

# Puffin Enterprise Cloud Portal Help

## Quick Start

---

Puffin Enterprise Cloud Portal is a cloud security admin console which allows you to track license usage and configure Internet security policies for Puffin users in your organization.

### Track license usage

**Dashboard** provides a quick overall picture of the available and taken seats in your enterprise license. Click the numbers on the top section for active device information.

### Enforce website access rules

**Web filtering** allows you to create blacklists and whitelists of Internet destinations to fend off potential threats. Scroll to **Add a new filtering rule** and add rules as needed.

### Perform system-wide configurations and site-specific security policies

System-wide file download, file upload, and certification verification (Enterprise-only) policies can be configured in **Configurations**. In addition to global settings, site-specific security settings can be configured in **Security policy**.

### Manage Puffin users

User whitelist lets you set the access permissions for Puffin Secure Browser based on individual user email addresses. By default, all users under your corporate domain can register to use Puffin Secure Browser. You can change the setting by deleting the default rule `@domain.com`. Then, add or import user email addresses to the whitelist.

### Control IP-based access (Enterprise feature)

IP access lists restrict Internet browsing in Puffin Secure Browser to specific IP addresses or IP address ranges. Scroll to **Add a new whitelisted IP address** and add IP addresses as needed.

## Dashboard

---

Dashboard presents a quick overall picture of the available and taken seats in your enterprise license. The following sections display different information about your license usage.

- **Monthly active devices** This section displays the number of active devices versus the maximum number of devices allowed in your enterprise plan. Click on the number to see detailed information on device IDs, their last active users, and last login time.
- **Other information** Dashboard also displays other information for your reference.
  - **User ID:** Your enterprise ID, also the username for logging into Puffin Enterprise Cloud Portal.

- **License type:** The license type of the plan you purchased from us.
- **Registration date:** The date your account is created.
- **Contact mail:** The IT administrator responsible for configuring settings on Enterprise Cloud Portal.
- **User whitelist:** Whether you have configured the User whitelist or not.
- **Web filtering:** Whether you have configured web filtering rules or not.
- **IP access lists (Enterprise feature):** Whether you have configured IP access lists or not.

## Web filtering

As an IT administrator, you can blacklist and whitelist URLs to prevent users from visiting certain websites. By taking control of users' Internet browsing, your organization is protected from viruses and malicious content found on some websites.

To enable web filtering for your organization, tick the checkbox **Enable web filter**.

### How do I configure Web filtering?

Web filtering can be done by two approaches: (1) allowing all websites and selectively blocking some (default, suitable for work environments), and (2) blocking all and selectively allowing some (suitable for educational institutions).

#### Approach 1: Allow access to all websites and add rules to block certain websites

By default, Puffin users are allowed to access all websites. When visiting **Web filtering** for the first time, the default rule **ALLOW \*** is placed at the bottom.

**Puffin Enterprise**

Dashboard  
Web filtering  
Security policy  
User whitelist  
IP access lists  
Registered users  
Active devices  
Configurations  
Access logs

### Web filtering

☒ **Enable web filter**

Web filtering allows you to set up rules to block or allow access to specific websites in the format of domains, hostnames, or specific URLs. ([How it works.](#))

**Add a new filtering rule**

Insert a rule before position: **1**

- Select - Domain, hostname, or page URL Add

Sample target	Type	Case sensitive	Web pages can be matched	Details
*	Everything	N	All web pages	<a href="#">i</a>
*.example.com	Domain	N	Pages of all hosts under the domain	<a href="#">i</a>
www.example.com	Hostname	N	Pages of a single host	<a href="#">i</a>
http://www.example.com/xyz	Page URL	Y	Pages starting with the same prefix	<a href="#">i</a>

**Filtering rules** Import/export

Pos.	Action	Target	Type	Priority
1.	ALLOW	*	Everything	

[Test an URL against composed filtering rules](#)

How to add a new rule:

1. Scroll to **Add a new filtering rule**.
2. (Optional) Set the position you want to insert the rule. The default is 1, at the top.

