

Content Security Policy [.2307 - .2211]

Last Modified on 03/10/2023 10:27 am CST

You are viewing a previous version of this article. See Content Security Policy for the most current information.

Tool Rights | Select the Content Security Policy (CSP) | Enforce, Report, or Disable the Content Security Policy (CSP) | Understand Violation Reports

Classic View: System Administration > User Security > Content Security Policy

Search Term: Content Security Policy

The Content Security Policy is an additional security directive which is added to the HTTP headers of all Campus pages. This tool allows administrators to control resources the user agent is allowed to load for a given page. Content Security Policies mostly involve specifying server origins and script endpoints, bolstering system security, especially against cross-site scripting attacks (XSS).

Unlike most Content Security Policies, this tool allows for flexibility to account for both the variety of pages used throughout Campus and custom development utilized by our customers. As a result, this tool provides a Basic Policy (all resources loaded from Campus) and a Custom Policy where users are able to build on top of the Basic policy to meet their individual needs.

For detailed information about the purpose and importance of CSPs, guidance on creating your own CSP, and understanding violation report syntax, see the Mozilla Content Security Policy guide.

This tool should only be used by a system administrator who manages and/or understands your district's Content Security Policy (CSP).

Content Securi	y Policy
nabling this tool all lements, prevents e Disable Report Only	ws you to increase user security by adding a Content Security Policy to all Infinite Campus-generated URLs. This policy restricts the source URLs for all page aments from unknown sources from being loaded, blocks cross-site scripts from accessing user data, and overall makes Infinite Campus more secure. Enforce CSP
'olicies and Vi Security Policies	lation Reports
Selected Policy Basic	▼
Summary	
The default Infin created product	te Campus Content Security Policy. This serves as the baseline for a custom Infinite Campus CSP, it includes all directives necessary for all Infinite Campus 1, and cannot be edited.

Image 1: Content Security Policy Tool

Tool Rights

Only users assigned a Product Security Role of **Student Information System (SIS)** are allowed to use this tool.

User Account	User Groups	Tool Rights	Calendar Rights
🕒 Save 😣	Delete 👂	Login As User 🛛 💡	User Rights Summa
User Account Ed Username Coretester Expires Date Force Passw Disabled SAML Account Con Allow Only Local C Product Security Data Change Staff Evaluati Student Infor Student Infor	itor itor ord Change figuration ampus Authenticatio Role Assignments Tracker ons mation System mation System - Gro mation System - Log	Password Reset Password Homepage Campus Application	

Image 2: Student Information System (SIS) Product Security Role

Select the Content Security Policy



(CSP)

The first step in setting your Content Security Policy is determining which policy works best for your district. See the sections below for more information about each policy:

- Basic
- Custom

Content Security Policy
Enabling this tool allows you to increase user security by adding a Content Security Policy to all Infinite Campus-generated URLs. This policy restricts the source URLs for all page elements, prevents elements from unknown sources from being loaded, blocks cross-site scripts from accessing user data, and overall makes Infinite Campus more secure. Disable Report Only Enforce CSP
Policies and Violation Reports
Security Policies Violation Reports
Selected Policy Basic Basic Custom
The default Infinite Campus Content Security Policy. This serves as the baseline for a custom Infinite Campus CSP, it includes all directives necessary for all Infinite Campus created products, and cannot be edited. View Details
Save

Image 3: Selecting a Policy

Basic Policy

The **Basic** policy is the default policy which includes all directives necessary for all Infinite Campuscreated products. For most users, especially those without custom or 3rd-party tooling which makes calls outside of the Campus product, the Basic policy will work well and should be selected.

To view a breakdown of what is included within the Basic CSP, click the **View Details** button (Image 4).

To set the policy:

- 1. Select 'Basic' in the Selected Policy dropdown list.
- Click Save. The policy is selected and saved however, it is set to Disabled by default. To begin using CSP functionality, Infinite Campus suggest setting it to Report Only and using the Violations Reports to audit any CSP violations prior to enforcing the policy.

