual servers associated with the application are Down.
  - **Out Of Service** – All virtual servers associated with the applications are out of service.
- **NA** – No virtual server is configured for the application.

- **Top issue** – The issue that has the maximum error counts on the application.

- **Top issue category** – The issue category that has the maximum errors *(Performance or Config)*.

- **Issue count** – The total issue counts for the application.

- **Response time** – The average response time to respond from the application.

- **Total requests** – The total requests received by the application.

- **Throughput** – The total network throughput for the application. Throughput is calculated by the **Req Bytes / Sec + Res Bytes / Sec** for the virtual servers.

- **Data volume** – The total data processed by the application.

- **Client connections** – The average client connections established by the application.

- **Server connections** – The average server connections established by the application.

You can also click + and select the categories that you want to view.

**Points to note:**

- After you add or edit an application, it may take a few minutes to reflect the application in the dashboard.

- If you delete an application, the dashboard still displays the deleted application, until Citrix App Delivery and Security service has its analytics data (maximum of 1-month duration).

For example, consider that you have created an application on Jan 2, 2020 and you have deleted the application on Jan 4, 2020. In this scenario:

- The dashboard can still display the deleted application on Jan 4, 2020, when you select the time duration for the last 1-day, 1-week and 1-month.

- The dashboard can still display the deleted application on Jan 5, 2020, when you select the time duration for the last 1 week and 1 month.

- When the duration exceeds the app deletion date, the application is not displayed in the dashboard. That is, the dashboard does not display the deleted application on Jan 6, 2020 (for the last 1 day), Jan 12, 2020 (for the last 1 week), and after February 5, 2020 (for the last 1 month).

- When you click the deleted application from the dashboard, the following message is displayed.
Application details

January 20, 2022

From the dashboard, click an application to drill down for further detailed information.

Select the time from the list to view:

- **Transaction Logs** – Enables you to view the detailed transaction for the application, such as response time > 500 ms, 5xx errors, and so on.
- **Performance** – Enables you to view the application performance such as app score and the issues that are affecting the app score.
- **Key Metrics** – Enables you to identify the application usage.
- **Web Insight** – Enables you to visualize the complete application from the perspectives of performance and usage.
- **Security** – Enables you to view the application WAF violations.

After you select the time from the list, the following application details are displayed:

- **App Score** – The application score for the selected time duration and the current issues that are impacting the application score. The final score is calculated as 100 minus total penalty.

- **All Services** – The services that are bound to the application. You can view the service status that is in **Up**, **Out of Service**, or **Down**.

Click to view the service details.
Citrix App Delivery and Security service

Select the service and click:

- **Bound Servers** to view the details of the servers associated with the service.
- **Bound Monitors** to view the details of the monitors associated with the service.

- **Issues** - The current issues that are affecting the app score. You can view the following issues:
  - Response Time
  - Server error (5xx)
  - Active services

**Response Time**

This issue detects when the application response time to respond to client requests deviates from the configured threshold value. Click the **Response Time** tab to view the issue details.

Under **Details**, you can view:
Citrix App Delivery and Security service

- The graph indicating the total events for the selected time. Click to apply filter and view details.
- The date and time that the issue has occurred.
- The total occurrences for the selected time.
- The issue severity such as low, medium, and high.
- The detection message indicating the total transaction response time exceeding the configured threshold value.

Active Services

This issue detects when the % of active services bound to the virtual server is lesser than the configured threshold value. Click the Active Services tab to view the issue details.

Under Details, you can view:

- The graph indicating the total events for the selected time duration. Click to apply filter and view details.
- The date and time that the issue has occurred.
- The total occurrences for the selected time duration.
- The issue severity such as low, medium, and high.
- The detection message indicating the % of active service sessions and the configured threshold value.

Server error 5xx

In some scenarios, the web server responds with status codes when it is unable to handle the requests for reasons such as invalid requests, temporary overloading, or server maintenance. These errors are
displayed with error codes, which define various scenarios of the errors. For example:

- **502 Bad Gateway**: The server is acting as a gateway or proxy and received an invalid response from the upstream server.
- **503 Service Unavailable**: The server is unavailable. The servers might be overloaded or down for maintenance.
- **504 Gateway Time-out**: The server is acting as a gateway or proxy and did not receive a timely response from the upstream server.

These can be temporary conditions, but sometimes you must implement a corrective measure on the webservers to make the webpages up and available.

Using the **Server Error 5xx** indicator, you can view these failures and take decisions about corrective actions to overcome the issues and ensure the client requests are served and the webpages are always available.

Select the **Server Error 5xx** tab to view the issue details.

The **Recommended Actions** to troubleshoot the issue are:

- Configure L7 monitors with appropriate parameters for the server that responds with 5xx errors. A monitor is an entity that tracks the service health. The appliance periodically probes the servers using the monitor bound to each service. If a server does not respond within a specified response timeout, and the specified probes fail, the service is marked DOWN. The appliance then performs load balancing among the remaining services.
- Troubleshoot the server.

Under **Details**, you can view:

- The time that occurred the unstable server anomaly.
- The service/service group name
- Total occurrences
- The anomaly severity such as high, low, and medium.
- The detection message indicating % of the responses from this service reporting 5xx errors.

## Set thresholds for app score

November 10, 2021

As an administrator, you can decide to select the components and configure thresholds for app score calculation. App score is the scoring system that defines:
Citrix App Delivery and Security service

- How well an application is performing.
- Whether the application is performing well in terms of responsiveness.

Navigate to Analytics > Applications and then select the settings icon.

In the Configure App Score page, you can select the components and configure thresholds to determine the final app score.

<table>
<thead>
<tr>
<th>App Score components</th>
<th>User configured thresholds</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response time</td>
<td>Yes</td>
<td>The time interval between sending a request packet and receiving the first response packet from the service configured on the virtual server.</td>
</tr>
</tbody>
</table>
By default, all components are enabled. If you disable any component, Citrix App Delivery and Security service performs the final app score calculation only based on the selected components.

### Application usage and lean period analytics (Key metrics)

March 1, 2022

As an administrator, you must ensure how the application is getting utilized. The application key metrics can help you identify the application usage. Since the traffic range to the application is unpredictable, some unusual application performance deviations might occur for a specific duration. In such scenarios, as an administrator, you might want to view and analyze such sudden spikes, and ensure if any immediate troubleshoot is required. Citrix App Delivery and Security service provides necessary details for a specific duration (1-hour, 1-day, 1-week, and 1-month).

Navigate to **Analytics > Applications**, click an application, and select the **Key Metrics** tab. You can view the following key metrics in a graphical format:

- Response Time
- 5xx error
- Requests per second
- Throughput
- Client connections
- Server connections
- Data Volume

### Lean period analytics

As an administrator, you might want to schedule a downtime to the web application for a planned upgrade. A typical downtime for an application can be 1-hour, 2-hour, or 4-hour, depending upon the...
 requirement. The **Key Metrics** tab analyzes the traffic pattern and provides suggestions to view the lean period for the application. You can select the time from the list (1-hour, 2-hour, or 4-hour) that you want to plan for the downtime. After you select the time from the list, you can analyze the traffic for metrics such as **Total Requests**, **Throughput**, and **Data Volume**. You can select the right time to schedule for a downtime when the application usage is less. The following example is to analyze the downtime for the 1-hour duration.

The heatmap view indicates the application usage for the selected time duration. The darker the color (blue), indicates the application usage is higher.

The heatmap view also suggests the top 5 least period (1, 2, 3, 4, and 5) to plan for the application downtime.

1 – Indicates the first suggestion for Wednesday from 4 pm to 5 pm.
2 – Indicates the second suggestion for Thursday from 9 pm to 10 pm.
3 – Indicates the third suggestion for Sunday from 7 am to 8 pm.
4 – Indicates the fourth suggestion for Wednesday from 12 pm to 1 pm.
5 – Indicates the fifth suggestion for Monday from 7 am to 8 pm.

You can also select any other day and time to schedule a downtime, after analyzing the traffic for all other days.

Click **See Details** to view further detailed information. Click the **Total Requests**, **Throughput**, or **Data Volume** tab to view details for the top 5 least period and also for the other days.
Application usage analytics (Web Insight)

June 30, 2022

Application owners must have the ability to evaluate and visualize the complete application from the perspectives of performance and usage. When you click an application, apart from the existing application performance metrics, the Web Insight tab displays the metrics details that help you to:

- Understand your application usage.
- Correlate any performance deviations with the usage metrics.
Note

For each metric, you can view options that indicate maximum value and total value. For example:

- The maximum client network latency for the selected duration. Consider that you have the network latency for client 1 = 30 ms, client 2 = 15 ms, and client 3 = 3 ms. In this scenario, the Client Network Latency displays 30 ms.