3. Toggle the dropdown list to select **ALLOW** or **BLOCK**. When no option is selected, **BLOCK** takes precedence.
4. Enter the domain, hostname, or URL you want to include in the input field.
5. Click **Add**.
6. The rule is added. It will take effect after users relaunch their Puffin Secure Browser.

**Note:** For blocking rules to work properly, the rule **ALLOW \*** must stay at the bottom of the list, indicating that it is the last rule for the web filtering service to check.

**Tip:** The web page includes instructions on the URL formats that Puffin Enterprise Cloud Portal supports. You can also refer to the *Work with URL formats* section for further details.

## Approach 2: Block access to all websites and add rules to allow certain websites

In educational institutions, educators may want to only whitelist certain educational websites and block juvenile students' access to inappropriate websites. In this case, the default rule **ALLOW \*** should be removed before the rule **BLOCK \***, which blocks access to all websites, can be added.

**How to remove the ALLOW \* rule:**

The screenshot shows the Puffin Enterprise Web filtering interface. On the left is a sidebar with navigation links: Dashboard, Web filtering, Security policy, User whitelist, IP access lists, Registered users, Active devices, Configurations, and Access logs. The main content area is titled 'Web filtering' and includes a toggle for 'Enable web filter'. Below this is a section 'Add a new filtering rule' with a success message: 'OK: new rule added and will be applied to new user connections'. It shows 'Insert a rule before position: 1'. A dropdown menu is set to '- Select -' and the input field contains 'Domain, hostname, or page URL'. Below this is a table with sample targets and their details. At the bottom is a 'Filtering rules' table with two rules: '1. ALLOW www.mit.edu Hostname' and '2. ALLOW \* Everything'. The first rule has a down arrow icon in its priority column, and the second rule has an up arrow icon. A 'Test an URL against composed filtering rules' link is at the bottom.

Sample target	Type	Case sensitive	Web pages can be matched	Details
*	Everything	N	All web pages	
*.example.com	Domain	N	Pages of all hosts under the domain	
www.example.com	Hostname	N	Pages of a single host	
http://www.example.com/xyz	Page URL	Y	Pages starting with the same prefix	

Pos.	Action	Target	Type	Priority	
1.	ALLOW	www.mit.edu	Hostname		
2.	ALLOW	*	Everything		

1. Scroll to **Add a new filtering rule**.
2. Then, add a rule which whitelists a website first.
3. Toggle the dropdown list and select **ALLOW**.
4. Enter the domain, hostname, or URL you want to include in the input field.
5. Click **Add**.
6. Click the down arrow to change the order of the rule you just added.
7. The rule is now below the rule **ALLOW \***.
8. The Trash icon now appears next to the rule **ALLOW \***.
9. Click the Trash icon to delete the rule.

10. Add a rule which blocks all websites.
11. Toggle the dropdown list and select **BLOCK**. Enter the wildcard character `*` in the input field.
12. Click **Add**.
13. Move the rule `BLOCK *` to the bottom of the list.
14. You can now start adding more URLs you want to whitelist by selecting **ALLOW** and entering domains, hostnames, or URLs.

**Note:** For blocking rules to work correctly, the rule `BLOCK *` must stay at the bottom of the list, indicating that it is the last rule for the web filtering service to check.

**Tip:** The page includes instructions on the URL formats that Puffin Enterprise Cloud Portal supports. You can also refer to the *Work with URL formats* section for further details.

## Work with URL formats

Puffin Enterprise Cloud Portal supports four types of URL formats, namely, the wildcard notation `\*` that includes all websites, domain names, hostnames, and page URLs.

### Allow or block all websites

The rule `ALLOW *` is enabled by default. The asterisk `*` encompasses all websites.

