Welcome to the product release notes for F5® Distributed Cloud Services. Each month, the product team will provide additional details on key features and enhancements in every release.

**Distributed Cloud Web Application and API Protection (WAAP)**

**API PROTECTION**

**API Authentication Discovery**

API Authentication Discovery identifies the authentication state and type of APIs within an application. The service can document authentication types based on the OpenAPI spec or their location within each API call, easily associating this data with app endpoints for analysis.

Authentication information that is part of a known OpenAPI spec can be automatically enforced, while unauthenticated traffic can be stopped in its initial stages, removing the need for origin API gateways to handle requests. This capability helps to augment API gateway functionality, delivering enhanced visibility, oversight and control over API behavior, authentication, and access. This enables organizations to identify gaps in API authentication, control access, and stop unauthorized access attempts to APIs and the back-end systems and data they connect.
JSON Web Token (JWT) Discovery

F5 Distributed Cloud WAAP now discovers header, payload, and signature information in JWTs, identifying useful fields for downstream analysis and visibility. The new WAAP capabilities enable discovering and analyzing the headers, payloads, and signatures within JWTs that may be indicators of compromise. It can detect user roles or user IDs and identify sensitive data in JWT payloads which can be used to guide remediation efforts to shore up and further protect insecure endpoints.

Increase in OpenAPI Schema Upload Limits (Up to 2.0 MB)

The platform now supports the upload of schema files up to 2.0 MB in size, allowing users to upload larger, more complex API schemas. This includes handling a larger number of endpoints, more details, and examples within each schema file.

BOT DEFENSE

New Protection Coverage Report

The Protection Coverage Report offers an in-depth exploration of traffic-flow patterns across secured endpoints, enabling users to analyze the proportion of flagged versus mitigated traffic for each endpoint. Paths are categorized by application and by function, such as login or checkout, making the reports more intuitive and highlighting the business value created by the protection.
Cloudflare Connector for F5 Distributed Cloud Bot Defense

The Cloudflare Connector for Distributed Cloud Bot Defense enables Cloudflare CDN customers to easily integrate F5’s bot-management service in the Cloudflare console. Once the F5 Connector module is deployed on Cloudflare, users will be able to view traffic statistics and security reports in the Console dashboard. The Cloudflare Connector highlights the F5 mission to protect any app deployed either on-premises, in the cloud, hybrid, or on third-party e-commerce platforms or CDNs. For more information, visit this Bot Defense page.

WEB APPLICATION FIREWALL (WAF)

WAF Signature Staging is Now Available

Signature staging is a new mechanism to evaluate new and/or modified attack signatures for a period of time before they are placed into operational/enforcement mode. The F5 Security Research Team frequently releases new signatures, updates existing signatures to improve their efficiency, and in some rare cases deletes signatures to avoid duplicates.

Some users prefer to place new and updated signatures into staging mode to give them time to review security events where these new or updated signatures are triggered and to tune policies before moving them into operation/enforcement mode. This new functionality will help users limit issues in their environment related to new signatures including incorrectly blocking good traffic and/or the generation of false positives. Additional guidance on setting this up can be found in the WAF how-to documentation.
**Cookie Tampering Protection**

Cookie tampering can be used in attacks such as session hijacking, where cookies with session identification information are stolen or modified by an attacker. This new functionality prevents attackers from modifying the value of session cookies. It can be configured by navigating to HTTP Load Balancer > Web Application Firewall > Cookie Protection section in the load balancers configuration.

**WAAP**

**Announcing WAAP Scheduled Reports**

The WAAP Scheduled Reports feature lets you schedule reports (daily, weekly, or monthly) with summary results (from one or more namespaces) to be emailed to users specified in the user groups. The feature is configured in the Manage > Reports section.

**New Dashboard for Malicious Users**

The new Malicious Users dashboard provides a global view of attackers for a specific namespace, along with the ability to drill down into specific malicious user details. This provides users greater context about potentially malicious clients that interact with their applications, including User, Country, City, Region, ASN, and Source IP, with easy filtering and drill-down capabilities. Users can easily track the most ominous threats with risk scoring and threat level assessments to quickly allow or deny any client from the UI.

![Figure 3: The new Malicious User dashboard provides greater context about potentially malicious clients.](image-url)
Application and Network Performance

MULTI-CLOUD NETWORKING

UI Change: Renaming "Cloud and Edge Sites" Tile to "Multi-Cloud Network Connect"

For the release of F5 Distributed Cloud Network Connect, the tile previously labeled “Cloud and Edge Sites” has a new name and a new landing page. The Multi-Cloud Network Connect landing page provides convenient access to feature overviews, quick start guides, and technical documentation. The previous default screen and all other features and content are available via the navigation sidebar, which remains unchanged. Future releases will add more network-specific features to this tile.

