

Edgecast

# Media Control Center (MCC) User Guide

---

**edgecast**

## Disclaimer

Care was taken in the creation of this guide. However, Edgecast cannot accept any responsibility for errors or omissions. There are no warranties, expressed or implied, including the warranty of merchantability or fitness for a particular purpose, accompanying this product.

## Trademark Information

EDGECAST is a registered trademark of Edgecast Inc.

## About This Guide

Media Control Center (MCC) User Guide

Version 4.23

6/2/2022

© 2022 Edgecast Inc. All rights reserved.

# Table of Contents

Media Control Center (MCC) .....	1
Overview .....	1
Dashboard .....	1
Performance .....	2
Usage.....	2
Accessing the MCC.....	3
Switching between Customer Accounts .....	3
Multi-Factor Authentication (MFA) .....	5
Reset Password .....	11
Navigating Within the MCC.....	13
Main Menu.....	14
Side Navigation Bar .....	15
User Settings Menu.....	15
Support Services .....	17
User Accounts .....	18
Overview .....	18
Privileges .....	18
User Account Administration.....	20
Creating a User Account .....	20
Modifying a User Account.....	21
Deleting a User Account.....	22
Custom User ID .....	22
Updating Profile Settings .....	23
Log Files.....	26
Overview .....	26
Log File Naming Convention .....	27

Log File Storage .....	28
CDN Storage (CDN Origin Server) .....	28
External Storage .....	30
Log File Format.....	32
HTTP Platforms .....	32
Third-Party Log Analysis Tools .....	42
Network Status .....	43
Overview .....	43
Network Status Notifications .....	44
Appendix A .....	46
Cache Status Codes .....	46
Appendix B .....	48
Privileges .....	48
Web Services REST API Access .....	63

# Media Control Center (MCC)

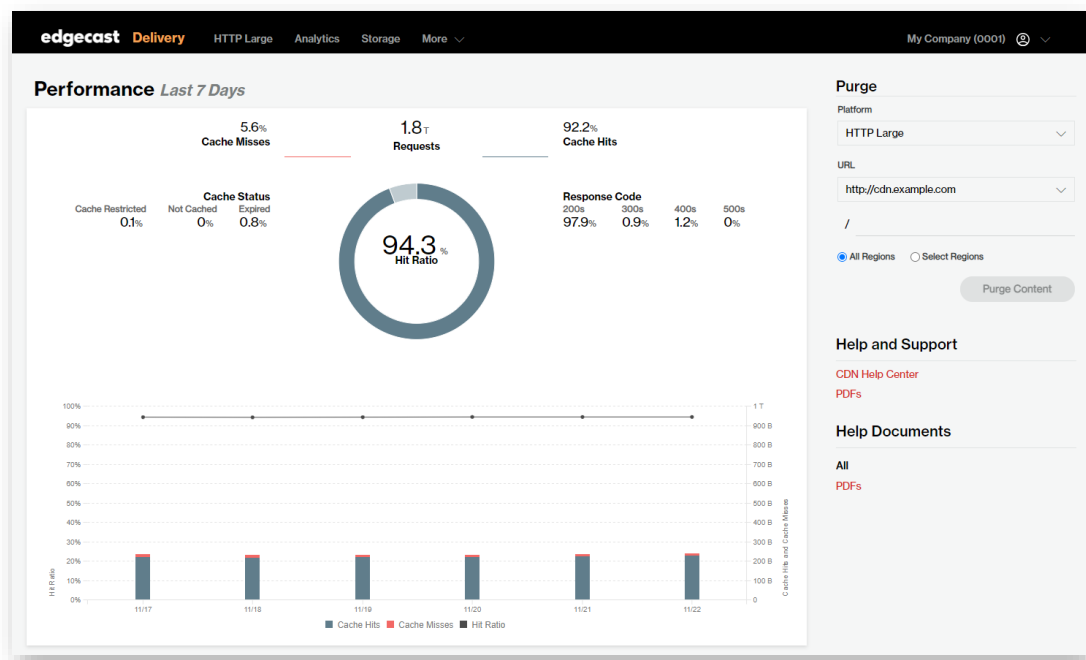
## Overview

The Media Control Center (MCC) site provides a central location from which you can view and modify your content delivery network (CDN) configuration. Additionally, you may generate reports that provide detailed information on how our CDN is delivering data to your clients. This allows you to analyze data delivery performance, in order to optimize how our CDN caches your organization's assets. The final aspect of MCC configuration allows you to determine who will have access to these features and settings.

## Dashboard

The MCC's landing page is known as the **Dashboard**. The **Dashboard** provides a space through which you can:

- View a breakdown of core CDN statistics.
- Purge previously cached content.
- Launch our online help.



MCC Dashboard

## Performance

The **Performance** section, which provides a high-level overview of CDN performance for your traffic over the last seven days, provides insight into:

- **Traffic:** View the total number of requests that were served via the CDN for your traffic. View bandwidth usage via the **Avg. Usage/Sec** graph that appears directly below the **Performance** section.
- **Cache Efficiency:** View the percentage of requests served from cached (i.e., cache hits) and those that were served from an origin server (i.e., cache misses). View statistics for additional cache status codes (e.g., Not Cached or Expired) directly below the Cache Misses metric.  
Alternatively, the following visual representations of cache efficiency are provided in the chart located at the bottom half of the **Performance** section:
  - **Line Graph:** A line graph provides a quick assessment of cache efficiency (i.e., hit ratio) over time. This line graph is plotted according to hit ratio (as indicated on the left-hand side of the graph).

---

**Note:** High cache efficiency (close to 100%) indicates that your traffic is being served optimally.

---
  - **Bar Chart:** A bar chart plots the number of cache hits and cache misses (as indicated on the right-hand side of the graph). Use this bar chart to visualize the proportion of cache hits to cache misses.
- **Response Code (HTTP Status Codes):** Verify that clients were able to receive your content by checking the HTTP status codes (i.e., response code) that were served. The percentage of requests that returned 4xx and 5xx status codes should be a tiny proportion of your overall traffic.

---

**Note:** Learn more about the updated terminology introduced in the Dashboard from the [CDN Help Center](#).

---

## Usage

This section contains graphs that provide insight into your bandwidth usage (Avg. Usage/Sec) and the amount of your data that was transferred via the CDN.

---

**Tip:** View usage information for a given month through the Core Report's Traffic Summary report.

---

---

## Accessing the MCC

The Media Control Center (MCC) is the main administrative hub for defining a CDN configuration for your organization. It can be viewed by following this link:

<https://my.edgecast.com>

---

**Tip:** Take advantage of your web browser's bookmark functionality to quickly access any page in the MCC.

---

Only personnel that have a MCC user account will be granted access to the MCC. Upon loading the MCC, a user will need to log in using the email address associated with their user account and their password. For information on how user accounts can be created or configured, please refer to the **User Accounts** chapter below.

---

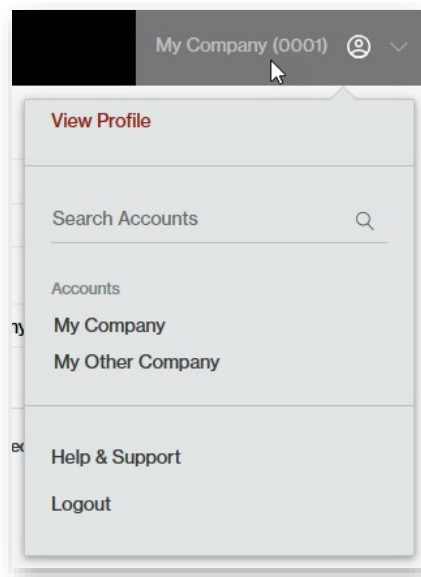
**Note:** Your administrator may require that you verify your identity when logging in to the MCC through multi-factor authentication (MFA).

**Note:** User privileges determine the level of access that a user will have to the MCC. A user without privileges will be unable to perform any tasks in the MCC.

---

## Switching between Customer Accounts

If you have access to multiple customer accounts, then you can switch between them by selecting the desired customer account from under the **Accounts** section of the user settings menu. Access the user settings menu by clicking on the customer account label from the portal's upper-right hand corner.



*User Settings Menu*

**Key information:**

- The **Accounts** section will only list the last 5 customer accounts that you have accessed.
- Search by customer account name when it is not listed under the **Account** sections.

---

**Note:** You cannot search by customer account number.

---

- If the desired customer account is not linked to your email address, then your CDN administrator should add a user with your email address to that customer account.

---

**Important:** Changing a user's email address is insufficient to establish a link to your account. Your CDN administrator must create a user to establish this link.

---

### Variations in Email Addresses

You are only allowed to switch between customer accounts that contain a user with your exact email address. A match will not be found if there is a single variation between the two email addresses. This occurs regardless of whether your email client handles both email addresses in the same manner.

#### Sample Scenario

Let's assume the following setup:

Customer Account	User's Email
My Customer 1	johnsmith@example.com
My Customer 2	johnsmith@example.com
My Customer 3	john.smith@example.com
My Customer 4	johnsmith+mycustomer4@example.com

We will now see what will happen when you log in using each of the above email addresses:

- Logging in as johnsmith@example.com will allow you to switch between My Customer 1 and My Customer 2.
- Logging in as john.smith@example.com will only grant you access to My Customer 3.
- Logging in as johnsmith+mycustomer4@example.com will only grant you access to My Customer 4.

### CDN Storage Access

You may only be granted CDN storage access to a single customer account. If you require CDN storage access for multiple customer accounts, then you will be required to use a different user account for each of those customer accounts. Please contact the CDN administrator for each desired customer account to ensure that your user account does not have CDN storage permissions for multiple customer accounts.



## Multi-Factor Authentication (MFA)

Protect your user account from unauthorized access by enabling multi-factor authentication (MFA). MFA is an additional security requirement that requires a time-sensitive token when logging into the MCC. This token, which confirms your identity, may be generated through either of the following methods:

- **Authenticator Application:** Look up a time-sensitive token within a Time-based One-time Password-compatible (TOTP) authenticator application (e.g., Google Authenticator) whenever you are challenged to provide a two-factor authentication token.
- **SMS Messaging:** Receive a time-sensitive token via a text message whenever you are challenged to provide a two-factor authentication token.

### Quick Start

Perform the following steps to set up multi-factor authentication for the first time:

1. Log in to the MCC.
2. Select whether to generate time-sensitive tokens through an authenticator application or text messages.
3. Perform either of the following procedures:
  - **Authenticator Application (Recommended)**
    - i. Install a TOTP-compatible authenticator app (e.g., Google Authenticator, Duo, or Authy).
    - ii. From within your authenticator app, create a new account and then scan the QR code.

- **Text Message**

Provide your mobile device's phone number (E.164 format).

Syntax (United States):

```
+1 {Area Code} {Phone Number}
```

Syntax (Other Countries):

```
+{Country Code} {Area Code} {Phone Number}
```

4. Provide the time-sensitive token that was generated by either an authenticator app or text message.

---

**Note:** Upon successfully completing MFA setup, all future login attempts will require that you provide a time-sensitive token.