Similarly, using an asterisk in a blocking rule `BLOCK *` blocks all websites. Refer to *Approach 2: Block access to all websites and add rules to allow certain websites* for instructions on adding a universal blocking rule.

**Note:** Be careful with using an asterisk as it would affect all browsing activities throughout your organization.

### Allow or block a whole domain

To include all web pages under a domain in a rule, place the wildcard notation `*` at the beginning of a domain and followed by a dot (.), e.g. `*.example.com`. `*.example.com` covers `login.example.com`, `www.example.com/example`, and so on.

It is not possible to use an asterisk to wildcard a different part of the domain. The following examples will **not** work:

- `example*.com`
- `*example.com`
- `example.*`

### Allow or block a hostname

To include all web pages under a hostname, enter the hostname to the rule, e.g. `www.example.com`. `www.example.com` covers all pages under `www.example.com`, but not `login.example.com` or `example.com`.

### Allow or block specific page URLs

Web filtering also supports allowing or blocking full URLs. You can allow or block certain parts of a website based specifically on the full URL. The full URL in a rule will be treated as a prefix, and all subordinate pages underneath would be covered by the rule.

## URL normalization for web filtering

Puffin Web filtering conforms to several URL normalization standards. There are certain guidelines to be followed to ensure that the URLs you enter would actually be allowed or blocked. The URL normalization criteria are listed as follows.

URL type	Guideline
Protocol Schema (both HTTP and HTTPS protocols are included; other protocols are not supported)	<code>http://www.example.com</code> or <code>https://www.example.com</code>
Username:Password (should be stripped)	<code>user:pass@example.com</code> → <code>example.com</code>
Ports (should be stripped)	<code>example.com:8080/abc</code> → <code>example.com/abc</code>
Trailing slashes (disregarded if entered)	<code>example.com/abc/</code> → <code>example.com/abc</code>
Character case (normalized to all lower case)	<code>EXAMPLE.cOm/abC</code> → <code>example.com/abc</code>
Page anchors (the hash sign #, automatically stripped)	<code>example.com/#info</code> → <code>example.com</code>

Web filtering only supports plainly defined rules. Using regular expressions is not supported.

## Quick verification of web filtering rules

Puffin Enterprise Cloud Portal provides a tool for you to quickly verify if the websites you want to allow or block are covered by the rules you have defined.

1. Scroll to **Test an URL against composed filtering rules**.
2. In the field next to **URL to test**, enter the URL you want to check.
3. Click **Test**.
4. If the URL can be accessed, the result would be **ALLOW**. If the URL is blocked, the result would be **BLOCK**.

### Composed filtering rules

[Import/export](#)

Pos.	Action	Target	Type	Priority	
1.	BLOCK	*.example.com	Domain	↓	🗑️
2.	ALLOW	*	Everything	↑	

#### Test an URL against composed filtering rules

URL to test

Test result: **BLOCK**

If you encounter any URLs which web filtering cannot allow or block, feel free to contact our customer service.