- The total bandwidth consumed across all available clients/servers for the selected duration. Consider that you have the bandwidth consumption for client 1 = 30 MB, Client 2 = 45 MB, Client 3 = 40 MB. In this scenario, the Bandwidth displays (30 MB + 45 MB + 40 MB) = 115 MB.

The following are the metrics you can view from the Web Insight tab:

- **Application Metrics** – Displays the overall application metrics.
  - **Requests** – Displays the total request received by the application
  - **Bandwidth** – Displays the total data consumed by the application
  - **Response Time** – Displays the average response time from the application
  - **Client Network Latency** – Displays the average network latency from client to application
  - **Server Network Latency** – Displays the average network latency from server to application
  - **Server processing Time** – Displays the average processing time from the server. If you have enabled Self-heal slow application servers capability, you can view details if a faulty server is replaced. The following example shows that a faulty server is replaced between 9:41 am and 9:42 am in the Last 1 hour duration.
• **Clients** – Displays the insights for clients accessing the application:

![Clients](image)

- **Total Clients** – Displays the total clients accessing the application.
- **Client Network Latency** – Displays the network latency from client to Citrix ADC. Click the **Client Network Latency** tab to view:
  * **Client** – The client IP address.
  * **Client Network Latency (avg)** – The average network latency from the client.
  * **Requests** – The total requests from the client.
- **Render Time** – Displays the time taken to render the server response. Click the **Render Time** tab to view:
  * **Client** – The client IP address.
  * **Render Time (avg)** – The average render time from the client.
  * **Requests** – The total requests from the client.

• **Servers** – Displays the insights for servers accessing the application:
Citrix App Delivery and Security service

<table>
<thead>
<tr>
<th>Servers</th>
<th>Unique servers accessing the application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Servers</td>
<td>Server Network Latency</td>
</tr>
<tr>
<td>2</td>
<td>&lt;1 ms max</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server Network Latency tab to view:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server – The server IP address.</td>
</tr>
<tr>
<td>Server Network Latency (avg) – The average network latency from the server.</td>
</tr>
<tr>
<td>Requests – The total requests from the server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server Response Time tab to view:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server – The server IP address.</td>
</tr>
<tr>
<td>Response Time (avg) – The average response time from the server.</td>
</tr>
<tr>
<td>Requests – The total requests from the server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bandwidth tab to view:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server – The server IP address.</td>
</tr>
<tr>
<td>Bandwidth – The total bandwidth consumed from the server.</td>
</tr>
<tr>
<td>Requests – The total requests from the server.</td>
</tr>
</tbody>
</table>

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix App Delivery and Security service

- **Geo Locations** – Displays the insights for clients accessing the application from a particular location:
  
  ![Geo Location Table](image)
  
  - **Total locations** – Displays the total client locations accessing the application.
  - **Response Time** – Displays the response time from the client location.
  - **Bandwidth** – Displays the total bandwidth consumed by clients across all locations.
  - **Requests** – Displays the total requests from all client locations.

  Click each tab to view:
  
  * **Location** – The location name.
  * **Response Time** – The average response time from the client location.
  * **Bandwidth** – The bandwidth consumed from the client location.
  * **Requests** – The total requests from the client location.

- **URLs** – Displays the insights for URLs with high load and render time:

  ![URLs Table](image)
  
  - **Total URLs** – Displays the total URLs.

© 1999–2022 Citrix Systems, Inc. All rights reserved.
- **Load Time** – Displays the time taken for the URL to load. Click the **Load Time** tab to view:
  - **URL** – The URL name.
  - **Load Time (avg)** – The average time taken for the URL to load.
  - **Requests** – The total requests from the URL.

- **Render Time** – Displays the time taken for the URL to render and display. Click the **Render Time** tab to view:
  - **URL** – The URL name.
  - **Render Time (avg)** – The average time taken for the URL to render.
  - **Requests** – The total requests from the URL.

- **HTTP Response Status** – Displays the insights for a specific completed HTTP request.

- **Response Status** – Displays the response code such as 2xx, 4xx, 5xx, and so on.

- **Response Status Reason** – Displays the response reason such as internal server error, Not found, and so on.

- **No of Occurrences** – Displays the total number of occurrences.

- **Operating system** – Displays the insights for the OS accessing the application.
Citrix App Delivery and Security service

- **Requests** – Displays the total requests from each operating system.
- **Bandwidth** – Displays the total bandwidth consumed by each operating system.
- **Load Time** – Displays the total time taken from each operating system to load from the server.

- **Browsers** – Displays the insights for the browser types used by the clients to access the application.
  
  - **Requests** – Displays the total requests from each browser.
  - **Bandwidth** – Displays the total bandwidth consumed by each browser.
  - **Load Time** – Displays the total time taken for a browser to load from the server.

- **SSL Errors** – Displays the insights for the SSL errors from front-end server and back-end server.
Citrix App Delivery and Security service

- **Total Errors** – Displays the total SSL error occurrences.

- **Frontend** – Displays the total SSL errors from the front-end server. Click the Frontend tab to view the SSL error type and total occurrences.

- **Backend** – Displays the total SSL errors from the back-end server. Click the Backend tab to view the SSL error type and total occurrences.

- **SSL Usage** – Displays the insights for the SSL usage such as SSL certificates, protocols, Ciphers, and Key Strength.

- **Certificates** – Displays the total SSL certificates. Click the Certificates tab to view the certificate name and total hits.

- **Protocols** – Displays the total SSL protocols. Click the Protocols tab to view details with SSL/TSL protocol and total hits.

- **Ciphers** – Displays the total Ciphers. Click the Ciphers tab to view details for each cipher suite name and total hits.

- **Key Strength** – Displays the total key strength used in SSL certificates. Click the Key Strength tab to view details for each key strength and total hits.
Security

July 20, 2022

The Security tab enables you to visualize actionable violation details to protect applications from attacks. Navigate to Analytics > Security for a single-pane solution to:

- Visualize applications with full visibility into the WAF and Bot threat details.
- Access the application WAF and Bot violations.
- Take corrective actions to secure the applications.

The Security page has the following options:

- **Application Overview** – Displays an overview with applications that have total violations, total WAF and Bot violations, violation by country, and so on.
- **All Violations** – Displays the application security violation details.

For more information, see Security violation details.

Application overview

The Application Overview page displays applications with full visibility into the WAF and Bot violation details.
1 – Displays the total affected applications, total violations, and total WAF violations for the selected duration.

2 – Displays the top 5 applications based on the total violations occurred. Click View All to view all application details.

3 – Displays the top WAF violations based on the occurrences and the actions applied.

4 – Displays a geo map view that provides visibility from which locations the violations have occurred.

5 – Provides the application name that has the highest violations for the selected duration.

**Violation categories**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAF</td>
<td></td>
</tr>
<tr>
<td>Bot</td>
<td></td>
</tr>
<tr>
<td>Cookie Hijack</td>
<td></td>
</tr>
<tr>
<td>Scraper</td>
<td></td>
</tr>
</tbody>
</table>
## Citrix App Delivery and Security Service

<table>
<thead>
<tr>
<th>WAF</th>
<th>Bot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Overflow</td>
<td>Screenshot Creator</td>
</tr>
<tr>
<td>Cookie Consistency</td>
<td>Search Engine</td>
</tr>
<tr>
<td>HTML SQL Inject</td>
<td>Service Agent</td>
</tr>
<tr>
<td>Cross-site scripting</td>
<td>Site Monitor</td>
</tr>
<tr>
<td>IP Reputation</td>
<td>Speed Tester</td>
</tr>
<tr>
<td>Signature Violation</td>
<td>Tool</td>
</tr>
<tr>
<td></td>
<td>Uncategorized</td>
</tr>
<tr>
<td></td>
<td>Virus Scanner</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Scanner</td>
</tr>
<tr>
<td></td>
<td>DeviceFP Wait Exceeded</td>
</tr>
<tr>
<td></td>
<td>Invalid DeviceFP</td>
</tr>
<tr>
<td></td>
<td>Invalid Captcha Response</td>
</tr>
<tr>
<td></td>
<td>Captcha Attempts Exceeded</td>
</tr>
<tr>
<td></td>
<td>Valid Captcha Response</td>
</tr>
<tr>
<td></td>
<td>Captcha Client Muted</td>
</tr>
<tr>
<td></td>
<td>Captcha Wait Time Exceeded</td>
</tr>
<tr>
<td></td>
<td>Request Size Limit Exceeded</td>
</tr>
<tr>
<td></td>
<td>Rate Limit Exceeded</td>
</tr>
<tr>
<td></td>
<td>Block list (IP, subnet, policy expression)</td>
</tr>
<tr>
<td></td>
<td>Allow list (IP, subnet, policy expression)</td>
</tr>
<tr>
<td></td>
<td>Zero Pixel Request</td>
</tr>
<tr>
<td></td>
<td>Source IP</td>
</tr>
<tr>
<td></td>
<td>Host</td>
</tr>
<tr>
<td></td>
<td>Geo Location</td>
</tr>
<tr>
<td></td>
<td>URL</td>
</tr>
<tr>
<td></td>
<td>Crawler</td>
</tr>
<tr>
<td></td>
<td>Feed Fetcher</td>
</tr>
<tr>
<td></td>
<td>Link Checker</td>
</tr>
</tbody>
</table>

© 1999–2022 Citrix Systems, Inc. All rights reserved.
View WAF violation details

Click an application from the Top Applications or from the View All option to view the WAF details.