---

## Authenticator Application

Look up a time-sensitive token within a Time-based One-time Password-compatible (TOTP) authenticator application (e.g., Google Authenticator, Duo, or Authy) whenever you are challenged to provide a two-factor authentication token.

### To set up multi-factor authentication through an authenticator application

1. Log in to the MCC.
2. Upon successfully logging in, you will be prompted to set up MFA.

---

**Tip:** If you are not prompted to set up MFA upon logging in, then you can modify your MFA configuration from the **Security** tab of your Identity dashboard (<https://manage.vdms.io/>).

---

3. Click **Select** within the **Authenticator App** section.
4. If you have not already installed a TOTP-compatible authenticator app (e.g., Google Authenticator, Duo, or Authy), then you should download and install it now.
5. From within your authenticator app, create an Edgecast account within your authenticator application.

---

**Tip:** Automatically define the account's name and secret key by scanning a QR code. Otherwise, you will need to manually enter this information.

**Note:** Once your account is successfully created, your authenticator app will continuously generate a time-sensitive token.

---

6. In the **Verification code** option, type the time-sensitive token generated by your authenticator app and then click **Verify**.

---

**Reminder:** Upon successfully completing MFA setup, all future login attempts will require that you provide a time-sensitive token.

---

### To use a different authenticator application or device

---

**Note:** This procedure requires access to your authenticator account. If you no longer have access to your authenticator account, then you will need to reset your MFA configuration by contacting support.

---


1. Disable authenticator application multi-factor authentication.
2. Perform steps 2 - 5 from the **To set up multi-factor authentication through an authenticator application** procedure.

## To disable authenticator application multi-factor authentication

---

**Note:** This procedure requires access to your authenticator account. If you no longer have access to your authenticator account, then you will need to reset your MFA configuration by contacting support.

---

1. Log in to the [Identity dashboard](#).
2. Navigate to the **Security** tab.
3. From within the **Authenticator App** section, click .
4. When prompted for confirmation, type your password within the **Enter your current password to confirm delete** option and then click **Delete**.

## Google Authenticator

Google Authenticator is a software application that generates tokens through which you can verify your identity to Google services and third-party applications (e.g., MCC). This software application can be installed on your desktop, Android cell phone, or iPhone/iPad devices.

Download links are provided below.

- [Android](#)
- [iPhone and iPad devices \(requires iTunes\)](#)

## Authenticator App Troubleshooting

### Token Does Not Work

If the token generated by your authenticator app does not work, check the following items:

- Is authenticator app MFA currently enabled?  
From the **Security** tab of the [Identity dashboard](#), check whether the **Authenticator App** section has been enabled (✔ **Enabled**). If you see an **Enable** button within this section, click it to enable authenticator app MFA.
- Are you using the current account?  
An authenticator app contains all of your accounts. This may include accounts created for other sites/applications and outdated accounts. An account is created whenever you configure authenticator app MFA. If you have configured it more than once, then you may have older accounts within your authenticator app that generate codes that will not work.
  - Verify that you are using the account that was created when your MFA configuration was last updated.
  - If you are unsure which account is being used for MFA, create an account by updating your authenticator app MFA configuration.

### Inaccessible Account

If you no longer have access to your authenticator app, then you will need to reset your MFA configuration by contacting support.

### Locked Account

Your account is automatically locked for 30 minutes after six consecutive unsuccessful log in attempts. Both credentials and multi-factor authentication challenges count towards this limit. If you are locked out of your account, perform either of the following steps:

- Reset your password.
- Wait 30 minutes.

### Remember this Computer

We currently do not support the ability to remember your computer. We plan on reintroducing the ability to remember a device in the near future.

### SMS Messaging

Text messages containing time-sensitive tokens can be sent directly to your cell phone or messaging device via SMS. Setting up SMS messaging does not require the installation of a software application. Provide the phone number corresponding to your cell phone or messaging device. A text message containing a time-sensitive token will be sent to your phone.

The syntax for specifying phone numbers varies by location.

- **Syntax (US-Based Phone Numbers):**

```
+1 {Area Code} {Phone Number}
```

Sample Phone Number (Los Angeles, United States):

```
+1 310 555 1212
```

- **Syntax (Phone Numbers Outside of the US):**

```
+{Country Code} {Area Code} {Phone Number}
```

Sample Phone Number (Rio de Janeiro, Brazil):

```
+55 21 5555 1212
```

---

**Note:** Standard text messaging rates may apply. We are not responsible for any fees that your cellular network carrier may charge for message transmission and delivery.

---

## To set up multi-factor authentication through text messages

1. Log in to the MCC.

---

**Tip:** If you are not prompted to set up MFA upon logging in, then you can modify your MFA configuration from the **Security** tab of your [Identity dashboard](#).

---

2. Click **Select** within the **Text Message** section.
3. Type your mobile device's phone number and then click **Send Text Message**.
4. In the **Verification code** option, type the time-sensitive token that was sent to the above phone number via text message.
5. In the **Enter your current password to confirm changes** option, type your password.
6. Click **Verify**.

---

**Reminder:** Upon successfully completing MFA setup, all future login attempts will require that you provide a time-sensitive token.

---

## To update your mobile phone number

---

**Note:** This procedure requires access to your mobile phone. If you no longer have access to your mobile phone number, then you will need to reset your MFA configuration by contacting support.

---


1. Disable text message multi-factor authentication.
2. Perform steps 2 - 6 from the **To set up multi-factor authentication through text messages** procedure.

## To disable text message multi-factor authentication

---

**Note:** This procedure requires access to your mobile phone. If you no longer have access to your mobile phone number, then you will need to reset your MFA configuration by contacting support.

---

1. Log in to the [Identity dashboard](#).
2. Navigate to the **Security** tab.
3. From within the **Text Message** section, click .
4. When prompted for confirmation, type your password within the **Enter your current password to confirm delete** option and then click **Delete**.

## SMS Messaging Troubleshooting

### Missing MFA Text Messages

If you are not receiving multi-factor authentication text messages, check the following items:

- Is text message MFA currently enabled?  
From the **Security** tab of the [Identity dashboard](#), check whether the **Text Message** section has been enabled (✔ **Enabled**). If you see an **Enable** button within this section, click it to enable text message MFA.
- Is it configured to send text messages to the phone number associated with your mobile device?  
If you are unsure, you can update your mobile phone number.
- Are you receiving other text messages?  
Verify that your messaging device has connectivity and that your SMS inbox is not full.

### Locked Account

Your account is automatically locked for 30 minutes after six consecutive unsuccessful log in attempts. Both credentials and multi-factor authentication challenges count towards this limit. If you are locked out of your account, perform either of the following steps:

- Reset your password.
- Wait 30 minutes.

### Remember this Computer

We currently do not support the ability to remember your computer. We plan on reintroducing the ability to remember a device in the near future.

## Switching Token Generation Method


Switch token generation method by deleting your existing MFA configuration. After which, you may set up a new configuration.

### To switch your token generation method

---

**Note:** This procedure requires the ability to generate a MFA token. If you cannot generate a token, then you will need to reset your MFA configuration by contacting support.

---

1. Log in to the [Identity dashboard](#).
2. Navigate to the **Security** tab.
3. Click .
4. When prompted for confirmation, type your password within the **Enter your current password to confirm delete** option and then click **Delete**.
5. Set up your new MFA configuration by performing either of the following steps:
  - **Authenticator App:** Perform steps 2 - 5 from the **To set up multi-factor authentication through an authenticator application** procedure.
  - **Text Messages:** Perform steps 2 - 6 from the **To set up multi-factor authentication through text messages** procedure.

## Reset Password

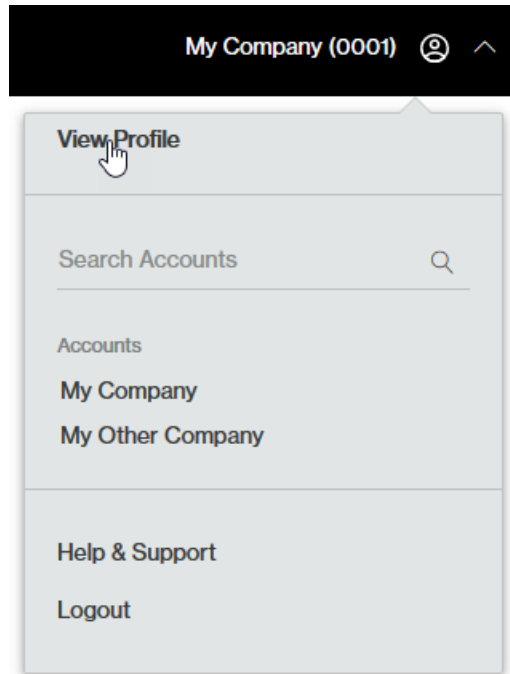
If a user cannot remember their MCC password, they can choose to reset it. Resetting a password will generate an email containing a password reset link. Once the user follows this link, he/she will be prompted to identify their email account and then set a new password.

### Key information:

- A password reset link is only valid for 1 hour.
- If a password reset link has expired before you have reset your password, then you will need to submit another password reset request.

## To reset your password

1. Follow the "Forgot your password?" link.
  - **Recommended Procedure:** Perform the following steps:
    - i. Navigate to your profile.



- ii. Click **Change Password**.
  - iii. Click the "Forgot Your Password?" link.
- **Alternate Procedure:** Click the "Forgot Your Password?" link that appears directly below the log in options on the **Media Control Center Login** page.

---

**Important:** This alternate procedure will not update your credentials for use with SFTP (recommended) / FTP access to CDN storage or our support center. If you forgot your password and do not have an active MCC session, you will need to reset your password from the **Media Control Center Login** page and then reset it again using the recommended procedure.

---

2. In the **Email** option, indicate the email address associated with the user account whose password will be reset.
3. Click **Submit**.
4. Check for new mail on the email account associated with your MCC user account. Open the message and then follow the provided link.
5. Confirm the email address for the user account whose password will be reset.
6. You will then be prompted to specify a new password and then confirm it.