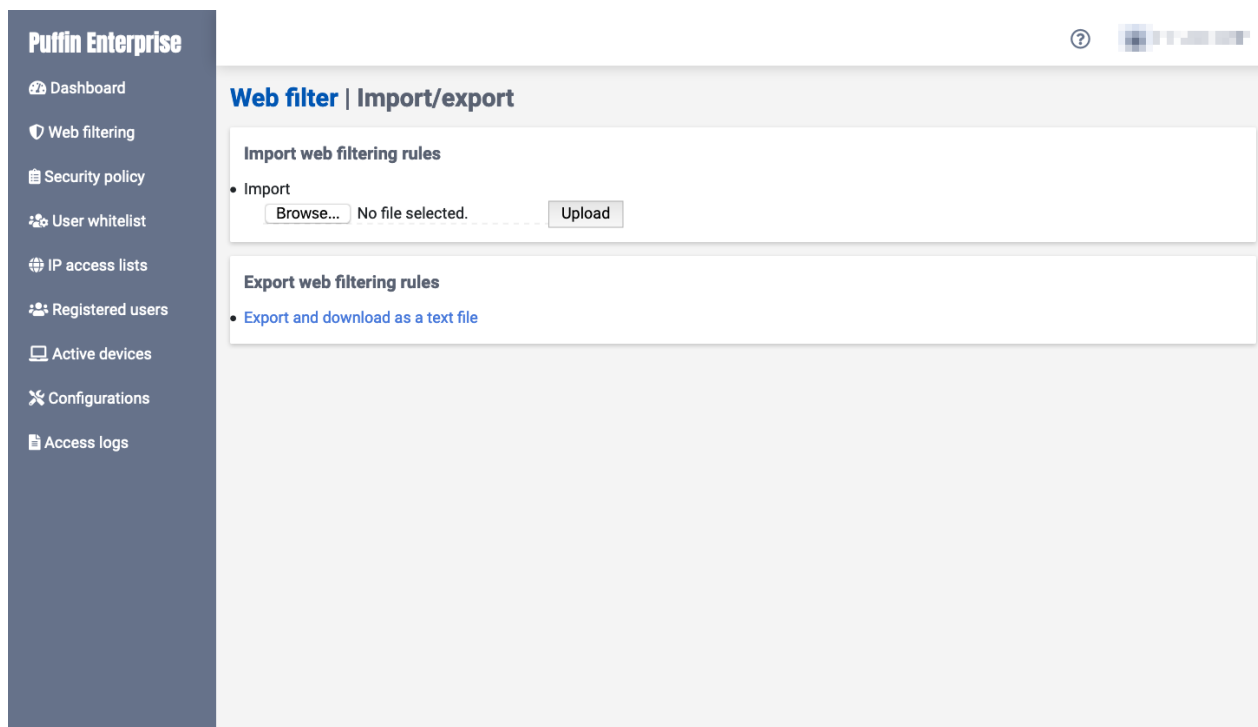
## Bulk Operations

In addition to adding web filtering rules one by one, Puffin Enterprise Cloud Portal provides bulk import and export features.

**Note:** The file uploader supports text files in the format of one rule per line. A rule consists of an action ( **ALLOW** or **BLOCK** ), a space, and the included websites. For example:

- **ALLOW \***
- **BLOCK www.example.com**
- **BLOCK \*.example.com**

How to import a text file:



1. Scroll to **Filtering rules**.
2. Click **Import/export**.
3. Under the **Import** section, click **Browse** and choose the target text file (.txt) to upload.
4. Click **Upload**.
5. Click **OK** when the confirmation dialog appears.
6. The rules are imported and will overwrite your existing data.

Once you've configured the web filtering rules, you can download a text file (.txt) of the rules to your hard drive. You can show this file to others to let them know the currently active web filtering rules without giving them access to Enterprise Cloud Portal.

Also, you may download the file, perform some editing, and import the file to Enterprise Cloud Portal again to implement new rules.

How to export your web filtering rules:

1. Scroll to **Composed filtering rules**.
2. Click **Import/export**.
3. Scroll to **Export web filtering rules**.

- Click **Export and download as a text file** and save the file to your local hard drive.

## Security Policy

Configure security policy settings for specific domains or hostnames when users visit them in Puffin Secure Browser.

### What security policies can I configure for my organization?

#### Add a new policy rule

**Action(s) to disable:**

☒ Certificate verification  
☒ Clipboard  
☒ File download  
☒ File upload

Add

Sample target	Type	Case sensitive	Web pages can be matched	Details
*.example.com	Domain	N	Pages of all hosts under the domain	
www.example.com	Hostname	N	Pages of a single host	

The available rules you can set up depend on the global settings in **Configurations**. Only when a component is turned on in **Configurations** can you configure its corresponding security policies. When the following components are turned on in Configurations, they will appear as available options in security policies.