UI Change: Renaming "Load balancers" Tile to “Multi-Cloud App Connect”

For the release of Distributed Cloud App Connect, the tile previously called “Load balancers” has a new name and a new landing page. The landing page for Multi-Cloud App Connect provides convenient access to feature overviews, quick start guides, and technical documentation. The previous default screen and all other features and content are available via the navigation sidebar, which remains unchanged. Future releases will add more application delivery and interconnect features to this tile.

Figure 4: The new Multi-Cloud Network Connect tile in the console.
New Site Type: Secure Mesh

The Secure Mesh site serves as a network gateway for managing network connectivity, security, and application interconnect and delivery across various on-premises scenarios such as Edge, Data Center, Co-location, and Branch. Secure Mesh is intended for virtual and physical form factors such as KVM, certified third-party hardware, and F5 Distributed Cloud gateway appliances. This site type is useful for securely connecting locations that have existing application infrastructure, and for presenting Distributed Cloud resources to users at specific locations.

Performance Enhancement Mode Now Supported for All Site Sizes and Types

Performance Enhancement Mode is now supported for all sizes and types of sites. Performance Enhancement Mode allows a choice to optimize the networking at a site for L7 app delivery (the current default) or L3 site-site connectivity. The mode for a site can be changed at any time, but applying the change will disrupt all network traffic to/from that site for up to five minutes.

Site Topology Added for Azure VNET Site

This feature gives a visual representation of the site topology for Azure VNET Sites, both Standalone VNET and Hub VNET. With the ability to view details about each VNET, subnets, number of deployed Mesh instances, route tables, and more, you can gain a better
understanding of your infrastructure and identify potential issues. This, in turn, helps you optimize your network performance, troubleshoot more effectively, and make informed decisions about your infrastructure.

HTTP and TCP Load Balancers Support Multiple Custom TLS Certificates
Customers can upload their own TLS certificates and Intermediate certificate chains to the Distributed Cloud platform for use as certificate objects. Those objects can be used across multiple HTTP and TCP load balancers while maintaining centralized management to simplify certificate updates. This new capability is available under Manage > Certificate Management section of Multi-Cloud App Connect service.

Application Performance and Reliability

DISTRIBUTED CLOUD CONTENT DELIVERY NETWORK (CDN)

Support for Summary View of CDN Access Logs
F5 Distributed Cloud CDN now supports the ability to view a summary of CDN Access Logs.

Spliced Downloads and Large File Support
Distributed Cloud CDN now supports the ability to separate larger files into smaller segments to improve download speed and efficiency. The previous file size limit was 50MB, but that limit has been removed. After splicing a file from the origin, the CDN serves the file segments concurrently to clients that utilize an HTTP range request. Clients can resume a download if it has been interrupted.

SYNTHETIC MONITORING

More Granularity of Timeout Thresholds in the Products
HTTP(s) and DNS Monitor timeout units have changed from seconds to milliseconds, enabling finer control over alerting thresholds.

![Figure 6](image-url) This image reflects the change in HTTP(s) and DNS Monitor units to milliseconds.
DNS

Number of DNS Records Can Now Be Displayed in the DNS ZonesListing

It is now possible to display on the DNS zones listing page the number of DNS records contained in each DNS zone. This is done through an additional field named "Number of DNS records" that can be added as part of the listing.

GLOBAL LOG RECEIVER

Support Added for Sumo Logic and NewRelic Targets

This release adds support for Sumo Logic and NewRelic as targets for the Global Log Receiver feature. This allows customers using those vendors to send their logs more easily, rather than having to use the generic HTTPS endpoint. For more information about adding Sumo Logic logs to your Global Log Receiver, read this DevCentral article.

Figure 7: Distributed Cloud Global Receiver offers native support for Sumo Logic, so users can easily connect a Distributed Cloud tenant to their Sumo Logic environment to work with security event data.
Modern Application Delivery

APP STACK

Deploy Mesh Sites on Edge or Data Center Using a Simplified Workflow

Users can easily deploy Mesh sites in edge locations or data centers via a simplified workflow in the Distributed Cloud Console. This feature enables customers to configure Mesh sites just as they do today with App Stack sites. Users can share common code with the App Stack sites since the code is similar.

Please see the full Distributed Cloud Changelog for additional information, including more new enhancements plus known issues and caveats. We hope you find the information contained in these release notes useful. If you have any feedback please email CS_DistributedCloudTeam@f5.com.