---

## Navigating Within the MCC

Navigate the MCC using the following controls:

- Main menu
- Side navigation bar
- User Settings menu

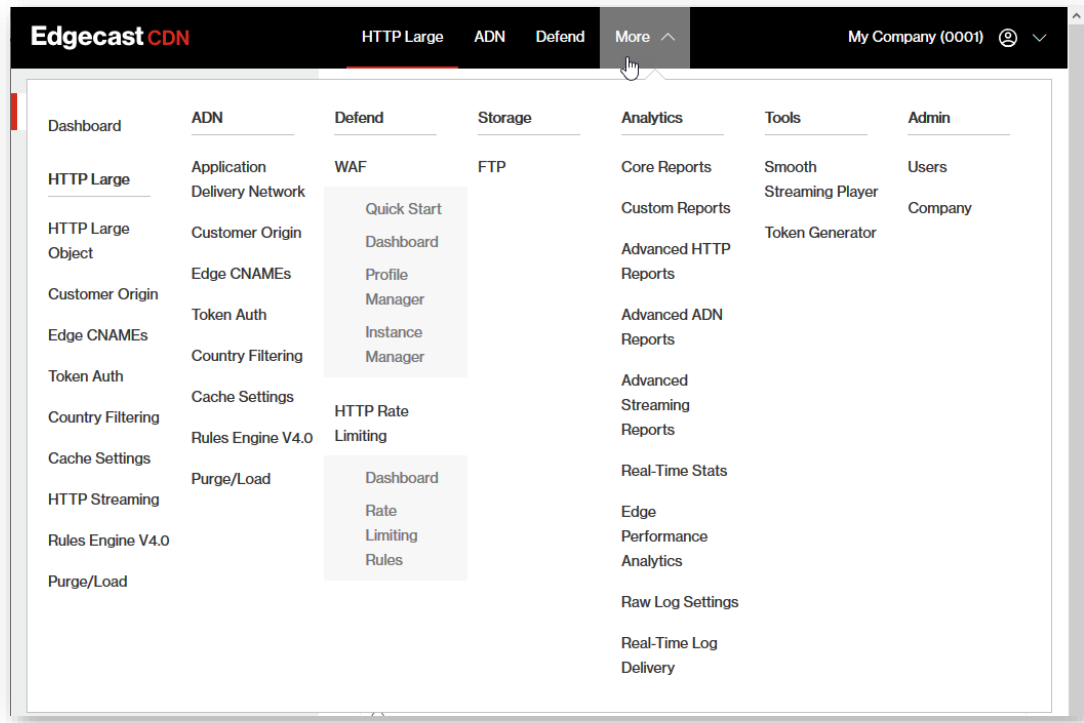
The following illustration indicates where to find these controls.



### MCC Controls

## Main Menu

The main menu, which is located at the top of the portal, provides access to the set of services that have been activated on your account. If this menu contains more than three items, then an additional menu item called "More" will appear. The **More** menu, as illustrated below, contains a listing of all top-level menus.



### *Main Menu (shown with an active More menu)*

Hovering over a menu will open a fly-out menu containing links for the pages associated with that category. Click on the desired menu item to navigate to that page.

## Missing Menu Items

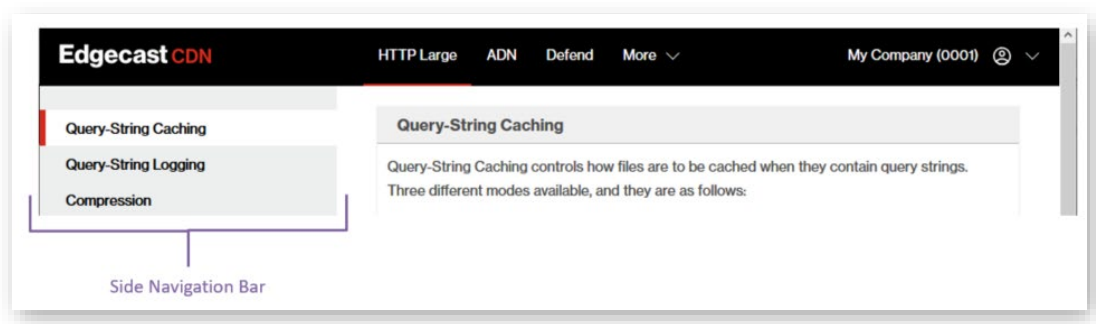
A menu item may not be available due to one of the following reasons:

- The menu item corresponds to a platform or service that your organization has not purchased.
- Your user account has not been authorized to view the menu item in question.

## Side Navigation Bar

A side navigation bar provides access to all of the pages associated with a particular service.

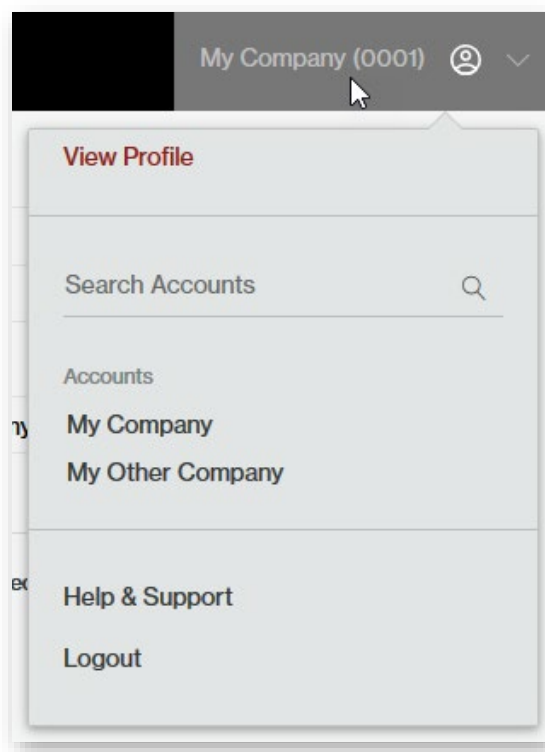
The following illustration shows the location of the side navigation bar.



*MCC (side navigation bar)*

## User Settings Menu

Access the user settings menu by clicking on the customer account label from the upper-right hand corner of the MCC as illustrated below.



*User Settings Menu*

The syntax for this menu's label is:

*Company\_Name (Account\_Number)*

**Note:** Note your customer account number. The CDN URLs generated for your account make use of this value.

A brief description is provided below for each link in this menu.

Name	Description
View Profile	Follow this link to: <ul style="list-style-type: none"><li>• View and/or modify your user account settings.</li><li>• Set notification settings.</li><li>• View and/or change your REST API token.</li></ul>
Language	Follow this link to choose the MCC's language when launched from the current web browser (e.g., Firefox or Chrome). <hr/> <b>Important:</b> Language selection takes place immediately.
Help and Support	This link provides access to our help centers that contain general usage and troubleshooting information on our CDN services. This page also contains a form through which a request for technical support may be submitted.
Logout	Follow this link to immediately end your current MCC session.

---

## Support Services


In addition to the MCC, which provides a central place through which you can perform CDN configuration, we offer the following additional support services:

- Create, manage, and review your company's technical support cases.

These services are provided through a separate portal that can be accessed through the following URL:

- <https://edgecast.service-now.com/>

---

**Tip:** Information on how to create and manage your support tickets can be viewed by clicking the Help () icon that appears in the upper-right hand corner of the SNC support center.

---

Access to these support services is limited to the users that have been created for your customer account in the MCC. In other words, only MCC users can create, review, and manage your company's technical support cases. By restricting access to your technical support cases, you can ensure that only authorized users will be privy to your sensitive information.

Key information about the Service-Now (SNC) support center:

- **Login:** A user will need to provide their MCC user account (i.e., email address) and password when logging in to SNC.
- **User Account Creation/Modification:** It may take up to 15 minutes before a new or modified user account can be used to log in to SNC. The types of user account modifications that can temporarily affect your access to SNC are changes made to your email address or password.
- If you are having trouble logging in to the support center, please try resetting your password using the recommended procedure defined in the **Reset Password** section.

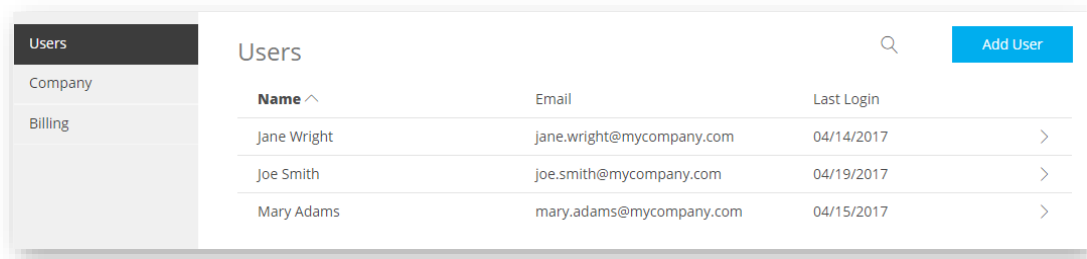
# User Accounts

---

## Overview

The MCC provides administrative control over who can access it and the actions a user can perform once access has been granted. By allowing varying levels of MCC access, different types of users across the organization can have access to the MCC in a controlled and secure manner.

Authorized administrators can manage user accounts from the **Users** page. Additionally, any user can modify their personal settings. This chapter will discuss how administrators can manage user accounts and how an individual user can update his profile information.



Users		Search	Add User
Name ^	Email	Last Login	
Jane Wright	jane.wright@mycompany.com	04/14/2017	>
Joe Smith	joe.smith@mycompany.com	04/19/2017	>
Mary Adams	mary.adams@mycompany.com	04/15/2017	>

### Users Page

---

## Privileges

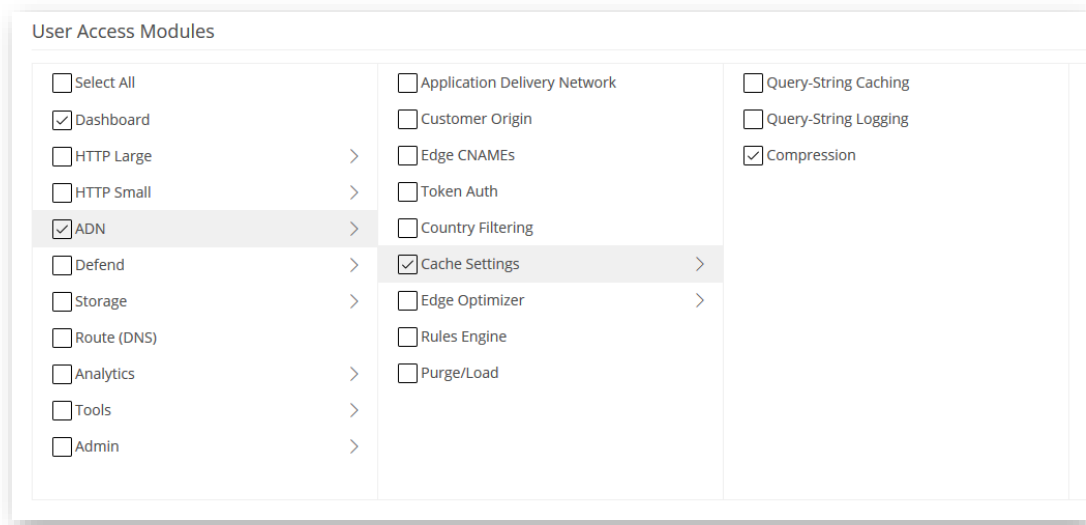
Access to the Media Control Center (MCC) is limited to the set of users that have been created for your organization. The MCC users for your organization are assigned a set of privileges by a MCC administrator. These privileges determine the level of access that a user will have when he/she logs into the MCC and the set of actions that may be performed when leveraging our REST API.

---

**Note:** Privileges only affect actions performed within the MCC or via our REST API. For example, although a user may not have permissions for the HTTP Large platform, he/she may still upload new content to the appropriate origin server and stream on-demand content through your account.