- Certificate verification (Enterprise feature)
- Clipboard (Enterprise feature)
- File download
- File upload

### How do I add a security policy?

1. Scroll to **Add a new policy rule**.
2. Enter a domain or hostname where you want to specify a security policy.
3. Check the options to include in this policy.
4. Click **Add**.
5. After adding a rule, you can still modify the affected features in the **Policy rules** section below.

### Bulk operations

In addition to adding security policy rules one by one, Puffin Enterprise Cloud Portal provides bulk import and export features.

**Note:** The file uploader supports text files in the format of one rule per line. Simply enter the domain name or hostname, followed by a space and the options you want to disable. For example:

```
*.example.com disable_cert_verification disable_clipboard disable_upload  
disable_download
```

#### How to import a text file:

1. Scroll to **Policy rules**.
2. Click **Import/export**.
3. Under the **Import security policy rules** section, click **Browse** and choose the target text file (.txt) to upload.
4. Click **Upload**.
5. Click **OK** when the confirmation dialog appears.
6. The user emails are imported and will overwrite your existing data.

Once you have configured all security policy rules, you can download a text file (.txt) of the list to your hard drive. You can perform some editing, and import the file to Enterprise Cloud Portal again to add new rules.

#### How to export your security policy rules:

1. Scroll to **Policy rules**.
2. Click **Import/export**.
3. Scroll to **Export security policy rules**.
4. Click **Export and download as a text file** and save the file to your local hard drive.

## User whitelist

Set the access permission for Puffin Secure Browser users based on user email addresses.

After subscribing to a Team or Enterprise plan, all users whose mail domain matches the one in your registration can activate their Puffin Secure Browser clients. This default setting is indicated as follows.

#### Mail/domain allowed to register

[↗ Import/export](#)

#	Mail / Domain	Scope	
1	@example.com <default>	All mails of the domain	

You can limit Puffin Secure Browser activation and usage to specific users in your organization by adding their email addresses to the user whitelist.

#### How to whitelist specific users:

1. Scroll to **Mail/domain allowed to register**.
2. Click the Trash icon next to the default domain.
3. Add user email addresses to the list one by one.

#### Note:

1. Only users from the domain associated with your account can be added to the whitelist. Adding users from other organizations is not supported at the moment.
2. You can add as many users as you like to the whitelist. However, only the number of users that does not exceed your license quota can register to use Puffin.

## Bulk operations



In addition to adding user emails one by one, Puffin Enterprise Cloud Portal provides bulk import and export features.

**Note:** The file uploader supports text files in the format of one mail address per line. Simply enter mail addresses and save them as a text (.txt) file.

#### How to import a text file:

1. Scroll to **Mail/domain allowed to register**.
2. Click **Import/export**.
3. Under the **Import mail domain/box** section, click **Browse** and choose the target text file (.txt) to upload.
4. Click **Upload**.
5. Click **OK** when the confirmation dialog appears.
6. The user emails are imported and will overwrite your existing data.

Once you've configured the user whitelist, you can download a text file (.txt) of the list to your hard drive. You can perform some editing, and import the file to Enterprise Cloud Portal again to add new users.

#### How to export your user whitelist:

1. Scroll to **Mail/domain allowed to register**.
2. Click **Import/export**.
3. Scroll to **Export mail domain/box**.
4. Click **Export and download as a text file** and save the file to your local hard drive.

## IP access lists

---

- This feature is only available to subscribers of the Enterprise plan.

IP access lists log the IPs of local users, remote users, and remote hosts in an authentication database that is configured to control access to Puffin Secure Browser. Unwanted traffic or users are blocked, making your networking environment isolated and safe from attackers.

To enable IP access lists for your organization, tick the checkbox **Only allow users from whitelisted IPs**.

#### How to add IPs to IP access lists:

1. Scroll to **Add a new whitelisted IP address**.
2. Enter an IP address or IP block (IP range) you wish to add.
3. Click **Add**.
4. The IP address is added. It will take effect after users relaunch their Puffin Secure Browser.