<table>
<thead>
<tr>
<th>APPLICATION</th>
<th>THREAT INDEX</th>
<th>TOTAL VIOLATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>stagingtest</td>
<td>7/7 High</td>
<td>5.8K</td>
</tr>
<tr>
<td>Dominoes-effect-Dominos-effect-svc-lb</td>
<td>7/7 High</td>
<td>27</td>
</tr>
<tr>
<td>Dominoes-effect-Dominos-effect-svc-lb_172.31.3...</td>
<td>7/7 High</td>
<td>7</td>
</tr>
</tbody>
</table>

The Security Overview page for the selected application is displayed. Under WAF, you can view:

- A graph view that indicates the total violations, threat index score, safety index score for the application.

- The violations based on types, severity, and actions applied.
Click **Logs** to view details based on the severity or action taken. You can also view the client IP address.

<table>
<thead>
<tr>
<th>TIME</th>
<th>VIOLATION TYPE</th>
<th>APPLICATION</th>
<th>SEVERITY</th>
<th>VIOLATION CATEGORY</th>
<th>CLIENT IP</th>
<th>ACTION TAKEN</th>
<th>REQUEST URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 Aug 06:31 am</td>
<td>Start URL</td>
<td>web_true_ip</td>
<td>Medium</td>
<td>Start URL</td>
<td>10.816.100.75</td>
<td>Blocked</td>
<td><a href="https://10.816.100.75">https://10.816.100.75</a>...</td>
</tr>
</tbody>
</table>

- **Transaction ID**: 2100064
- **Event Time**: 23 Aug 06:31 am - 24 Aug 06:31 am
- **Total Attacks**: 1
- **Country**: NA
- **Location**: Unknown
- **Violation Value**: NA
- **Found In**: Other Location
- **True Client IP**: 10.10.102.1
- **Violation Category**: NA
- **Region**: NA
- **Violation Name**: NA
- **Threat Index**: 5

• The violations affected on the application. Under **Violation Details**, you can view the affected violation details. Click each violation to view details such as:
  - **What Happened** – Indicates the total occurrences and the last occurred date and time.
  - **Event Details** – Displays a geo map that indicates the client IP and other violation details such as violation type, client IP, location, and so on.

©1999‒2022 Citrix Systems, Inc. All rights reserved.
View bot violation details

From the **Bot** tab, click an application from the Top Applications or from the **View All** option to view the bot details.

The **Security Overview** page for the selected application is displayed. Under **Bot**, you can view:

- A graph indicating total bots, total bad bots, total good bots, and total ratio between human users and bots accessing the application.

- The violations based on the bot types, severity, and actions applied.

Click **Logs** to view details based on severity or actions taken. If a detected bot is a Signature type bot, you can view more details such as Bot developer and Signature ID. The Signature ID enables you to identify if the detected bot is a good bot or a bad bot.
• The violations affected on the application. Under Violation Details, you can view the affected violation details. Click each violation to view details such as:

  – **What Happened** – Indicates the total occurrences and the last occurred date and time.

  – **Event Details** – Displays a geo map that indicates the client IP and other violation details such as violation type, client IP, location, and so on.
All Violations

In the All Violations page, you can view:

- The total WAF and bot violations affected across all applications.

  ![Bot violations and WAF violations](image)

- The total applications affected, and top violations based on the total occurrences.
• Violation details. For each violation, Citrix App Delivery and Security service monitors the behavior for a specific time duration and detects violations for unusual behaviors. You can click the tab to view the violation details. You can view details such as:
  - The total occurrences, last occurred, and total applications affected.
  - Under event details, you can view:
    * The affected application name. You can also select the application from the list if two or more applications are affected with violations.
    * The Threat Index score (For WAF violations).
    * A geo map indicating the locations that the violations have occurred.
    * Violation details such as violation time, violation type, action taken, location, and so on (For WAF violations).
    * Violation details such as violation time, client IP, bot type, Action taken, and Location (For bot violations).

Integration with Splunk

June 30, 2022

You can integrate Citrix App Delivery and Security with Splunk to view analytics for WAF and Bot violations in your Splunk dashboard. Splunk add-on enables you to:

• Combine all other external data sources.
• Provide greater visibility of analytics in a centralized place.

Citrix App Delivery and Security collects Bot and WAF events and sends to Splunk periodically. The Splunk Common Information Model (CIM) add-on converts the events to CIM compatible data. As an
Citrix App Delivery and Security service

administrator, using the CIM compatible data, you can view the WAF and Bot violations in the Splunk dashboard.

**Prerequisites**

For Splunk integration, you must:

- Set up the global setting
- Set up the HTTP Event Collector endpoint in Splunk
- Install the Splunk Common Information Model (CIM) add-on
- Install the Citrix CIM normalizer
- Add the Splunk HTTP collector and token details

**Set up the global setting**

1. Log on to Splunk.
2. Navigate to Settings > Data Inputs > HTTP event collector
   The HTTP event collector page is displayed.
3. Click Global Settings
4. Specify the following parameters and click Save.
   
   **Note:**
   By default, the HTTP Port Number indicates the default port. If you have any other preferred port number, you can specify the required port number.

**Set up the HTTP Event Collector endpoint in Splunk**

1. Log on to Splunk.
2. Navigate to Settings > Data Inputs > HTTP event collector
   The HTTP event collector page is displayed.
3. Click New Token.
4. Specify the following:
   a) **Name**: Specify a name of your choice.
   b) **Source name override (optional)**: If you set a value, it overrides the source value for HTTP event collector.
   c) **Description (optional)**: Specify a description.
d) **Output Group (optional):** By default, this option is selected as *None*.

e) **Enable indexer acknowledgement:** By default, this option is not selected.

f) Click *Next*.

g) In the **Input Settings** page, specify the **Source Type**, **App context**, **Index**, and then click **Review**.

h) Review if everything you have specified is correct and then click **Submit**.

A token gets generated. You must use this token when you add details in Citrix App Delivery and Security.

**Install the Splunk Common Information Model**

In Splunk, you must install the Splunk CIM to ensure that the data are populated in the dashboard.

1. Log on to Splunk.
2. Navigate to **Apps > Find More Apps**.
3. Type **CIM** in the search bar and press **Enter** to get the **Splunk Common Information Model** (*CIM*) add-on, and click **Install**.

**Install the Citrix CIM normalizer**

After you install the Splunk CIM, you must install the Citrix CIM normalizer to transform the events into the Splunk CIM.

1. Log on to Citrix downloads page and download the **Citrix CIM add-on for Splunk**
2. In the Splunk portal, navigate to **Apps > Manage Apps**.
3. Click **Install App from file**.
4. Upload the **.spl** or **.tgz** file and click **Upload**.

You receive a notification message on the **Apps** page that the add-on is installed.

**Add the Splunk HTTP collector and token details**

After you generate a token, you must add details in Citrix App Delivery and Security to integrate with Splunk.

1. Log on to Citrix App Delivery and Security.
2. Navigate to **Analytics** and click the **Splunk Log** tab.

The **Subscription** page is displayed.
3. Click Add.

4. In the **Select features to subscribe** tab enables you to select the features that you want to export and click Next.

   - **Realtime Export** - The selected violations are exported to Splunk immediately.
   - **Periodic Export** - The selected violations are exported to Splunk based on the duration you select.