---

Privileges associated with a platform or service that has not been activated on your customer account will not be displayed. For example, notice that the Token Auth and Rules Engine privileges are not shown in the following illustration. These privileges are unavailable because the Token-Based Authentication and the Rules Engine features have not been activated on that customer account. For more information, please contact your CDN account manager.



**Partial List of Privileges (Shown without the Token Auth and the Rules Engine Privileges)**

Privileges are organized according to how a user may navigate to the corresponding page. View the children associated with a privilege by clicking on it. A child privilege cannot be granted without its parent privilege. Therefore, granting a child privilege will automatically grant all of its parent privileges. This principle is illustrated in the above illustration. Granting the Compression privilege automatically granted both the ADN and the Cache Settings privileges.

---

**Note:** A > icon indicates that a privilege contains one or more child privileges.

---

**Key information:**

- Parent privileges only control whether the corresponding menu will be enabled or disabled.  
For example, if the Defend privilege is enabled and all of its sub-privileges are disabled, then access will be allowed to the Defend menu but you will be unable to access Web Application Firewall or Rate Limiting pages.
- The ability to view or administer a particular platform or feature depends on whether you have purchased it.
- A user's ability to modify his/her own basic profile settings is not controlled by privileges.

---

**Note:** For more information, please refer to **Appendix B: Privileges**.

---

---

## User Account Administration

An administrator determines:

- Who can access the MCC.
- The set of actions that may be performed within it.

This establishes a controlled and secure manner through which users may interact with the MCC.

---

**Important:** If a user account has access to multiple customer accounts, please limit that user's CDN storage access, which is granted by the FTP and RSYNC privileges, to a single customer account. If a user account requires CDN storage access for multiple customer accounts, then you should create a user for each additional customer account for which the user requires CDN storage access. Unintended consequences may occur when a single user account is granted FTP or RSYNC privileges to multiple customer accounts.


**Tip:** Update your own profile, password, and Web Services REST API token from your profile.

---

The ability to administer MCC users is determined by the following privileges:

- **Users:** View a list of users and the date/time at which they last logged into the MCC. It also allows read-only access to a user's properties.
- **Add user administration:** Allows the creation of a user account.
- **Edit user administration:** Allows the modification and deletion of a user account.

---

**Tip:** If you are looking for a more efficient way to find a particular user, try clicking  from the **Users** page. The results of such a search will display all users whose first name, last name, or email address contain the specified search term.

**Note:** A user cannot delete his/her own account or the primary MCC user account.

---

## Creating a User Account

Create a user account by performing the following steps:

1. Navigate to the **Users** page.
2. Click **Add User**.
3. Under the **Name** option, assign the user a first and last name.
4. Under the **Email Address** option, define the email address through the user will log in to the MCC and to which notifications will be sent.
5. Click **Next**.
6. Grant the minimum set of privileges and REST API access required by that user.



7. Click **Create User**.

---

**Reminder:** The ability to create a user requires the Add user administration privilege.

---

Once a user has been created, an email will be sent to the email address associated with the new user account. This email will indicate that a MCC user account has been created and it will provide a user account activation link. A new user will need to follow the user account activation link where the user will be prompted to enter their email address. After which, the new user will need to specify a password and confirm that it meets the minimum password complexity requirements. The new account will be activated upon successfully setting a password.

---

**Reminder:** All MCC users also have access to the Service-Now support center. This support center provides the capability to view/update technical support cases and access a Knowledge Base.

---

## Modifying a User Account

---

**Note:** The ability to modify a user's settings or privileges requires the Edit user administration privilege. Read-only settings will be displayed when the user attempting this action only has sufficient privileges (i.e., Users privilege) to view users.

---

Modify any user listed on the **Users** page by clicking on that user's row. A form displaying the user's information will be displayed. Make the desired changes. If you would like to view/modify that user's permissions, click **Permissions** and reassign them as needed. Click **Save** to update that user's account.

---

**Note:** Changes made to a user's privileges do not fully take effect until the next time that user logs in to the MCC. If the user is currently logged in and would like for his/her new privileges to take effect, you should suggest that he/she log out and then log back in to the MCC.

---

## Password Expiration

A password expiration policy defines the maximum number of days that can elapse before a password must be changed.

---

**Tip:** Setting a password policy to never expire is highly discouraged.

---

### To set a user's password expiration policy

1. From the **Users** page, click on the desired user.
2. Click **More Details V** to expand it.
3. In the **Password Reset Duration** option, choose the desired password expiration policy.
4. Click **Save**.

## Deleting a User Account

Any user, except for the primary administrator and the current user, may be deleted.

---

**Reminder:** The ability to delete a user is determined by the Edit user administration privilege.

---

### To delete a user

1. Navigate to the **Users** page.
2. Click on the desired user.
3. Click **More Details V** to expand it.
4. Click **Delete User Account**.
5. Confirm the deletion of this user account by typing "DELETE" and then clicking **Delete**.

## Custom User ID

Each user can be assigned a customized ID. This custom ID can be tailored to match an internal naming convention. For example, the custom ID for each user could be their Active Directory user name.

---

**Note:** A user may modify their own custom ID from their profile.

**Note:** The capability to modify another user's custom user ID requires the Edit user administration privilege.

---

## Updating Profile Settings

You may view and/or modify your own profile settings, such as:

- Name
- Email address
- Address information
- Phone number

### Key information:

- The **E-Mail/Username** option serves a dual purpose.
  - It defines the user name through which the MCC may be accessed.
  - It determines the email address to which a variety of email notifications, such as CDN maintenance information and IP address updates, may be sent. Email notifications may be toggled from your profile.
- Updating the **Mobile** option will set/change the mobile device to which 2FA tokens may be sent.
- Sign up for email and/or text messaging notifications through the **Notification Settings** section of your profile.
- Although an administrator that has been granted the Edit user administration privilege may modify any user's settings, only a particular user can determine whether he/she would like to receive email notifications or change his/her password.

### To update your profile settings

1. Navigate to your profile by clicking **View Profile** from the upper-right hand corner of the MCC.
2. Click **Edit**. The options listed on your profile can now be modified.
3. Update the desired settings and then click **Save**.

## Web Services REST API Token

The Web Services REST API token is a value that identifies and authenticates a user when performing a call to the Web Services REST API. It is recommended that a user take the appropriate precautions to prevent this value from being disseminated. For example, a user should never leave a MCC session unattended.

---

**Important:** The ability to view or generate a unique Web Services REST API token is determined by a privilege. If you have been granted REST API access, then additional privileges determine the set of operations that you may perform.

---

If you suspect that a token value has been compromised, then you should perform the following steps:

1. Generate a new primary token.
2. Update any applications or scripts that rely on the old Web Services REST API token.
3. Distribute your applications or scripts to the appropriate entities and/or locations.
4. Delete the backup Web Services REST API token.

### Best Practices: Web Services REST API Token Security

Web Services REST API tokens should be treated like any other security credential or password. It is paramount to keep this type of token as secure as possible. We have observed incidents in which customers lost control of their Web Services REST API token and then experienced unauthorized access on their account.

The following precautions are recommended:

- Ensure that a Web Service REST API token is not shared within or outside of your organization. For example, they should not be inadvertently posted on an online support form.
- Periodically change your Web Service REST API token.
- Perform general administrative security tasks on a regular basis. These tasks include:
  - Remove old user accounts.
  - Change passwords on a regular basis.
  - Remind users to use complex passwords.

## Password

A user may change his/her own password. Make sure that the specified password meets the following requirements:

- Consists of the following types of characters:
  - **Upper-case letters:** Specify at least one upper-case character (i.e., A-Z).
  - **Lower-case letters:** Specify at least one lower-case character (i.e., a-z).
  - **Numbers:** Specify at least one number (i.e., 0-9).
  - **Symbols:** Specify at least one symbol (e.g., !, @, and #).
- A minimum length of eight characters.
- Different from your current password.

# Log Files

---

## Overview

---

**Important:** Information on Real-Time Log Delivery may be found within the **Analytics Suite User Guide**.

---

A record of basic CDN activity can be archived as an asset in your CDN storage account or on an external server. This record is known as a raw log file. The following types of CDN activity/statistics are recorded in raw log files:

- Bandwidth usage
- Traffic statistics
- Cache
- Storage usage

Additionally, supplemental information is stored for each action that takes place. For example, the CDN and edge CNAME URLs associated with each request is also stored in our raw log files. Our reporting tools rely on this data to provide reports and graphs for the different types of CDN activity that took place for your account. For example, reports can be generated for the total amount of traffic generated by a particular region for your account, the hourly bandwidth for a particular platform, the amount of data transferred per platform, and cache hit statistics.

Log files are collected approximately every 15 minutes from around the world. If a server is unable to provide log file information at a given time, then the server will deliver it when communication resumes.

**Note:** Activity in a log file is time-stamped using GMT notation. This allows you to keep track of when an event took place, regardless of the time zone where it was recorded.

---

---

## Log File Naming Convention

The following naming convention is used to name raw log files:

- *Platform\_xxxx\_YYYYMMDD\_nnnn.log.gz*

As you may be able to tell from the above file naming convention, the following two file name extensions are assigned to raw log files:

- **Gz:** The .gz file name extension indicates that the raw log data has been compressed using the gzip file format. A software application is required to decompress this file type.
- **Log:** The .log file name extension indicates that the text file corresponds to a log file. Although this file type can be opened with a text editor, you may wish to open it using a third-party reports & analytics tool.

A description is provided for the different elements in the log file name.

Variable	Description
Platform	This term represents the CDN platform for which activity was logged. Valid values for this term are listed below: <ul style="list-style-type: none"><li>• <b>wpc:</b> HTTP Large platform</li><li>• <b>wac:</b> HTTP Small platform</li><li>• <b>adn:</b> Application Delivery Network platform</li></ul>
xxxx	This term represents your CDN account number (e.g., 0001). This account number can be viewed from the upper-right hand corner of the MCC.
YYYY	This term represents the four digit year on which the log file was generated by a CDN server.
MM	This term represents the two digit month on which the log file was generated by a CDN server.
DD	This term represents the two digit day on which the log file was generated by a CDN server.
nnnn	This term is replaced by a four digit number that ensures that all of the log files generated for the current day are assigned a unique name.

---

## Log File Storage

Basic log data is automatically archived on our servers. As a result, you will always be able to access basic information about your CDN activity data through the Core Reporting module. Core reports are available by finding the **Analytics** menu from within the main menu and then selecting **Core Reports**. However, you may wish to store more detailed log information or use a third-party tool to analyze your log data. For this reason, we allow you to store log information on a CDN origin server and/or to deliver them directly to your servers.

---

**Important:** Log files are not stored on CDN or customer storage by default. If you would like to retain this data, make sure to enable log file archival for CDN and/or customer storage.

**Important:** If you are unable to enable the storage and delivery of raw log files on a platform, it is due to the fact that CDN traffic for that platform is being tracked through a logless system. Platforms that have been assigned to a logless system will also be unable to take advantage of other log-dependent features, such as the following Analytics reporting modules: Advanced Content Analytics and Edge Performance Analytics. For more information, please contact your CDN account manager.