**Note:** IP access lists support the CIDR (Classless Inter-Domain Routing) notation, in which the IP address is suffixed with a slash and a number, used to specify the length of the associated routing prefix, e.g.

5.6.7.0/24 .

## Bulk operations

In addition to adding IP addresses one by one, Puffin Enterprise Cloud Portal provides bulk import and export features.

**Note:** The file uploader supports text files in the format of one IP address per line. Simply enter mail addresses and save them as a text (.txt) file.

#### How to import a text file:

1. Scroll to **Allowed IP addresses**.
2. Click **Import/export**.
3. Under the **Import user IP** section, click **Browse** and choose the target text file (.txt) to upload.
4. Click **Upload**.
5. Click **OK** when the confirmation dialog appears.
6. The IP addresses are imported and will overwrite your existing data.

Once you've configured the IP access lists, you can download a text file (.txt) of the lists to your hard drive. You can perform some editing, and import the file to Enterprise Cloud Portal again to add new IP addresses.

#### How to export your IP access lists:

1. Scroll to **Allowed IP addresses**.
2. Click **Import/export**.
3. Scroll to **Export user IP**.
4. Click **Export and download as a text file** and save the file to your local hard drive.

## Registered users

---

**Registered users** allow you to see who in your organization has activated Puffin, and how many devices have been associated with their email addresses. All users who have successfully activated Puffin will be listed in this page.

### How to see details of my organization's monthly active users?

1. Click **Monthly active users** on the upper right corner.
2. Select the month you would like from the dropdown menu.
3. You can click on the user emails one by one to see the detailed login history.

Note: User login history is kept for 60 days on Enterprise Cloud Portal.

## Active devices

---

In addition to monitoring your license usage from the Dashboard, information on active devices in your organization can be retrieved from **Active devices**.

**Active devices** display the devices, their last active users in your organization, and the last active dates.

### How to see details of my organization's monthly active devices?

Follow the steps below to quickly look up monthly active devices.

1. Select the month you would like from the dropdown menu at the top.
2. You can click on the device IDs one by one to see the detailed login history.

Note: Device login history is kept for 60 days on Enterprise Cloud Portal.

## Configurations

---

After installation, IT administrators should review all configurations in this section to enforce the appropriate security measures for the organization. Configurations affect all Puffin Secure Browser instances and all websites users visit. The following components can be turned on and off.

- Certificate verification
- Clipboard
- File upload
- File download
- Document preview

### Certificate verification

- This component is only available to subscribers of the Enterprise plan.

☒ **Enforce certificate verification**

For HTTPS web pages, allow only web pages that pass SSL certificate verification

Websites using the HTTPS connection need a security certificate, which secures and encrypts data going back and forth between the server and the web browser. Visiting websites whose security certificate is broken, expired, or missing may pose security risks to your corporate network.

By default, the option **Enforce certificate verification** is **ON**.

To allow users to access websites with bad certificates, uncheck **Enforce certificate verification**.

Alternatively, you can keep **Enforce certificate verification** on and whitelist certain websites that have not passed certificate verification in **Security policy**. For details, refer to the section on **Security policy** in this document.


### Clipboard

- This component is only available to subscribers of the Enterprise plan.

☒ **Enable clipboard**

Enable clipboard operations between the local device and remote websites

Allowed action(s)

- CUT/COPY & PASTE - 

It is common practice to use copying and pasting functions in a browser. For convenience of usage, the option **Enable clipboard** is **ON** by default.

However, you may want to restrict clipboard access in Puffin Secure Browser for the following reasons.

- To prevent users from leaking sensitive data in your organization.
- To prevent users from copying malicious content to local devices.

To give you more control on how much you would like to allow clipboard access in Puffin Secure Browser, we provide three options.