5. In the **Specify export configuration** tab:
   a) **End Point Type** – Select Splunk from the list.
   b) **End Point** – Specify the Splunk end point details. The end point must be in the `https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event` format.

   **Note:**
   It is recommended to use HTTPS for security reasons.
   - **SPLUNK_PUBLIC_IP** – A valid IP address configured for Splunk.
   - **SPLUNK_HEC_PORT** – Denotes the port number that you have specified during the HTTP event endpoint configuration. The default port number is 8088.
   - **Services/collector/event** – Denotes the path for the HEC application.
   c) **Authentication token** – Copy and paste the authentication token from the Splunk page.
   d) Click Next.

6. In the **Subscribe** page:
   a) **Export Frequency** – Select Daily or Hourly from the list. Based on the selection, Citrix App Delivery and Security exports the details to Splunk.
Citrix App Delivery and Security service

Note
Applicable only if you have selected violations in Periodic Export.

b) Subscription Name – Specify a name of your choice and select Enable Notifications.

c) Click Submit.

Note:
- When you configure with Periodic Export option for the first time, the selected features data get pushed to Splunk immediately. The next export frequency happens based on your selection (daily or hourly).
- When you configure with Realtime Export option for the first time, the selected features data pushed to Splunk immediately as soon as the violations are detected in Citrix App Delivery and Security.

After you configure, you can view details in the Subscriptions page.
Select the subscription name and click View Logs to view details such as subscription created, modified, deleted, data exported, and so on.

Verify details in Splunk

After you add details in Citrix App Delivery and Security, you can verify if Splunk receives the events.

1. From the Splunk home page, click Search & Reporting.
2. In the search bar, type the details in the search bar, select the duration from the list, and click the search icon or press Enter. For example, you can type sourcetype="bot" or sourcetype ="waf" to check the details.

The following search result is an example for a WAF violation:
The following search result is for a Bot violation:

Access Pivot details

You must identify the Data Model type to see the pivot details. For example, the Splunk add-on converts the WAF and Bot events in CIM format, with the closest data model type such as Alert and Intrusion Detection.

To access the events in Splunk:

1. Navigate to Settings > Data Models.
2. Identify the Intrusion Detection data model and click Pivot.
3. Select a Dataset. In the following example, the IDS Attacks option is selected.

The total count of IDS Attacks is displayed.

You can also click the + button to add more details to the table. The following example displays the details based on severity, category, and signature ID:

**Splunk dashboard**

Using a dashboard, you can view details of WAF and Bot violation analytics with panels such as charts, tables, lists, and so on. You can configure a:

- Dashboard with applications that use the CIM compatible data.
- Custom dashboard that pulls data from the CIM data models.

Depending upon your choice, you can create the dashboard. For more information, see the About dashboard section in Splunk documentation.

**Web Insight dashboard**

July 19, 2022

The Web Insight dashboard provides visibility into detailed metrics for web applications and clients. This Web Insight enables you to evaluate and visualize the complete application from the perspectives of performance and usage together. As an administrator, you can view Web Insight for:

- An application. Navigate to Analytics > Applications, click an application, and select Web Insight tab to view the detailed metrics. For more information, see Application usage analytics.
- All applications. Navigate to Analytics > Web Insight and click each tab (Applications and Clients) to view the following metrics:

<table>
<thead>
<tr>
<th>Applications</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Clients</td>
</tr>
<tr>
<td>Servers</td>
<td>Geo Locations</td>
</tr>
<tr>
<td>Domains</td>
<td>HTTP Request Methods</td>
</tr>
<tr>
<td>Geo Locations</td>
<td>HTTP Response Status</td>
</tr>
<tr>
<td>URLs</td>
<td>URLs</td>
</tr>
<tr>
<td>HTTP Request Methods</td>
<td>Operating System</td>
</tr>
<tr>
<td>HTTP Response Status</td>
<td>Browsers</td>
</tr>
<tr>
<td>Applications</td>
<td>Clients</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SSL Errors</td>
<td>SSL Errors</td>
</tr>
<tr>
<td>SSL Usage</td>
<td>SSL Usage</td>
</tr>
</tbody>
</table>
Citrix App Delivery and Security service

In each metric, you can view the top 5 results based on the selected metric. For example, if you click the **Requests** tab under **Servers**, the top 5 results display based on the highest requests rates. The **See more** option enables you to view all results.

You can click to drill down further to analyze the issue and take troubleshooting actions faster.

**Use case**

Consider that you want to analyze the server network latency for 1-month time duration and take a decision whether to scale up or scale down the production environment. To analyze:

1. Select **Last 1 Month** from the list and from the **Applications** tab, scroll down to **Servers**, and click a server.

2. Click **Server Network Latency** tab to analyze the latency.

The average latency indicates 10.01 s and from the graph, you can analyze that the server network latency for the last 1 month seems to be high. As an administrator, you can take a decision to scale up the production environment.
Multi-site application analytics

July 12, 2022

After you configure and deploy the multi-site applications, you can view analytics for the multi-site applications. For more information on how to configure multi-site applications, see configure the multi-site applications. The analytics for multi-site applications enable you to:

- Visualize an overview of all configured applications with details such as status, total requests, and stickiness rate.
- Drill down an application and view key metrics such as **Total Requests**, **Stickiness hit ratio**, and **Health** for the selected application.
- View the application performance based on its each configured site level.
- Understand the configured sites’ performance for the selected time duration.

Navigate to Analytics, click the Multi-Site Applications tab, and select the duration from the list to view the dashboard.

Dashboard overview

1 – Enables you to select the duration from the list to view details for a specific duration.

2 – Enables you to apply filters and view applications. You can apply filters for:

- **Multi-site Application State** – Enables you to view application based on the current application status such as **UP**, **Out of Service**, **Review**, and **Not Applicable**. By default, you can view applications that are in **Up**, **Out Of Service**, and **Review** status. To view applications that are in **Not Applicable** status, you must select the **Not Applicable** option.
  - **UP** – All configured sites are up and running
  - **Out of Service** – All configured sites are down and not accessible
Citrix App Delivery and Security service

- **Review** – One or more configured sites is down and not accessible
- **Not Applicable** – The multi-site application is configured, but not deployed

- **Total Requests** – A histogram that displays the total number of requests received by the applications. Click the histogram or drag to select the range to apply filter and view applications.
- **Stickiness Hit Ratio** - A histogram that displays the total percentage of successful or cached requests received by the applications.

3 – Enables you to view the overview of the applications based on the selected time duration and filters applied (if any).

4 - A search bar that enables you to filter applications based on the application names.

**Key Metrics**

Click an application from the table to view the application key metrics. Under **Summary**, you can view the status of the application, including its sites for the selected duration.

In this page, you can:

- Select the duration from the list and view details
- Select the site from the location list and view details
- Analyze the sites performance for the selected duration.
- Visualize how the site has performed for the selected duration.
  - **Healthy** – Indicates both application and its sites are up
  - **Degraded** – Indicates the application is intermittently available
  - **Unhealthy** – Indicates the site is down and unavailable
  - **Maintenance** – Indicates the site is in maintenance mode. For more information on setting a site in maintenance mode, see [Maintenance mode](#).
**Citrix App Delivery and Security service**

- **Not Deployed** – Indicates the applications that are configured, but not yet deployed.

- **Time Slice** – The duration for which the site performance status is monitored and updated. Depending upon the selected duration, the time slice period changes.

  For example, if you select **Last 1 Day** from the list, the time slice for the selected duration is 12 minutes. This means, each rectangle displayed in the chart represents a 12-minute duration. For every 12 minutes, the site performance is monitored and the status (Healthy, Degraded, Unhealthy, and Maintenance) is updated.

  • Select the site from the list and monitor only the selected site.

You can view the following key metrics in a graphical format for the selected application:

- **Request Rate** – The requests received by the application for the selected duration.

- **Health** – The health status of the application for the selected duration.

- **Stickiness Hit Ratio** – The successfully cached requests received by the application for the selected duration.

- **Geo locations** – Displays a geo map that indicates the top 5 locations based on the number of requests from each location. Click **See more locations** to view details for all locations.
Under Request Rate and Stickiness Hit Ratio, you can view:

- **Max** – The highest value for the selected duration. For example, the max value for the total requests in the key metrics image represents 1.27/sec. This value represents the highest request per second received during the selected duration.

- **Average** – The average value for the selected duration.

Under Health, you can view:

- **Max** – The total number of healthy sites for the selected duration. If all sites are healthy for a specific duration, it indicates 100% as the maximum.