---

### CDN Storage (CDN Origin Server)

Log files can be automatically archived to a CDN origin server. Enabling log file archival will store log files for the selected platforms in a folder called "Logs" on your CDN origin server. You can access log data stored on a CDN origin server through your preferred FTP/SFTP client.

Log data storage options can be configured from the **Raw Log Settings** page. In addition to being able to turn it on/off on a per platform basis, you may also determine how long log files will be retained on the CDN origin server.

---

**Note:** Your account will be billed for the amount of storage space used on a CDN origin server. For a detailed explanation of account billing, please contact your CDN account manager.

---



### To configure log storage options

1. Navigate to the **Raw Log Settings** page.
2. Perform one of the following:
  - If you do not wish to archive log files on to CDN storage, then you should select the **Log storage is turned off** option.
  - If you would like to archive log files, then you should perform the following steps:
    - i. Make sure that the **Log storage is turned on** option is selected.
    - ii. Mark each platform for which you would like to store log data.
    - iii. Clear each platform for which log data will be discarded.
    - iv. In the **Please keep log files for** option, you should select the amount of time that the log files for each selected platform should be kept. If you choose "unlimited," then log files will not be automatically deleted from the CDN origin server.
3. Click **Update** to save your changes.

## External Storage

In addition to storing log data on CDN storage, it may also be delivered to your web server via SFTP. Additionally, opt-in to receive email notifications whenever a log file cannot be delivered to your web server.

---

**Important:** Due to the security risks inherent to FTP (e.g., authentication via cleartext passwords), log delivery over FTP is undergoing end-of-life and will only be available until September 1, 2018. If you are currently using FTP for log delivery, please update your log delivery configuration to use SFTP immediately.

**Reminder:** A prerequisite for archiving raw log files to your own server is enabling raw log file archival to CDN storage. If this is undesired, the length of time that raw log files will be stored on CDN storage can be minimized by setting the retention period to 1 day.

---

### To configure log file delivery settings

1. Navigate to the **Raw Log Settings** page.
2. Verify that raw log file storage has been enabled for the desired platforms.
3. Perform one of the following:
  - **Enable Log Delivery:** Archive log files to an external server by selecting the **Enabled** option from the **FTP and SFTP Delivery Settings** section.
  - **Disable Log Delivery:** If log files should not be archived to an external server, then make sure that the **Disabled** option is selected from the **FTP and SFTP Delivery Settings** section and then click **Update**. Skip all remaining steps.
4. In the **Log Delivery Type** option, verify that "SFTP" is selected.
5. In the **Port** option, select the port to which log data will be sent.
6. In the **Notification E-mail** option, type the email address to which an email will be sent when a log file is not successfully delivered to your server.
7. In the **Hostname** option, type the hostname or IP address of the server where log files will be archived. Make sure to exclude protocol information (i.e., sftp://).
8. In the **Directory Path** option, type the path to the folder where log files will be archived. This path starts at the root folder of the server specified in the previous step. Make sure to start this path with a forward slash (e.g., /Logs).
9. In the **Username** option, type the name of the user that has SFTP access to the specified server. Make sure that the specified user has been granted read/write to the folder defined in the **Directory Path** option.

10. Determine whether the above user will be authenticated via a password or a RSA private key.
  - **Password Authentication:** In the **Password** option, type the password associated with the specified user account.
  - **Private Key Authentication:** Perform the following steps:
    - i. Paste the desired RSA private key into the **Private Key Text** option.
    - ii. Make sure that the same private key is stored in the home directory assigned to the user specified in the **Username** option.
11. Click **Update** to save your settings.
12. Configure your firewall to allow access to the following subnetworks:

```
108.161.253.0/25
192.16.62.0/25
192.16.61.128/25
192.229.176.0/24
```

---

## Log File Format

As previously mentioned, raw log files are generated on a regular basis by our servers around the world. These servers will generate a raw log file for each platform for which they audited CDN activity. The log data generated for each platform varies due to the nature of the activity being recorded (e.g., HTTP GET requests vs. streaming). As a result, the log file format is different for each platform.

### HTTP Platforms

A single log file format is used to record CDN activity for the HTTP Large, HTTP Small, and Application Delivery Network platforms. This format can be customized, so that you can easily integrate CDN log data with your third-party report generation application. In addition to providing information on how to customize the log file format, we describe the default log file format and the fields that can be included in a log file. This information will help you get acquainted with the type of log information that you can leverage into a third-party report.

### Default Log File Format

The default format used to record HTTP activity in a raw log file is similar to an extended W3C log. An extended W3C log file is an ASCII text-based format defined by W3C and used as the default log file format by IIS. The main differences between our default log file format and the extended W3C log format are the following:

- Our servers record date and time as a single field using Unix time (a.k.a. POSIX time or Unix epoch) in our log files. A standard extended W3C log file format, on the other hand, records date and time as two separate fields using the GMT time zone. The date and time format used by the extended W3C log file format is described below.
  - **Date format (Extended W3C):** YYYY-MM-DD
  - **Time format (Extended W3C):** HH:MM, HH:MM:SS, or HH:MM:SS.S.

Our servers record an additional field where the account number associated with the customer is reported.

Our servers record an additional field called "x-ec\_custom-1" that can be used to log custom information. The information that will be logged by this field is determined by an HTTP Rules Engine feature.

The following list indicates the default order in which data is recorded in a raw log file:

Date/Time (timestamp)  
Time Taken (time-taken)  
Client IP Address (c-ip)  
File Size (filesize)  
Edge Server IP Address (s-ip)  
Edge Server Port (s-port)  
[Cache and HTTP] Status Code (sc-status)  
Bytes Sent (sc-bytes)  
HTTP Method (cs-method)  
Request URL (cs-uri-stem)  
-  
Remote Server Time Taken (rs-duration)  
Remote Server - Bytes Sent (rs-bytes)  
Referrer (c-referrer)  
User Agent (c-user-agent)  
Customer Account Number (customer-id)  
Custom Log Field 1 (x-ec\_custom-1)

---

**Note:** For a description of a particular field, please refer to the **Log File Field Definition** topic.

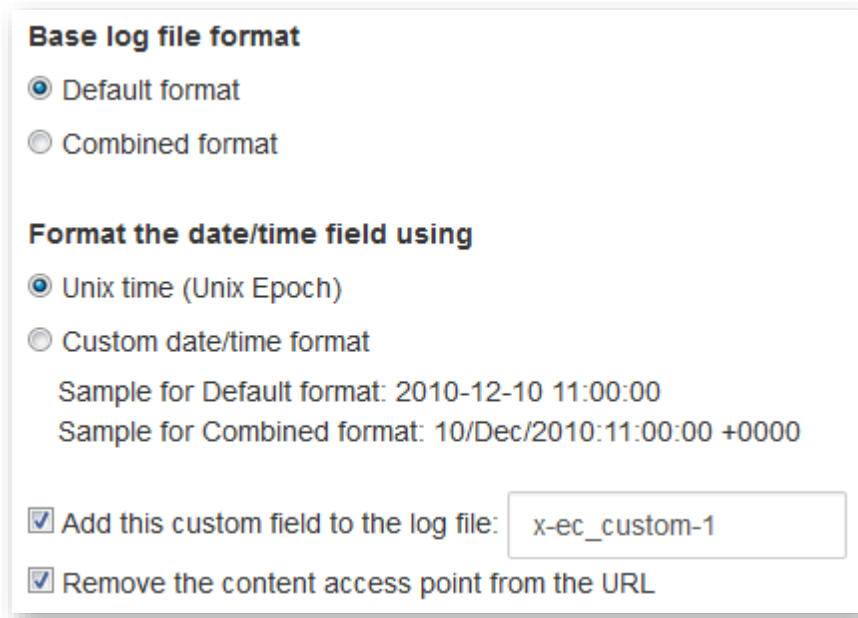
---

### [Restoring the Default Log File Format Configuration](#)

If you have customized how HTTP activity is recorded in our log files and would like to restore the default log file format, then you will need to make sure that the **Log Format Settings** section of the **Raw Log Settings** page is configured as follows:

- **Base log file format:** The **Default format** option should be selected.
- **Format the date/time field using:** The **Unix time (Unix Epoch)** option should be selected.
- **Add this custom field to the log file:** This option should be marked and set to "x-ec\_custom-1."
- **Remove the content access point from the URL:** This option should be cleared.

Your log file format settings should look like the following illustration:



**Base log file format**

Default format

Combined format

**Format the date/time field using**

Unix time (Unix Epoch)

Custom date/time format

Sample for Default format: 2010-12-10 11:00:00

Sample for Combined format: 10/Dec/2010:11:00:00 +0000

Add this custom field to the log file:

Remove the content access point from the URL

#### Default Log File Format Settings

### Log File Field Definition

Each raw log file consists of a set of fields that describe HTTP activity data. The exact set of fields that will be included in your raw log file depends on whether you have configured your raw log file to use the default or combined log file format. Additionally, you can also choose whether a custom field will be included in the raw log file and the header information that will be included. For more information, please refer to the **Custom Log File Format** topic.

The fields that can be defined in a raw log file are listed and described below.

---

**Note:** If you are using the combined log format, then the field names will not be reported as a header in each raw log file. For information on the order in which data will be recorded, please refer to the **Base Log File Format** section of the **Custom Log File Format** topic.

---

Field	Name	Applicable Log Format(s)	Description
-	-	Default	This field always reports "-."
c-ip	Client IP Address	Default Combined	The IP address of the client that made the request to the server.
c-referrer	Referrer	Default Combined	The URL of the site from which the request originated. This field will typically be set to "-" for the HTTP Small and the ADN platforms.

<b>Field</b>	<b>Name</b>	<b>Applicable Log Format(s)</b>	<b>Description</b>
cs-method	HTTP Method	Default	The type of action that was requested. This field is reported according to the HTTP method (i.e., GET, HEAD, POST, PUT, and DELETE) that was used to make the request.
cs-uri-stem	Request URL	Default Combined	The URL for the CDN content that was requested, posted, or deleted.
c-user-agent	User Agent	Default Combined	The user agent that the client used to perform CDN activity.
customer-id	Customer Account Number	Default	The customer account number through which the request was processed.
filesize	File Size	Default Combined	The size of the requested asset in bytes.
rs-bytes	Remote Server Bytes Sent	Default	The sum of the number of bytes read from both of the following sources: <ul style="list-style-type: none"> <li>• Requesting Client</li> <li>• Origin Server</li> </ul>
rs-duration	Remote Server Time Taken	Default	The length of time, in milliseconds, that it took the origin server to process the requested action. This field does not take into account network time.
sc-bytes	Bytes Sent	Default	The number of bytes that the edge server sent to the client.