- **CUT/COPY and PASTE:** This option allows users to use all clipboard functions.
- **CUT/COPY only:** Users can only copy content from Puffin Secure Browser, but they cannot paste content from their device clipboard to the web.
- **PASTE only:** Users can paste content from the device clipboard to the web, but they cannot copy content from the web to their device clipboard.

Alternatively, you can keep **Enable clipboard** on, use the default option **CUT/COPY and PASTE**, while restricting specific website's clipboard access. For details, refer to the section on **Security policy** in this document.

## File upload

### ☒ **Enable file upload**

Allow uploading local files to remote websites

By default, the option **Enable file upload** is **ON**.

You can restrict Puffin Secure Browser users from uploading files to the web. This feature helps prevent users from uploading malicious attachments to their emails or any web forms.

To disable all file uploads in Puffin Secure Browser, simply uncheck **Enable file upload**.

Alternatively, you can keep **Enable file upload** on, while restricting specific website's file uploads. For details, refer to the section on **Security policy** in this document.

## File download

### ☒ **Enable file download**

Allow downloading remote files to local storage

Download destinations

- ☒ Google Drive
- ☒ Dropbox
- ☒ Microsoft OneDrive
- ☒ Local computer/device

Maximum file size

- Should not exceed 2048MB

2048 MB

By default, the option **Enable file download** is **ON**.

Puffin Secure Browser supports downloading files directly to cloud storage services and local storage. For our Enterprise subscribers, virus scans are automatically performed before files are downloaded to the destination of your choice.

The download destinations you can allow in Puffin Secure Browsers are as follows.

- Google Drive
- Dropbox

- Microsoft OneDrive
- Local device/computer

#### How to prevent users from directly downloading files to any destination:

1. Scroll to **Enable file download**.
2. In the **Download destinations** section, uncheck any destinations you wish to disable.
3. Click **Save**.

The allowed downloaded file size in Puffin Secure Browser is up to **2GB (2048MB)**. To change the allowed maximum file size, follow the steps below.

1. Scroll to **Enable file download**.
2. In the **Maximum file size** section, enter a new number in MB (Megabytes) as the allowed file size.
3. Click **Save**.

To disable all file downloads in Puffin Secure Browser, simply uncheck **Enable file download**.

Alternatively, you can keep **Enable file download** on, while restricting specific website's file downloads. For details, refer to the section on **Security policy** in this document.

## Document Preview

- This component is only available to subscribers of the Enterprise plan.

#### ☒ **Enable document preview**

Allow users to preview document content before downloading the file.

( **Supported document types**)

Puffin Secure Browser provides the ability to preview Microsoft Office documents without having to download them to your device. For convenience of usage, the option **Enable document preview** is **ON** by default.

The supported document types are as follows.

- Word documents (\*.doc, \*.docx)
- PowerPoint presentations (\*.ppt, \*.pptx)
- Excel files (\*.xls, \*.xlsx)
- PDF files (\*.pdf)

Note: Users can always preview PDF files regardless of the **Document Preview** setting.

To disable the document preview feature in Puffin Secure Browser, simply uncheck **Enable document preview**.

## Access logs

---

Use Puffin Enterprise Cloud Portal's reports to gain a better understanding of how users are using Puffin Secure Browser.

### When are logs generated?

The reports we currently offer are web access logs, which are generated 24 hours after new websites are visited.

### What information is included in web access logs?

The information included in web access logs is listed as follows:

- The time when a website is accessed (format: `YY/MM/DD hh:mm:ss` )
- The IP address of the user.
- The user's platform.
- The user's email address.
- The pseudonym of the user's device.
- The website URL.

### How do I download the logs?

1. Scroll to **Logs available for download (CSV format)**.
2. If logs are available, links named after dates would be displayed.
3. Click any dated links to download the log for the day.

Downloadable logs are offered in the **CSV format**. This lets you create more advanced reports and charts using other data analytics tools.