- **Average** – The average percentage of healthy sites for the selected duration. The average % is calculated based on the healthy sites and unhealthy sites for the selected duration.

Under Geo Location, you can view:

- **Locations** – Indicates the total locations.

- **Requests** – Indicates the total requests across all locations for the selected duration.

**Manage SSL certificates**

March 10, 2022

An SSL certificate is an essential part of any SSL transaction. You might need multiple certificates for different apps and domains. Using the Citrix App Delivery and Security service, you can add certificates to a central repository instead of uploading a certificate each time you create an application.
Later, you can simply select a certificate to use with an app while configuring the app. You can select one or more certificates to bind to an endpoint. The same certificate can be used by multiple apps.

You can add certificates to a certificate chain and the Citrix App Delivery and Security service automatically links the certificates based on the issuer and subject fields in the certificates.

The following options for uploading certificates are available:

- Upload a single file also known as a certificate bundle. This file contains all the certificates and key that form part of the certificate chain.
- Upload two files – the server certificate file and the certificate chain file.
- Multiple files – Server certificate file, each of the intermediate certificates in a separate file, and the root certificate file.

The central repository for the SSL certificates in the Citrix App Delivery and Security service is called the SSL Certificate Manager. Your SSL certificates are safely stored here. You can upload your certificate files here and attach them to your applications.

**Add an SSL certificate**

1. Navigate to **SSL Certificate Manager** and click **Create SSL Certificate**.

2. In the **Create SSL Certificate** page, specify the following parameters:
   - **Certificate Name**: Name for the certificate. Must contain only ASCII alphanumeric, underscore, and hyphen characters. Cannot be changed after the certificate is created. Max length = 30 characters.
   - **Certificate File**: Upload the certificate file from your local computer.
   - **Key File**: Upload the key file from your local computer.
   - **Key Password (if required)**: If you have an encrypted private key in PEM format, type the passphrase that was used to encrypt the private key.
   - To add the certificate to the chain, select **Add certificate in certificate chain**. Select an intermediate certificate or a certificate bundle to upload to the certificate chain. Click **Add**.

3. Click **Create**.
Modify or delete an SSL certificate

You can delete or update the certificate and key file. You can also update the certificate in the certificate chain.

To update a certificate

1. Navigate to SSL Certificate Manager.
2. In the SSL Certificate page, click the Edit icon for the certificate that you want to update.
3. In the Update SSL Certificate page, select one or both of the following and upload the file.
To delete a certificate

1. Navigate to **SSL Certificate Manager**.
2. In the **SSL Certificate** page, click the **Delete** icon for the certificate that you want to delete.
3. When prompted, click **Yes, Delete**.

**Monitor self-healing**

June 21, 2022

The Citrix App Delivery and Security Service – Citrix Managed edition, offers self-healing capability for the application server. The self-healing capability provides deep application analytics with improved application experience and security.

With the self-healing capability:

- You can automatically detect, remediate, and replace the defective server with a healthy server whenever the performance of an application server degrades or starts to malfunction.
- You can automatically detect the security attacks and take remediation actions.
Citrix App Delivery and Security service

If an anomaly is detected in one of the instances of an application, it generates an alert and can automatically take remediation actions. The detected anomalies and corrective steps are logged inside the Action History.

The following use cases are supported as part of the self-healing capability:

- **Automatically replace Slow Server**: In a stack of applications running as a back-end server in an Autoscale group, if one of the instances goes faulty. And if that instance starts responding slowly based on the response time. Then, the self-healing feature enables detecting the faulty server and replacing the faulty server with the healthy server automatically. For more information, see Create Services.

- **Block past offenders**: Enables you to check and send alerts if the client IPs are causing excessive AppSec violations in the last 20 minutes. For more information, see SQL injection and Cross-site scripting.

**Action History**: Enables you to view the actions that are taken in the context of self-healing. For more information, see Action History.

**Prerequisites**

Before accessing the action history tile, you must complete the following preliminary steps:

- Create a Citrix cloud access profile.
- Create an application environment.

For more information, see Deliver a modern application.

**Action History**

The action history functionality enables you to view anomalous events that have been detected and the corresponding corrective actions that are taken as part of self-healing.

For example,

- The action history view enables you to check if one of the services that comprise an Autoscale group is slow compared to the rest of the services. If an automatic replacement of slow servers is enabled, then the respective action shows up in this history.

- The action history view displays the event where the client IPs have been causing excessive AppSec violations. If an automatic remediation is enabled, then the action history view displays the details of when the offending client IP was blocked.

All the actions are taken automatically. You can view the details of the actions taken in the Action History.
Overview

When an Action takes place, we see a log entry in the Action History. The action history view displays the records in a table with the following details:

- The time of action.
- The action that was taken.
- The event that leads to the trigger of an action.
- The application name or network function on which the corresponding anomaly event happens.

You can filter the action history view based on the following parameters:

- The time interval at which the actions are run.
- The application name on which the actions are run.
- The action taken.
- The network function on which the actions are run.

Actions

There are two types of Actions:

- Log only actions: You can enable log only type of actions. These entries are the records registered by the application when an anomaly is detected.

- Log and Remediation actions: Along with logs, you can also configure the CADS service to automatically correct the anomaly. These entries are the corrective actions taken by the application to recover from the anomaly. For example, if there is a slow-server anomaly, the corrective action is to replace the slow server.

You can start with the log only actions, and if you want to enable automatic remediation action, you can switch the actions from log only actions to log and remediation actions based on the requirement.

Using the Action History

To access the integrated Action History in the CADS service application:

1. Sign in the CADS service application.
2. In the left Navigation pane, click Action History.

Sort, filter, and search logs in the Action History

Use the search feature to view information about the specific actions. The filters can be applied to get a more focused view of the alerts based on the time interval.
• Sort the data by selecting the required columns.
  – Click the Add icon at the top right of the table header to add or remove columns. This launches the Add / Remove columns modal dialog.
  – To remove a column, unselect the check box of the required column listed under Current Columns pane in the Add / Remove columns modal dialog. Click Update. The removed column now appears under the Add Columns pane.
  – To add a removed column, select the check box of the required column listed under the Add Columns pane in the Add / Remove columns modal dialog. Click Update. The added column now appears under the Current Columns pane.

• Sort the data by using the time interval drop-down list next to the search box.
The available options are PRESET TIME and CUSTOM.
  – You can sort the data to view the data in the PRESET TIME.
    Under PRESET TIME, the available options are,
    * Last 1 Hour (1H): Displays the data for the previous one hour.
    * Last 12 Hours (12H): Displays the data for the previous 12 hours.
    * Last 1 Day (1D): Displays the data for the previous day.
    * Last 1 Week (1W): Displays the data for the previous week.
    * Last 1 Month (1M): Displays the data for the previous month.
  – You can also sort the data by customizing the time interval under CUSTOM.
    You can choose the required date and time range. Click From to select the starting range and click To for selecting the ending range of the date and time.

• The table might spill over to many pages. You can select the number of row entries in a page from the drop-down list at the bottom of the table.

• To perform advanced search, you can use filters such as Action-Taken, and Application-Name in the search box to view the specific data.
  – Click the search box and choose the required option, Action-Taken, or Application-Name
  – Select the suitable operator for the chosen option. The available operators are,
    = equals to some value
    ~ contains same value
  – You can combine the search query by using the logical operators: AND (Requires both to be true). The AND logical operator requires both the values to be true.

**Action History View**

The following parameters are displayed in the action history table view:
TIME:
This field displays the time at which the action was taken. Select the Action log list based on the specific duration.

ACTION TAKEN:
This field displays the action that was taken because of an alert. For example, replace a slow server or log.

APPLICATION NAME:
This field displays the name of the application on which the action was taken.

NETWORK FUNCTION:
This field displays the name of the network function on which the block, or unblock IP actions were taken.

ALERT TYPE:
This field displays the type of alert.

The following types of alerts are supported in CADS service:
- ads-slow-server
- ads-appsec-offending-client

ALERT MESSAGE:
This field displays information about the alert type, the alert, and the action that was taken.
API definitions in the Citrix App Delivery and Security service

June 2, 2022

An API definition allows you to describe API resources and the operations allowed on these API resources. After the API definition is created, you can use it while configuring a new application and also in application settings such as, content routes for an end point, content transform, and security protection. The API resource paths are available as a filter condition. For more information, see Add endpoints. Select the API definitions while creating a modern application. For more information, see Deliver a modern application.