Field	Name	Applicable Log Format(s)	Description
sc-status	Status Code	Default Combined	<p><b>Syntax:</b></p> <ul style="list-style-type: none"> <li>• <b>Default log file:</b> <i>CacheStatusCode/HTTPStatus Code</i></li> <li>• <b>Combined log file:</b> <i>HTTPStatusCode</i></li> </ul> <p><b>Status code definitions:</b></p> <ul style="list-style-type: none"> <li>• <b>CacheStatusCode:</b> The cache status code (e.g., TCP_HIT) returned by an edge server. For more information, please refer to the <b>Appendix A: Cache Status Codes</b>.</li> <li>• <b>HTTPStatusCode:</b> The HTTP status code (e.g., 200) that originated from an origin server, origin shield server, ADN gateway server, or an edge server.</li> </ul>
s-ip	Edge Server IP Address	Default	The IP address associated with the edge server that processed the request.
s-port	Edge Server Port	Default	The port number associated with the edge server that processed the request.
timestamp	Date/Time	Default Combined	The date and time (GMT) at which an edge server delivered the requested content to the client. The format in which date/time is reported is determined by your log file format settings. By default, this field is reported in Unix time. For more information, please refer to the <b>Default Log File Format</b> and <b>Custom Log File Format</b> topics.
time-taken	Time Taken	Default	The length of time, in milliseconds, that it took to process the requested action. This field does not take into account network time.



Field	Name	Applicable Log Format(s)	Description
x-ec_custom-1	Custom Log Field 1	Default	This is a custom field that can report request and response headers. This field will only appear in a raw log file when the <b>Add this custom field to the log file</b> option is marked. The type of headers that will be logged is determined by the rules that have been associated with each platform. For more information, please refer to the <b>Custom Field</b> section of the <b>Custom Log File Format</b> topic.

### Custom Log File Format

The format in which data generated for CDN activity over the HTTP protocol is stored in a raw log file is determined by the settings defined in the **Log Format Settings** section of the **Raw Log Settings** page. These log file formatting settings allow you to:

- Define the base log file format
- Define the date/time format
- Determine whether a custom field will be included
- Determine whether the content access point will be logged

---

**Important:** Typically, data mining tools require a consistent log format when analyzing data over a period of time. If you plan on using a data mining application on your log data, then it is key to keep changes to your log file to a minimum. Please contact your CDN account manager before making any changes.

---

## Base Log File Format

The base log file format determines the basic format that will be used to record HTTP activity in a raw log file. Once you have selected a base log file format, you can adjust other log file format settings (e.g., date/time format) to achieve your optimal log format. When choosing a base log file format, you will need to choose between the following two log file formats:

- **Default format:** The default log file format is similar to an extended W3C log file format. This type of format is described in the **Default Log File Format** topic.
- **Combined format:** A combined log file format is similar to the default log file format used by Apache web servers. The following list of fields indicates the type of data and the order in which it is recorded in a raw log file:
  - Client IP Address
  - Client Identification
  - Client User Name - HTTP Authentication
  - Date/Time
  - Request URL
  - Request Status Code
  - File Size
  - Referrer
  - User Agent
  - Custom Log Field 1

---

**Note:** Unlike the default log file format, the combined format does not provide a list of field headers in each raw log file.

**Note:** By default, the Client Identification and the Client User Name – HTTP Authentication fields report a dash (i.e., -) for each request.

**Note:** Custom Log Field 1 will only be reported if custom logging is turned on when the CDN activity being reported takes place.

---

## Date/Time Format

A CDN server records the date and time at which it processed the request for an asset in a log field called "timestamp." The format in which data is recorded in this field can be customized in one of the following ways:

- **Unix time (Unix Epoch):** Date and time can be recorded in the timestamp field as the number of seconds since Unix time (a.k.a. POSIX time or Unix epoch). Unix time starts on 1970-01-01 at 00:00:00 GMT. For example, if the timestamp field reports "1294401600" then the request was processed on 1/07/2011 at 12:00:00 GMT. This is the default format for the timestamp field.
- **Custom date/time (Default format):** If the base log file format is set to **Default format**, then selecting the **Custom date/time format** option will record date and time in the timestamp field using the following format: YYYY-MM-DD hh:mm:ss (e.g., 2012-01-07 12:00:00). Each date/time variable is defined below.
  - **YYYY:** Indicates a year in the Gregorian calendar using a four digit number (e.g., 2012).
  - **MM:** Indicates a month of the year between 01 (January) and 12 (December).
  - **DD:** Indicates a day of the month between 01 and 31.
  - **hh:** Indicates an hour of the day (GMT) between 00 and 24.
  - **mm:** Indicates minutes between 00 and 59.
  - **ss:** Indicates seconds between 00 and 59.
- **Custom date/time (Combined format):** If the base log file format is set to **Combined format**, then selecting the **Custom date/time format** option will record date and time in the timestamp field using the following format: DD/MMM/YYYY:hh:mm:ss +hhhh (e.g., 07/Jan/2011:12:00:00 +0800). Each date/time variable is defined below.
  - **DD:** Indicates a day of the month between 01 and 31.
  - **MMM:** Indicates a three letter abbreviation for a month of the year (e.g., Jan).
  - **YYYY:** Indicates a year in the Gregorian calendar using a four digit number (e.g., 2012).
  - **hh:** Indicates an hour of the day between 00 and 24.
  - **mm:** Indicates minutes between 00 and 59.
  - **ss:** Indicates seconds between 00 and 59.
  - **+hhhh:** Indicates the hour differential between the time reported and GMT.

## Custom Field

By default, a custom field called "x-ec\_custom-1" is included in your raw log files. If you have not configured HTTP Rules Engine to log data in this field, then it will always report "-" in your raw log files. However, if you have created a rule that includes the "Custom Log Field 1" feature, then you can log HTTP request and/or response headers in this custom field.

---

**Note:** Changing the name of your custom field will not affect whether HTTP request and/or response headers are logged.

**Reminder:** If you are using the combined log format, then the name associated with your custom log field will not be reported in your raw log file.

---

If you decide to take advantage of a custom field to log HTTP request and/or response headers, then you will need to create a rule that takes advantage of the "Custom Log Field 1" feature. When configuring the "Custom Log Field 1" feature, you will need to specify each request and response header that you would like to log. A header can be specified using the following syntax:

Header Type	Syntax	Example
Request	<code>%{requestheader}i</code>	<code>%{Accept-Encoding}i</code>
Response	<code>%{responseheader}o</code>	<code>%{Content-Type}o</code>

---

**Note:** Before specifying a header, you will need to know whether it is a request (inbound) or a response (outbound) header. This will allow you to add the appropriate identifier (i.e., i or o) to the header variable (e.g., `%{Cookie}i` or `%{Content-Range}o`).

---

If you would like to specify multiple headers, then it is recommended that you use a separator to indicate each header. For example, you could use an abbreviation for each header (e.g., AE: `%{Accept-Encoding}i` CT: `%{Content-Type}o`).

---

**Tip:** Adding the "Custom Log Field 1" feature to a rule that is set to match "Always" allows you to log all transactions for that platform.

**Note:** You must create a rule for each HTTP platform for which you would like to log data in the custom field.

---

If you decide that you do not wish to include a custom field, then you can clear the **Add this custom field to the log file** option. This will prevent HTTP Rules Engine from logging HTTP request and/or response headers in your log file.

## To determine whether header information will be logged

1. Navigate to the **Raw Log Settings** page.
2. Perform one of the following:
  - **To log header information:**
    - i. Make sure that the **Add this custom field to the log file** option is marked. If desired, you can change the name that will be assigned to your custom field. If you changed this setting, then you should click **Update**.
    - ii. Navigate to the **Rules Engine** page associated with the platform for which header information will be logged.
    - iii. If a rule that takes advantage of the "Custom Log Field 1" feature does not exist, then you will need to create one now. When configuring the "Custom Log Field 1" feature, you will need to specify each request and response header that you would like to log (e.g., `%{Accept-Encoding}i` and `%{Content-Type}o`). Save your rule by clicking **Add**.
    - iv. Repeat the previous step for each desired platform.

---

**Reminder:** Append the appropriate identifier (i.e., i or o) to the header name to indicate whether you would like to log requests (inbound) or responses (outbound).

---

- **To exclude the custom field from raw log data:**
  - i. Make sure that the **Add this custom field to the log file** option is cleared. If you changed this setting, then you should click **Update**.
  - ii. Navigate to the **Rules Engine** page associated with the platform for which header information will be logged.
  - iii. Modify or disable the rule that logs header information into your custom field.

## Content Access Point

A content access point is a relative path that starts directly after the CDN domain (e.g., `/800001/MyOrigin` or `/000001`). By default, this information is reported in the `cs-uri-stem` field in the log file. The `cs-uri-stem` field identifies the asset that was requested by the client. The **Remove the content access point from the URL** option determines whether this information is reported in that field.

---

## Third-Party Log Analysis Tools

Log data is collected from multiple servers around the world and then combined into a single log file. As a result of dealing with servers from the around the world, the time stamps associated with each logged item may not appear in sequential order. This may cause an issue with certain third-party log analysis tools. Therefore, you may need to adjust the configuration of your log analysis tool. Please refer to the documentation of your log analysis tool for configuration instructions.

---

**Note:** Certain log data, such as the loading of content into RAM or the pre-caching of content, is generated from communication between our servers. The URL for these log records will be recorded as `http://localhost/` or `http://127.0.0.1/`. You will need to configure your log analysis tool to exclude or ignore these entries.

**Note:** Although logged data may not appear in sequential order in the log files, the timestamp for each logged item will accurately reflect when the action took place using the GMT time zone.

---

# Network Status

---

## Overview

Track status information for all of our platforms, services, and POP locations through the **Network Status** page (<http://status.edgecast.com/>).

View the following information at a glance:

Status	Description
Overview	<p>A color-coded bar that indicates overall network status is provided at the top of the page.</p> <ul style="list-style-type: none"><li>• <b>Operational:</b> A green status bar will be displayed when all services are operational.</li><li>• <b>Active Incident:</b> A color-coded status bar that reads "Active Incident" will be displayed when at least one service is experiencing a performance-impacting incident.</li></ul>
Geographical	<p>A global map showing the health of each of our POPs is provided under the <b>Locations</b> section.</p> <hr/> <p><b>Tip:</b> View a POP's location and status information by hovering over it.</p> <hr/>
Active Incidents	<p>A section for each ongoing incident will be included on the <b>Network Status</b> page. Each section provides detailed information for an active incident.</p>
Service	<p>A list of services and their current status is provided below active incidents.</p>
Historical	<p>A historical log of incidents for the last two days is provided at the bottom of the page.</p> <hr/> <p><b>Note:</b> This incident log excludes any ongoing incidents.</p> <hr/>

---

## Network Status Notifications

Be automatically notified of maintenance windows and network status updates by subscribing to receive status updates.

---

**Important:** Push notifications are managed by a third-party vendor called "Status.io." By subscribing to receive status notifications, you agree to share your contact information with Status.io and be covered by their security and privacy policies.

---

Subscribe to receive notifications by performing the following steps:

1. From the **Network Status** page, click **Subscribe**.
2. Perform one of the following tasks:

<b>Delivery Method</b>	<b>Procedure</b>
Email	Perform the following steps to receive notifications by email: <ol style="list-style-type: none"><li>1. From the <b>Email</b> tab, type the email address to which email notifications will be sent.</li><li>2. Click <b>Agree and Subscribe</b>.</li></ol>
Text Message (SMS)	Perform the following steps to receive notifications by text message: <ol style="list-style-type: none"><li>1. From the <b>SMS</b> tab, select the country associated with the desired phone number.</li><li>2. Type the desired phone number. <hr/><b>Note:</b> Make sure to include an area code or city code as needed.<hr/></li><li>3. Click <b>Agree and Subscribe</b>.</li></ol>
Web Server (Webhook)	Perform the following steps to push notifications to a web server: <ol style="list-style-type: none"><li>1. From the <b>Webhook</b> tab, define the URL to which a HTTP POST request will be sent.</li><li>2. Type the email address through which this webhook will be managed.</li><li>3. Click <b>Agree and Subscribe</b>.</li><li>4. Update your web server to perform a custom action upon receiving each POST request.</li></ol>
RSS Feed	View our <a href="#">RSS feed</a> by clicking the "RSS Feed" link from the <b>RSS</b> tab. <hr/> <b>Important:</b> The available subscription options depends on the browser used to access the RSS feed. <hr/>



3. Repeat steps 1 and 2 as needed.

#### **To manage your status notification subscription**

1. Find an email sent by Edgecast Notification <noreply@status.io>. An email may be sent from this sender under the following circumstances:
  - Upon signing up to receive status notifications by email.
  - Whenever an incident is created or updated.
  - Whenever a maintenance window is scheduled or updated.
2. Click the "Manage my preferences" or the subscription confirmation link.
3. Perform one or more of the following steps:
  - **Update your Email Address:**
    - i. From the **Email Address** option, type the desired email address.
    - ii. Click **Save Subscription** to save the updated email address.
  - **Add or Remove Notifications:**
    - i. Mark or clear the desired notifications.
    - ii. Click **Save Subscription** to save the updated notification settings.
  - **Unsubscribe:** Click the "Unsubscribe" link from the bottom of the page.

---

**Note:** Unsubscribe from our RSS feed via the browser, add-on, or RSS reader through which the subscription was initiated.

---

# Appendix A

---

## Cache Status Codes

Each cache status that is reported for CDN activity is defined below.

Cache Status	Description
CONFIG_NOCACHE	This status indicates that a customer-specific configuration on our edge servers prevented the asset from being cached. For example, an HTTP Rules Engine rule can prevent an asset from being cached by enabling the Bypass Cache feature for qualifying requests.
NONE	This status indicates that a cache content freshness check was not performed. This check is skipped when Token-Based Authentication denies a request or when an HTTP request method is used that bypasses cache (e.g., PUT, DELETE, etc).
TCP_CLIENT_REFRESH_MISS	<p>This status is reported when an HTTP client (e.g., browser) forces an edge server to retrieve a new version of a stale asset from the origin server.</p> <p>By default, our servers prevent an HTTP client from forcing our edge servers to retrieve a new version of the asset from the origin server. However, this behavior can be overridden through the use of the HTTP Rules Engine feature called "Honor No-Cache Request."</p>
TCP_EXPIRED_HIT	This status is reported when a request that targeted an asset with an expired time to live (TTL), such as when the asset's max-age has expired, was served directly from the POP to the client. An expired request typically results in a revalidation request to the origin server. In order for a TCP_EXPIRED_HIT to occur, the origin server must indicate that a newer version of the asset does not exist. This type of situation will typically update that asset's Cache-Control and Expires headers.
TCP_EXPIRED_MISS	This status is reported when a newer version of an expired cached asset is served from the POP to the client. This occurs when the TTL for a cached asset has expired (e.g., expired max-age) and the origin server returns a newer version of that asset. This new version of the asset will be served to the client instead of the cached version. Additionally, it will be cached on the edge server and the client.

Cache Status	Description
TCP_HIT	This status is reported when a request is served directly from the POP to the client. An asset is immediately served from a POP when it is cached on the POP closest to the client and it has a valid TTL. TTL is determined by the Cache-Control: s-maxage, Cache-Control: max-age, and Expires headers.
TCP_MISS	This status indicates that a cached version of the requested asset was not found on the POP closest to the client. The asset will be requested from either an origin server or an origin shield server. If the origin server or the origin shield server returns an asset, it will be served to the client and cached on both the client and the edge server. Otherwise, a non-200 status code (e.g., 403 Forbidden, 404 Not Found, etc.) will be returned.
TCP_PARTIAL_HIT	<p>This status is reported when a request results in a hit for a partially cached asset. The requested asset is immediately served from the POP to the client.</p> <hr/> <p><b>Note:</b> The Partial Cache Sharing feature (HTTP Rules Engine) enables the capability to generate partially cached content.</p> <hr/>
UNCACHEABLE	This status is reported when an asset's Cache-Control and Expires headers indicate that it should not be cached on a POP or by the HTTP client. These types of requests are served from the origin server.

# Appendix B

## Privileges

A description and the scope of each privilege are provided below.

**Note:** Certain privileges only determine whether a menu item will be enabled. If a user navigates to that menu item, then the first child page, as determined by the order in which the permissions are listed below, for which that user has been granted access will be loaded. If all of the children of that parent privilege have been denied to that user, then the user will receive a message indicating insufficient access.

Privilege	Secures	Additional Information
Dashboard	<b>Dashboard</b> page	If a user does not have this privilege, then the default start page for that user will be the page associated with the first menu item for which that user has privileges. This is calculated from the left hand side of the page to the right.
HTTP Large	<b>HTTP Large</b> menu item	
HTTP Large Object	<b>HTTP Large Object</b> page	This privilege does not affect a user's ability to use the URLs that are displayed on this page.
Customer Origin	<b>Customer Origin</b> page	
Edge CNAMEs	<b>Edge CNAMEs</b> page	
Token Auth	<b>Token Auth</b> page	This privilege does not control whether a knowledgeable user with the proper resources (i.e., current encryption key and encoder/decoder) can encrypt and/or decrypt token values.
Country Filtering	<b>Country Filtering</b> page	
Cache Settings	<b>Cache Settings</b> menu item	
Query-String Caching	<b>Query-String Caching</b> page	
Query-String Logging	<b>Query-String Logging</b> page	

<b>Privilege</b>	<b>Secures</b>	<b>Additional Information</b>
Compression	<b>Compression</b> page	
HTTP Streaming	<b>HTTP Streaming</b> menu item	
Rules Engine	<b>Rules Engine</b> page	
Purge/Load	<b>Purge/Load</b> page	
HTTP Small	<b>HTTP Small</b> menu item	
HTTP Small Object	<b>HTTP Small Object</b> page	This privilege does not affect a user's ability to use the URLs that are displayed on this page.
Customer Origin	<b>Customer Origin</b> page	
Edge CNAMEs	<b>Edge CNAMEs</b> page	
Token Auth	<b>Token Auth</b> page	This privilege does not control whether a knowledgeable user with the proper resources (i.e., current encryption key and encoder/decoder) can encrypt and/or decrypt token values.
Country Filtering	<b>Country Filtering</b> page	
Cache Settings	<b>Cache Setting</b> menu item	
Query-String Caching	<b>Query-String Caching</b> page	
Query-String Logging	<b>Query-String Logging</b> page	
Compression	<b>Compression</b> page	
Rules Engine	<b>Rules Engine</b> page	
Purge/Load	<b>Purge/Load</b> page	
ADN	<b>ADN</b> menu item	
Application Delivery Network	<b>Application Delivery Network</b> page	This privilege does not affect a user's ability to use the URLs that are displayed on this page.
Customer Origin	<b>Customer Origin</b> page	
Edge CNAMEs	<b>Edge CNAMEs</b> page	

<b>Privilege</b>	<b>Secures</b>	<b>Additional Information</b>
Token Auth	<b>Token Auth</b> page	This privilege does not control whether a knowledgeable user with the proper resources (i.e., current encryption key and encoder/decoder) can encrypt and/or decrypt token values.
Country Filtering	<b>Country Filtering</b> page	
Cache Settings	<b>Cache Setting</b> menu item	
Query-String Caching	<b>Query-String Caching</b> page	
Query-String Logging	<b>Query-String Logging</b> page	
Compression	<b>Compression</b> page	
Rules Engine	<b>Rules Engine</b> page	
Purge/Load	<b>Purge/Load</b> page	
Defend	<b>Defend</b> menu item	
WAF	<b>WAF</b> menu item	
Welcome	<b>Welcome</b> page	
Dashboard	<b>Dashboard</b> page	
Profile Manager	<b>Profile Manager</b> page	This privilege contains sub-privileges that determine whether a user may create, edit, delete, or view a profile.
Instance Manager	<b>Instance Manager</b> page	This privilege contains sub-privileges that determine whether a user may create, edit, delete, or view an instance.
HTTP Rate Limiting	<b>HTTP Rate Limiting</b> menu item	
Dashboard	<b>Dashboard</b> page	
Rate Limiting Rules	<b>Rate Limiting Rules</b> page	
Storage	<b>Storage</b> menu item	

<b>Privilege</b>	<b>Secures</b>	<b>Additional Information</b>
FTP	<b>FTP</b> page	<p>This privilege also determines whether a user will be able to authenticate to CDN storage via a third-party FTP client.</p> <hr/> <p><b>Important:</b> If a user account has access to multiple customer accounts, please limit the user's CDN storage access to a single customer account.</p> <hr/>
RSYNC	<b>RSYNC</b> page	<p>This privilege also determines whether a user will be able to authenticate to CDN storage via a third-party RSYNC tool.</p> <hr/> <p><b>Important:</b> If a user account has access to multiple customer accounts, please limit the user's CDN storage access to a single customer account.</p> <hr/>
Route (DNS)	<b>Route (DNS)</b> menu item	
Analytics	<b>Analytics</b> menu item	
Core Reports	<b>Core Reports</b> menu item	
Traffic Summary	<b>Traffic Summary</b> page	
Bandwidth	<b>Bandwidth</b> menu item	<p>Each individual Bandwidth report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below.</p> <ul style="list-style-type: none"> <li>• HTTP Large</li> <li>• HTTPS Large</li> <li>• HTTP Small</li> <li>• HTTPS Small</li> <li>• ADN</li> <li>• ADN SSL</li> </ul>

Privilege	Secures	Additional Information
Data Transferred	<b>Data Transferred</b> menu item	<p>Each individual Data Transferred report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below.</p> <ul style="list-style-type: none"> <li>• HTTP Large</li> <li>• HTTPS Large</li> <li>• HTTP Small</li> <li>• HTTPS Small</li> <li>• ADN</li> <li>• ADN SSL</li> </ul>
Hits	<b>Hits</b> menu item	<p>Each individual Hits report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below.</p> <ul style="list-style-type: none"> <li>• All Platforms</li> <li>• HTTP Large</li> <li>• HTTP Small</li> <li>• ADN</li> </ul>
Cache Statuses	<b>Cache Statuses</b> menu item	<p>Each individual Cache Statuses report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below.</p> <ul style="list-style-type: none"> <li>• All Platforms</li> <li>• HTTP Large</li> <li>• HTTP Small</li> <li>• ADN</li> </ul>