Create an API definition

1. Navigate to API Definitions > Add API.
2. Type a name for the API definition. Specify the following parameters:
   - **Title** - Title for the API definition.
   - **Version** - API version.
   - **Base Path** - The base path for the API definition. The base path is appended as a prefix to the API resource.
   - **Host** - The FQDN or IP address where the API service is located.
   - **API Resources** – Specify the methods and paths to the API resources.
3. Click Create.
Manage an API definition

The API Definitions page lists the uploaded definition. The following fields are displayed.

- Name
- Title
- Version
- Actions

In the Actions column, click the pencil icon to edit the API definition. Click the trash can icon to delete the API definition.
View audit log

June 1, 2022

The Citrix App Delivery and Security Service – Citrix Managed, offers audit log capability for the applications and environments. The audit log capability enables you to view the events or logs generated by the actions such as creation, deletion, modification, deployment, and Un deployment of an application or environment.

You can use the CADS service to track all events on Citrix environments. These messages can help you manage and monitor your application.

You can use filters to search the audit log messages. The filters help you to narrow down your results and find exactly what you are looking for and in real time.

With the audit log capability:

- You can track the activities and login information.
- You can filter the queries based on the required parameters and get the refined results of the action.

Prerequisites

Before accessing the audit log, you must complete the following preliminary steps:

- Create a Citrix cloud access profile.
- Create an application environment.

For more information, see Deliver a modern application.

Overview

When an action is done, an event is generated, we see a log entry in the Audit Log. The Audit Log view displays the records in a table with the following details:

- The time of action.
• The doer of the action.
• The action that was taken on a particular resource.
• The particular action that was taken.
• The status of the action.
• The message showing the details of the action.

You can filter the Audit Log view based on the following parameters:

• The time interval at which the actions are run.
• The particular resource name on which the actions are run.
• The resource on which the actions are run.
• The operation that specifies the particular action run on the resource.
• The event source from which the events are generated.

**Using the Audit Log**

To access the integrated Audit Log in the CADS service application:

1. Sign in to the CADS service application.
2. In the left Navigation pane, click the **Audit Log**.

**Sort, Filter, and Search logs in the Audit Log**

Use the search feature to view information about the specific actions. The filters can be applied to get a more focused view of the actions based on the time interval.

• Sort the data by selecting the required columns.
• Click the **Add** icon at the top right of the table header to add or remove columns. This launches the Add / Remove columns modal dialog.
  - To remove a column, unselect the checkbox of the required column listed under **Current Columns** pane in the **Add / Remove columns** modal dialog. Click **Update**. The removed column now appears under **Add Columns** pane.
  - To add a removed column, select the checkbox of the required column listed under **Add Columns** pane in the **Add / Remove columns** modal dialog. Click **Update**. The added column now appears under **Current Columns** pane.
• Sort the data by using the time interval drop-down list next to the search box. By default, the **Last 1 Week** option is set. The available options are **PRESET TIME** and **CUSTOM**.
• You can sort the data to view the data in the **PRESSET TIME**.

Under **PRESSET TIME**, the available options are,

- **Last 1 Hour (1H)**, displays the data for the previous one hour.
- **Last 12 Hours (12H)**, displays the data for the previous 12 hours.
- **Last 1 Day (1D)**, displays the data for the previous day.
- **Last 1 Week (1W)**, displays the data for the previous week.
- **Last 1 Month (1M)**, displays the data for the previous month.

• You can also sort the data by customizing the time interval under **CUSTOM**. You can choose the required date and time range. Click **From** to select the starting range and click **To** for selecting the ending range of the date and time.

• To do advanced search, you can use filters such as Event-source, Operation, Resource, and Resource name in the search box to view the specific data.

  - Click the search box and choose the required option.
  - Select the suitable operator for the chosen option. The available operators are,

    - “=” equals to some value.

  - You can combine the search query by using the following logical operators:

    - **AND**. The **AND** logical operator requires both the values to be true.

---

**Audit Log View**

The following parameters are displayed in the Audit Log table view:

**TIME:**

![Audit Log Table View](image)
Citrix App Delivery and Security service

This field displays the time at which the action was taken. You can sort the audit log list based on the specific duration.

**USER:**
This field displays the details about the doer of the action. For example, user id, user name, or email id.

**RESOURCE NAME:**
This field displays the name of the resource on which the action is run.

**OPERATION:**
This field displays the type of operation done because of the action.

The following types of operations are supported in the CADS service:

- **CREATE.** For example, when an action is started to create an environment.
- **DELETE.** For example, when an action is started to delete an environment.
- **DEPLOY.** For example, when an action is started to deploy an environment.

**STATE:**
This field displays the status of the action.

The following types of states are supported in the CADS service:

- **STARTED.** For example, when an action is started to deploy an environment.
- **COMPLETED.** For example, when an action is started to create an environment.
- **FAILED.** For example, when an started action is not completed during the creation of an environment.

**MESSAGE:**
This field displays information about the particular action.

Click **View more** to get more details on the action.
How-to articles

March 30, 2022

Citrix App Delivery and Security service – Citrix Managed provides an outcome-focused model that allows you to specify the generic, functional, and business intent of your application deployment.

CADS service "How-to articles" are simple, relevant, and easy to implement articles on the features available with the service. The following articles are a step-by-step guide for using CADS service features to secure your application and to keep your data confidential.

Get an A+ security rating for your application in the Qualys SSL Lab test

Rewrite HTTP headers for rewrite content transform

Get an A+ security rating for your application in the Qualys SSL lab test

March 22, 2022

Using insecure ciphers and protocols for transactions can impact the privacy, data integrity, and security of the users accessing your applications. Your application might be compromised if the correct settings are not in place.
How does the Citrix App Delivery and Security service help in getting an A+ security rating by Qualys SSL Labs?

SSL keeps your connection secure and prevents anyone from reading or modifying information while it is transferred between the two systems. Qualys SSL Labs rates the applications based on the ciphers, protocols, and other SSL settings. If your application servers meet the required settings, they are given an A+ rating. For more information, see SSL Server Test.

As an application owner, you can choose to secure your application by selecting **A+ Security**. When you select this option, the service selects the required ciphers, certificates, key exchange algorithms, and protocols required to get an A+ rating on your back-end application servers. The service adds this setting using SSL policies.

**Create an SSL policy with A+ security intent using the GUI**

Start the **Create Application** workflow. After specifying the application details and creating services, add endpoints.

For more information about specifying application details, see **Create an application**. For more information about creating services, see **Create services**.

For more information about creating an endpoint, see **Add endpoint**.

1. Navigate to **Endpoints**.
2. Click **Add Endpoint**.
3. Modify an existing endpoint or click **Create Endpoint**.
4. Click **Add SSL Policy**.
5. Type a name for the policy and select **A+ Security**.

6. Click **Create**.
An SSL policy is added with the A+ security intent to secure your application.

**Create an SSL policy with A+ security intent using the API**

Send the API to the following endpoint.

<table>
<thead>
<tr>
<th>Method</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>/adcaas/nitro/v1/config/network_functions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Header</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>application/json</td>
</tr>
<tr>
<td>Cookie</td>
<td>SESSID=</td>
</tr>
<tr>
<td>ADS_SERVICE_TYPE</td>
<td>INTENT</td>
</tr>
</tbody>
</table>

The following snippet is an example of the API payload.
Example response

```json
{
  "network_functions": [
    {
      "name": "DemoSSLPolicy",
      "type": "ssl_frontend",
      "ssl_frontend_params": {
        "aplussecurity": true,
        "ciphers": [],
        "tls1": false,
        "tls11": false,
        "tls12": false,
        "tls13": false
      }
    }
  ]
}
```
Use this policy while creating an application as required.

**Create an application with SSL policy for A+ security intent using the API**

The following API creates an application with the specified:

- Environment
- Services
- Endpoints including a valid certificate
- Load balancing configuration

Send the API to the following endpoint.

<table>
<thead>
<tr>
<th>Method</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>/adcaas/nitro/v1/config/applications</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Header</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>application/json</td>
</tr>
<tr>
<td>Cookie</td>
<td>SESSID=</td>
</tr>
<tr>
<td>ADS_SERVICE_TYPE</td>
<td>INTENT</td>
</tr>
</tbody>
</table>

The following snippet is an example of the API payload.

```json
{
  "applications":
  {
    "type": "ssl_frontend",
    "updated_at": "2021-12-10T10:35:50Z"
  }
}
```
"edition": "premium",
"name": "DemoAppHTTPS",
"type": "aws",
"environment": {
  "id": "3b6ed423c509404915c57a06ee676e6b"
}

"endpoints": [
  {
    "name": "DemoHTTPSEndpoint",
    "endpoint_type": "External",
    "fqdns": [],
    "fqdn_auto_allocated": true,
    "listeners": [
      {
        "port": 443,
        "protocol": "HTTPS",
        "certificates": [
          "3bf39d58-7fcc-49b8-b050-a230681c97ac"
        ],
        "ssl_network_function": {
          "name": "DemoSSLPolicy"
        },
        "is_https_redirect": true,
        "redirect_port": 80
      }
    ]
  },
  {
    "name": "DemoLB",
    "type": "lb",
    "lb_params": {
      "algorithm": "ROUND_ROBIN"
    }
  }
]
"stickinessType": "SOURCE_IP"
}
}

"name": "DemoSSLPolicy",
"type": "ssl_frontend",
"ssl_frontend_params": {
  "aplussecurity": true,
  "ciphers": [],
  "tls1": false,
  "tls11": false,
  "tls12": false,
  "tls13": false
}
}

"application_services": [
{
  "name": "DemoAppSvc",
  "protocol": "HTTPS",
  "port": 443,
  "app_server_type": "servers",
  "aws AutoscaleGroup": "",
  "aws Instances": [],
  "servers": [
  {
    "type": "IPAddress",
    "value": "2.2.2.2"
  }
  ],
  "network_functions": [
  {
    "name": "DemoLB",
    "type": "lb"
  }
  ]}
Example response

```json
{
    "applications": [
        {
            "application_endpoints": [
                {
                    "default_route": "DemoAppSvc",
                    "endpoint_id": "fac30d4b980deccb291f97cdfd7d63f2",
                    "endpoint_name": "DemoHTTPSEndpoint",
                    "id": "968d6af0fc0d50a5b30cf99fe19ddf20",
                    "routes": []
                }
            ],
            "application_services": [
                {
                    "app_server_type": "servers",
```
"id": "0ad8677bf3dffe9bce95b20bd48818ed",
"name": "DemoAppSvc",
"network_functions": [
{
  "name": "DemoLB",
  "type": "lb"
}
],
"port": 443,
"protocol": "HTTPS",
"servers": [
{
  "type": "IPAddress",
  "value": "192.0.2.2"
}
],
"slow_server_settings": {
  "action": "detect"
},
"created_at": "2021-12-10T11:09:42Z",
"deployed_at": null,
"edition": "premium",
"environment": {
  "cloud": "aws",
  "id": "3b6ed423c509404915c57a06ee675e6b",
  "name": "DemoEnv"
},
"id": "501d0fa420bbcd6d079cbbda7faf6e12",
"job_id": null,
"name": "DemoAppHTTPS",
"status": "INDRAFT",
"type": "aws",
"updated_at": "2021-12-10T11:09:42Z"}
Rewrite HTTP headers for rewrite content transform

July 19, 2022

Citrix App Delivery and Security service – Citrix Managed edition, content transform feature enables rewrite of information in requests or responses from the client or the server. Rewriting provides access to the requested content without showing unnecessary details about the website’s actual configuration. Following are a few scenarios in which the rewrite is useful:

- **Improve Security.** You can rewrite all the `http://` to `https://` in the response body.
- **Retain visitor on the website.** You can display a custom 404 error page instead of the default 404 error page. You can display the website home page or a site map instead of the default 404 error page. This helps retain visitors on the website even when the 404 error exists.
- **Redirect visitors.** You can use rewrite to redirect the website instance to a different location while using the old URL.
- **Publish SEO and user-friendly URLs.** When a page on a site has a complicated or a lengthy URL, you can rewrite it to a simple, easy-to-remember URL, also referred to as the ‘cool URL’.
- **Set default URLs.** You can append the default page name to the URL of a website. For example, if the default page of a company’s website is `http://www.example.com/index.php`, and the user enters `example.com` in the browser address bar, you can rewrite the URL to always point to `example.com/index.php`.

When you enable the rewrite feature, the CADS service can modify the headers and body of the HTTP requests and responses.

In the HTTP traffic, you can take the following actions:

- Modify the URL of a request
- Add, modify, or delete headers
- Add, replace, or delete any specific string within the body or headers.

Here is a use case that explains configuring the content transform in the CADS service by defining the rewrite rule and action to remove the HTTP header and client IP from the request to keep the customer data confidential.
**Problem Statement**

A mid-sized manufacturing company uses its website to handle a large portion of its sales, deliveries, and customer support. The manufacturing company has two domains: example.com, for its website and email to customers, and example.net, for its intranet. Customers use the website to place orders, request quotes, research products, and customer service. The company can take specific action on HTTP requests based on the criteria such as user location, header, IP address, and while doing so, the website must have no performance degradation and keep customer data confidential.

**How does CADS service content transform feature solve the problem?**

With the CADS service content transform feature, you can deliver an application configuring content transform to do specific tasks. The service balances the website load and manages traffic to-and-from the company's web servers.

Content transform enables you to respond to HTTP requests depending on the requirement. It examines the request from the client or response from the server and forwards the request depending on the applicable rule. Also, it evaluates the data and applies one or more actions based on the set rule.

**Example**

The following examples are seen in the server room of the Example Inc., a mid-sized manufacturing company that uses its website to handle a substantial portion of its sales, deliveries, and customer support. The company therefore has several web servers.

The company’s system administrators use the rewrite features to do the tasks.

**Scenario 1: Remove an HTTP Header in request**

Example Inc. wants to remove the old x-forwarded-for and client-IP HTTP headers from incoming requests, so that only the x-forwarded-for headers are the ones added by the local server. This configuration can be done using the content transform.

The example below explains how to set up configuration in the CADS service. The procedures are shortened assuming that you are familiar with the basics of creating rewrite rules.

For more detailed information about creating rewrite rules, see Add content transform.

In the **Create Rewrite Rule** dialog box, create two rules one for x-forwarded-for and another for client-IP

- Create the rewrite rule for x-forwarded-for
  
  **Rule Name:** act_del_xfor

- Check if the following condition exists:
HTTP HEADER: HTTP Request Header

Operator: Exists

Value: x-forwarded-for

• Create a rewrite action with the following description:

Type: Remove a HTTP Header in Request

Value: x-forwarded-for

• Create the rewrite rule for client-IP

Rule Name: act_del_client

• Check if the following condition exists:

HTTP HEADER: HTTP Request Header

Operator: Exists

Value: client-IP

• Create a rewrite action with the following description:

Type: Remove a HTTP Header in Request

Value: client-IP

All old x-forwarded-for and client-IP HTTP headers are now deleted from incoming requests.

Assumptions

The following are the assumptions made in this example:

• You have created an environment and a cloud access profile.
• You have specified the basic details, such as the name of the application, environment, services, and endpoints by navigating to Applications > New Application.

Follow these steps to configure the content transform:

• Step 1: Navigate to Application > Content Transform.
• Step 2: Create or Select. Here, you can create or add an existing Rewrite rule or a Responder rule.
• Step 3: Configure content transform, for your requirements. Here you can add the condition and actions suitable for your requirements and then bind the content transform to the services.
• Step 4: Deploy the application.
Citrix App Delivery and Security service

Remove an HTTP header in the request using the GUI

• **Step 1**: Navigate to Applications > Content Transform
  1. In the Deliver an Application page, click Create
  2. In the Create Content Transform page, click Create Content Transform
  3. In the Create Content Transform page, type a name in Content Transform Name.

• **Step 2**: Configure content transform, rewrite rules and actions. Create two rewrite rules one for `x-forwarded-for` and another for `client-IP`

  In the Add Rewrite Rule page, enter the following parameters, then click Add.
  **Rule name**: Example

  1. **If the following condition is met:**
     - Select HTTP Request Header in the drop-down list
     - Select Exists operator
     - Select Value and type `x-forwarded-for`
  2. **Then do the following:**
     - Select Remove the HTTP Header in Request
     - In the Header Name type `x-forwarded-for`
     - **Rule name**: Example1
  3. **If the following condition is met:**
     - Select HTTP Request Header in the drop-down list
     - Select Exists operator
     - Select Value and type `client-IP`
  4. **Then do the following:**
     - Select Remove the HTTP Header in Request
     - In the Header Name type `client-IP`
5. In the **Create Content Transform** page, click **Create**.

6. In the **Select Content Transform** page, click **Add**, to add the content transform.

7. In the **Deliver and Application** page, Select the preferred service in the **Services** dropdown list by selecting the checkbox.