<b>Privilege</b>	<b>Secures</b>	<b>Additional Information</b>
Cache Hit Ratio	<b>Cache Hit Ratio</b> menu item	Each individual Cache Hit Ratio report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below. <ul style="list-style-type: none"> <li>• All Platforms</li> <li>• HTTP Large</li> <li>• HTTP Small</li> <li>• ADN</li> </ul>
Cnames	<b>Cnames</b> menu item	Each individual Cnames report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below. <ul style="list-style-type: none"> <li>• All Platforms</li> <li>• HTTP Large</li> <li>• HTTP Small</li> <li>• ADN</li> </ul>
CDN Storage	<b>CDN Storage</b> menu item	
Usage	<b>Usage</b> page	
IPv4/IPv6	<b>IPv4/IPv6</b> menu item	
Data Transferred	<b>IPv4/IPv6 Data Transferred</b> page	
DNS	<b>DNS</b> menu item	
Route Summary Query	<b>Route Summary Query Count</b> page	
Notes	<b>Notes</b> page	
Custom Reports	<b>Custom Reports</b> menu item	

Privilege	Secures	Additional Information
Edge CNAMEs	<b>Edge CNAMEs</b> page	<p>Each individual report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below.</p> <ul style="list-style-type: none"> <li>• All Platforms</li> <li>• HTTP Large</li> <li>• HTTP Small</li> <li>• ADN</li> </ul>
Notes	<b>Notes</b> page	
Advanced HTTP Reports	<b>Advanced HTTP Reports</b> menu item	

Privilege	Secures	Additional Information
HTTP Large Platform	<b>HTTP Large Platform</b> menu item	<p>Each individual Advanced HTTP (HTTP Large) report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below.</p> <ul style="list-style-type: none"> <li>• World Map</li> <li>• United States Map</li> <li>• Canada Map</li> <li>• Europe Map</li> <li>• Asia Pacific Map</li> <li>• Top Cities</li> <li>• Top Countries</li> <li>• Daily Summary</li> <li>• By Hour</li> <li>• By File</li> <li>• By File Detail</li> <li>• By File Type</li> <li>• By Directory</li> <li>• By Browser</li> <li>• By Referrer</li> <li>• By Download</li> <li>• By 404 Errors</li> </ul>
Notes	<b>Notes</b> page	
Advanced ADN Reports	<b>Advanced ADN Reports</b> menu item	

Privilege	Secures	Additional Information
ADN Platform	<b>ADN Platform</b> menu item	<p>Each individual Advanced ADN report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below.</p> <ul style="list-style-type: none"> <li>• World Map</li> <li>• United States Map</li> <li>• Canada Map</li> <li>• Europe Map</li> <li>• Asia Pacific Map</li> <li>• Top Cities</li> <li>• Top Countries</li> <li>• Daily Summary</li> <li>• By Hour</li> <li>• By File</li> <li>• By File Detail</li> <li>• By File Type</li> <li>• By Directory</li> <li>• By Browser</li> <li>• By Referrer</li> <li>• By Download</li> <li>• By 404 Errors</li> </ul>
Notes	<b>Notes</b> page	
Advanced Streaming Reports	<b>Advanced Streaming Reports</b> menu item	
Notes	<b>Notes</b> page	

Privilege	Secures	Additional Information
Real-Time Stats	<b>Real-Time Stats</b> menu item	<p>Each individual Real-Time Statistics report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below.</p> <ul style="list-style-type: none"> <li>• Overview</li> <li>• HTTP Large Object</li> <li>• HTTP Small Object</li> <li>• ADN</li> <li>• Other Stats</li> <li>• Real-Time Alerts</li> </ul>
Edge Performance Analytics	<b>Edge Performance Analytics</b> menu item	
Dashboard	<b>Dashboard</b> page	
HTTP Large Object	<b>HTTP Large Object</b> page	<p>Each individual HTTP Large (Edge Performance Analytics) report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below.</p> <ul style="list-style-type: none"> <li>• Daily Summary</li> <li>• Hourly Summary</li> <li>• Protocols</li> <li>• HTTP Methods</li> <li>• URLs</li> <li>• Cnames</li> <li>• Origins</li> <li>• Geo POPs</li> <li>• Clients</li> <li>• Cache Statuses</li> <li>• NONE Details</li> <li>• CONFIG_NOCACHE Details</li> <li>• UNCACHEABLE Details</li> </ul>

Privilege	Secures	Additional Information
		<ul style="list-style-type: none"> <li>• TCP_HIT Details</li> <li>• TCP_MISS Details</li> <li>• TCP_EXPIRED_HIT Details</li> <li>• TCP_EXPIRED_MISS Details</li> <li>• TCP_CLIENT_REFRESH_MISS Details</li> <li>• Client Request Types</li> <li>• User Agents</li> <li>• Referrers</li> <li>• Compression Types</li> <li>• File Types</li> <li>• Unique Files</li> <li>• Token Auth Summary</li> <li>• Token Auth Deny Details</li> <li>• HTTP Response Codes</li> <li>• 404 Errors</li> <li>• 403 Errors</li> <li>• 4xx Errors</li> <li>• 504 Errors</li> <li>• 502 Errors</li> <li>• 5xx Errors</li> </ul>

Privilege	Secures	Additional Information
HTTP Small Object	HTTP Small Object page	<p>Each individual HTTP Small Object (Edge Performance Analytics) report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below.</p> <ul style="list-style-type: none"> <li>• Daily Summary</li> <li>• Hourly Summary</li> <li>• Protocols</li> <li>• HTTP Methods</li> <li>• URLs</li> <li>• Cnames</li> <li>• Origins</li> <li>• Geo POPs</li> <li>• Clients</li> <li>• Cache Statuses</li> <li>• NONE Details</li> <li>• CONFIG_NOCACHE Details</li> <li>• UNCACHEABLE Details</li> <li>• TCP_HIT Details</li> <li>• TCP_MISS Details</li> <li>• TCP_EXPIRED_HIT Details</li> <li>• TCP_EXPIRED_MISS Details</li> <li>• TCP_CLIENT_REFRESH_MISS Details</li> <li>• Client Request Types</li> <li>• User Agents</li> <li>• Compression Types</li> <li>• File Types</li> <li>• Unique Files</li> <li>• Token Auth Summary</li> <li>• Token Auth Deny Details</li> </ul>

Privilege	Secures	Additional Information
		<ul style="list-style-type: none"> <li>• HTTP Response Codes</li> <li>• 404 Errors</li> <li>• 403 Errors</li> <li>• 4xx Errors</li> <li>• 504 Errors</li> <li>• 502 Errors</li> <li>• 5xx Errors</li> </ul>
ADN	ADN page	<p>Each individual ADN (Edge Performance Analytics) report has a dedicated privilege that controls whether a user will be allowed to access the page on which that report resides. These privileges are listed below.</p> <ul style="list-style-type: none"> <li>• Daily Summary</li> <li>• Hourly Summary</li> <li>• Protocols</li> <li>• HTTP Methods</li> <li>• URLs</li> <li>• Cnames</li> <li>• Origins</li> <li>• Geo POPs</li> <li>• Clients</li> <li>• Cache Statuses</li> <li>• NONE Details</li> <li>• CONFIG_NOCACHE Details</li> <li>• UNCACHEABLE Details</li> <li>• TCP_HIT Details</li> <li>• TCP_MISS Details</li> <li>• TCP_EXPIRED_HIT Details</li> <li>• TCP_EXPIRED_MISS Details</li> <li>• TCP_CLIENT_REFRESH_MISS Details</li> </ul>



Privilege	Secures	Additional Information
		<ul style="list-style-type: none"> <li>• Client Request Types</li> <li>• User Agents</li> <li>• Compression Types</li> <li>• File Types</li> <li>• Unique Files</li> <li>• Token Auth Summary</li> <li>• Token Auth Deny Details</li> <li>• HTTP Response Codes</li> <li>• 404 Errors</li> <li>• 403 Errors</li> <li>• 4xx Errors</li> <li>• 504 Errors</li> <li>• 502 Errors</li> <li>• 5xx Errors</li> </ul>
Raw Log Settings	<b>Raw Log Settings</b> page	
Real-Time Log Settings	<b>Real-Time Log Settings</b> page	
Report Builder	<b>Report Builder</b> page	
Tools	<b>Tools</b> menu item	
JW Player	<b>JW Player</b> page	
Smooth Streaming Player	<b>Smooth Streaming Player</b> page	
Token Generator	<b>Token Generator</b> page	
Video Support Player	<b>Video Support Player</b> page	
Admin	<b>Admin</b> menu item	

Privilege	Secures	Additional Information
Users	Users page	<p>In addition to granting access to the <b>Users</b> page, this privilege also allows read-only access to each user's properties.</p> <p>This privilege contains the following sub-privileges:</p> <ul style="list-style-type: none"> <li>• <b>Add user administration:</b> Grants the ability to create users.</li> <li>• <b>Edit user administration:</b> Grants the ability to modify a user's settings.</li> </ul> <hr/> <p><b>Note:</b> A user's custom ID may be defined when adding or modifying a user.</p> <hr/>
Company Settings	Company Settings menu item	

---

## Web Services REST API Access

Our REST API endpoints are organized by service, such as `mcc`, `reporting`, and `realtimestats`. These services allow you to automate core CDN tasks, such as:

- Purging content
- Loading content
- Administering publishing points for streaming
- Generate report data
- Retrieve real-time statistics on CDN usage

The ability to automate tasks through our endpoints requires the use of a Web Service REST API token. A unique Web Service REST API token is assigned to a user when one or more HTTP methods have been granted. The available types of HTTP methods are described below.

HTTP Method	Description
GET	Retrieves report data and information about your CDN configuration.
POST	Creates a CDN configuration (e.g., customer origins or edge CNAMEs).
PUT	Use this HTTP method to: <ul style="list-style-type: none"><li>• Perform actions (e.g., purge and load content)</li><li>• Define CDN settings (e.g., cache settings)</li><li>• Update a CDN configuration (e.g., customer origins or edge CNAMEs)</li></ul>
DELETE	Deletes a CDN configuration (e.g., customer origin and edge CNAMEs)

---

**Note:** A HTTP method must be specified when calling an endpoint. This method determines the type of action that will take place.

---

A request to our REST API will only be honored when the user associated with the token has been granted sufficient permissions. Specifically, the user must be granted both the HTTP method (i.e., GET, PUT, POST, or DELETE) being requested and sufficient privileges to perform the action within the MCC.

---

**Important:** A request submitted with a token with insufficient permissions will return a 403 Forbidden.

---

### To define a user's level of access to the REST API

1. Navigate to the **Users** page.
2. Click on the desired user.
3. Click **Permissions**.
4. Under the **API Access** section, determine the scope of a user's API access by marking or clearing the checkboxes that appear next to each HTTP method.
5. Under the **User Access Modules** section, grant the privileges that correspond to the set of actions that will be automated.
6. Click **Save**.