All old `x-forwarded-for` and `client-IP` HTTP headers are now deleted from incoming requests.

**Remove an HTTP Header in Request using the API**

**Prerequisites**

- A managed application is created under an environment using an auto generated FQDN.
- For the purpose of this document, it is not relevant whether the application has been created through the UI or the API.
- You have the environment details.

Set the following values in your API request:

```plaintext
1  Header:
2  Content-Type: application/json
3  INTERNAL_CLOUD_NITRO: true
4  isCloud: true
5  Accept: application/json
6  Cookie: SESSID=
7  
8  <!--NeedCopy--> 
```
Overview

The following API configuration guidelines apply to configuring content transform, primary data center managed by the CADS service. To create a content transform in this deployment mode, you need the environment id.

While the remainder of this document assumes that the managed application pre-exists, it provides instructions on retrieving the environment details using CADS service APIs.

Retrieve environment details:

```
1 Request URL:
2 GET https://adcaas/nitro/v1/config/environments?owned_by=self
3 <!--NeedCopy-->n
```

The response is an array with details of all the deployed environments.

Note: The following response payload is adjusted for readability and only includes a single environment when the managed application is deployed.

```
1 {
2     "environments" : [
3         {
4             "cloud" : "aws",
5             "id" : "f3826bb4fafe7a31367a335171dc45b4",
6             "aws_params" : {
7                 <snip>
8             "region" : "us-east-2",
9             "availability_zones" : [
10                 "us-east-2a"
11             }
12         }
13     }
14 }
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Here, the retrieved environment id is f3826bb4fafe7a31367a335171dc45b4. This environment id is used while binding the network function to the application service.

**Add a content transform to check the HTTP response for client-IP and x-forwarded-for.**

**Add Filters:**

Filters must be created before creating content transform network functions. These filters are used while creating content transform network functions.

```
Request URL:
POST https://adcaas/nitro/v1/config/filters

The filters are configured as follows:

- Create two filters with names, check-client-ip and check-x-forwarded-for.
- The condition detects if the request header contains the data client-ip and x-forwarded-for.
```
Request Payload to create a filter:

```json
{
  "filters": [
    {
      "name": "check-client-ip",
      "expression": {
        "exists": {
          "req_header": {
            "name": "client-ip"
          }
        }
      }
    },
    {
      "name": "check-x-forwarded-for",
    }
  ]
}
```
Example Response: If the unique ID is received in the response the filters are successfully created.
"req_header": {
  "name": "client-ip"
}

"id": "ac1105409aea48f4f04d6fe8d1b2b9de",
"name": "check-client-ip"

"expression": {
  "exists": {
    "req_header": {
      "name": "x-forwarded-for"
    }
  }
}


Create the network function:
Filters must be created before creating a content transform network function.

Request URL:
```
1 POST https://adcaas/nitro/v1/config/network_functions
```

A content transform is configured as follows:
- **ContentTransformNF** is the name of the content transform.
- Content transform feature is enabled.
- Rule names are set to **remove-client-IP** and **remove-x-forwarded-for**
- Rewrite action is to remove the header in the request, when the header name is either **client-IP** or **x-forwarded-for** is detected.

Request Payload to create a Content Rule Network function to remove the identified HTTP response headers **client-IP** and **x-forwarded-for**

```
{
   "network_functions": [{
      "name": "ContentTransformNF",
      "type": "content_transform",
   }

```
"content_transform_params": {
  "enable_content_transform": true,
  "rule_list": [
    {
      "rule_name": "remove-client-ip",
      "filter_name": "check-client-ip",
      "rewrite_action": "remove_header_in_request",
      "remove_header_in_request_params": {
        "header_name": "client-ip"
      },
      "state": true
    },
    {
      "rule_name": "remove-x-forwarded-for",
      "filter_name": "check-x-forwarded-for",
      "rewrite_action": "remove_header_in_request",
      "remove_header_in_request_params": {
        "header_name": "x-forwarded-for"
      },
      "state": true
    }
  ]
}
Example response: If the unique ID is received in the response, the network function of the type of content transform is successfully created.

```json
{
  "network_functions": [
    {
      "content_transform_params": {
        "enable_content_transform": true,
        "rule_list": [
          {
            "rule_name": "remove-client-ip",
            "filter_name": "check-client-ip",
            "rewrite_action": "remove_header_in_request",
            "remove_header_in_request_params": {
              "header_name": "client-ip"
            }
          }
        ]
      }
    }
  ]
} <--NeedCopy-->
```
"state": true

"rule_name": "remove-x-forwarded-for",
"filter_name": "check-x-forwarded-for",
"rewrite_action": "remove_header_in_request",
"remove_header_in_request_params": {
  "header_name": "x-forwarded-for"
}

"state": true

"created_at": "2021-11-26T08:35:38Z",
"id": "1df2628479d0c1b5b1d8040bddd04cccb4",
"name": "ContentTransformNF",
"type": "content_transform",
"updated_at": "2021-11-26T08:35:38Z"
Bind the network function to the application service:

The application services can be associated with the existing network functions just by specifying the name/id and type of the network function in the payload.

```
POST https://adcaas/nitro/v1/config/applications

Note: Specify the retrieved environment id in the application payload. The environment id retrieved is f3826bb4afe7a31367a335171dc45b4.
```

```
Headers:
Content-Type: application/json
INTERNAL_CLOUD_NITRO: true
isCloud: true
Accept: application/json
Cookie: SESSID=

The content transform network function created can be used in the application payload as follows:

```
{
  "applications": [{
    "edition": "premium",
    "name": "DemoApp",
    "type": "aws",
    "environment": {
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.
"id": "f3826bb4fafe7a31367a335171dc45b4",

"endpoints": [],

"network_functions": [],

"filters": [],

"application_services": [

  {

    "name": "DemoAppSvc",

    "protocol": "HTTP",

    "port": 80,

    "app_server_type": "servers",

    "aws_autoscalegroup": "",

    "aws_instances": [],

    "servers": [

      {

        "type": "IPAddress",

        "value": "2.2.2.2"

      }

    ],

    "certificates": []

  }

]
"network_functions": [
{
  "name": "LB_default",
  "type": "lb"
},
{
  "name": "ContentTransformNF",
  "type": "content_transform"
}
],
"application_endpoints": [
{
  "endpoint_name": "DemoApp",
  "default_route": "DemoAppSvc",
  "routes": []
}]
}
Application response: The unique ID is received in the response. The application is successfully created.

```json
{
  "applications": [
    {
      "application_endpoints": [
        {
          "default_route": "DemoAppSvc",
          "endpoint_id": "d2982a29642ad23f1416846523e546b",
          "endpoint_name": "DemoEndpoint",
          "id": "bc7c9038e1fced6ae176a5525f5d3860",
          "routes": []
        }
      ],
      "application_services": [
        {
```
"app_server_type": "servers",
"certificates": [],
"id": "c34fb994ae7f9a73fbe6956fca5f511d",
"name": "DemoAppSvc",
"network_functions": [
{
"name": "LB_default",
"type": "lb"
},
{
"name": "ContentTransformNF",
"type": "content_transform"
}
],
"port": 80,
"protocol": "HTTP",
"servers": [
{
"type": "IPAddress",
"id": "c34fb994ae7f9a73fbe6956fca5f511d",
"name": "DemoAppSvc",
"network_functions": [
{
"name": "LB_default",
"type": "lb"
},
{
"name": "ContentTransformNF",
"type": "content_transform"
}
],
"port": 80,
"protocol": "HTTP",
"servers": []
"value": "2.2.2.2"
}
]
"slow_server_settings": {
"action": "detect"
}

"created_at": "2021-11-26T08:47:59Z",
"deployed_at": null,
"edition": "premium",
"environment": {
"cloud": "aws",
"id": "3b6ed423c509404915c57a06ee675e6b",
"name": "DemoEnv"
}
,
"id": "2839de5e613060fb85b0ec0aa1eb378c",
"job_id": null,
"name": "DemoApp",
"status": "INDRAFT",}
Here, the retrieved application id is 2839de5e613060fb85b0ec0aa1eb378c. This application id is used while deploying the application.

**Deploy the application:**

```
  Request URL
  POST https://adcaas/nitro/v1/config/applications//actions/deploy
```

Provide the **new** retrieved from the application response. This API call creates a background job to deploy the application. Here the retrieved application id is 2839de5e613060fb85b0ec0aa1eb378c.

After deploying the application, when the incoming traffic contains any confidential information, the CADS service initiates the action as defined in the rewrite rule and action to remove the specified HTTP header and the client IP.