plicies and Violation Repo	ts			
Security Policies Violation Repo	ts			
Selected Policy				
Basic •				
Summary				
The default Infinite Campus Con created products, and cannot be View Details	Int Security Policy. This serves as the baseline for a custom Infinite Campus CSP, it includes all directives necessary for all Infinite Campus dited.			
	mpus Content Security Policy Detail You can only enable/disable the basic CSP. If another policy is enabled, this will be disabled automatically.			
Save				
	content Security Policy			
	ame: Status:			
	Basic Enabled			
	escription			
	The default infinite Campus Content Security Policy. This serves as the baseline for a custom infinite Campus CSP, It includes all directives necessary for all infinite Campus created products, and cannot be edited.			
	efault CSP:			
	The Content Security Policy that will be applied to campus pages by default. Any page that does not have a '/apps' or '/portal' url will use this security policy.			
	default-ere-'self 'uneafauline''uneafauval' data: http://net.adobe.com.https://k.infinitacampus.com			
	fort-src: 'self data: https://*.bootstrapcdn.com			
	frame-src: 'self' https://*.youtube.com data: http://get.adobe.com https://www.google.com			
	img-src: 'self data: blob. https://vanguard.com https://vinfiniteampus.com https://swagger.io https://encrypted-tbn3.gstatic.com https://v.posting.cc			
	script-src. seir unsare-imme unsare-eval www.gstatic.com/https://www.google.com/ style-src; seif' unsafe-inline' unsafe-eval www.gstatic.com https://*.bootstrap.cdn.com http://*.cloudflare.com			
	iplication CSP:			
	The Content Security Policy that will be applied to pages with the '/apps' url.			
	ortal CSP:			
	The Content Security Policy that will be applied to pages with the '/portal' url.			

Image 4: Selecting and Viewing the Basic Policy

Custom Policy

Infinite 🗠 .

The **Custom** policy is everything contained within the Basic policy (all directives necessary for all Infinite Campus-created products) with the ability to build on top of it with your own AllowListed applications.

To view and modify the policy, select 'Custom' in the **Selected Policy** dropdown list and click **View Details**. An editor will appear, detailing everything contained within the policy. To edit and add to the policy, click the **Edit** button (Image 5).

Infinite Campus		
Policies and Violation Repo	orts orts idd additional security directives to the default Infinite Campus CSP	
Save Campus Conter Name: Custor	: Content Security Policy Detail :nt Security Policy	Status: Disabled
Description		
A cust	tom policy allows you to add additional security directives to the default Infinite Campu	JS CSP.
Default C	25P:	
The Co	ontent Security Policy that will be applied to campus pages by default. Any page that d	loes not have a '/apps' or '/portal' url will use this security policy.
defaul font-su frame- img-su script- style-s	It-src: 'self 'unsafe-inline' 'unsafe-eval' data: http://get.adobe.com https://*.infinitecam .rc: 'self' data: https://*.bootstrapcdn.com -src: 'self' https://*.youtube.com data: http://get.adobe.com https://www.google.com .rc: 'self' data: blob: https://*.vanguard.com https://*.infinitecampus.com https://*.swag .src: 'self' 'unsafe-inline' 'unsafe-eval' www.gstatic.com https://*.bootstrapcdn.com http .src: 'self' 'unsafe-inline' 'unsafe-eval' www.gstatic.com https://*.bootstrapcdn.com http://*.bootstrapcdn.com http://*.bootstrapcdn	pus.com gger.io https://encrypted-tbn3.gstatic.com https://*.postimg.cc r://*.cloudflare.com
Applicatio	ion CSP:	
The Co	ontent Security Policy that will be applied to pages with the '/apps' url.	+
Portal CS	SP:	
The Co	ontent Security Policy that will be applied to pages with the '/portal' url.	+
Edit	Close Enable	

Image 5: Viewing and Editing the Custom Policy

The first screen allows you to edit the **CSP Name** and **Description** of the policy. Once complete, select **Next** (Image 6).

nfinite Campus			
	2	3	(4)
Content Security Policy Details	Default CSP	Application CSP	Portai CSP
CSP Name: *			
Custom			
Description:			
			A
		Cancel Next	

Image 6: Modifying the Custom CSP Name and Description

This second editor contains the default CSP used for Campus pages. Add any additional pages as needed. Once complete, select **Next** (Image 7).



Details Default CSF	3 Application CSP Portal CSP
Default Content Security Policy	
This is the Content Security Policy that will be applied to campus pages by	fault. Any page that does not have a '/apps' or '/portal' url will use this security policy.
default-src	
Campus default-src:	Additions to default-sro:
'self' 'unsafe-inline' 'unsafe-eval' data: http://get.adobe.com https://*.infir	ampus.co
font-src	
Campus font-src:	Additions to font-src:
'self' data: https://*.bootstrapcdn.com	
img-src	
Campus img-src:	Additions to img-src:
'self' data: blob: https://*.vanguard.com https://*.infinitecampus.com htt	/*.swagge https://*.gstatic.com
scrint-src	
Campus script-src:	Additions to script-src:
'self' 'unsafe-inline' 'unsafe-eval' www.gstatic.com https://www.google.co	
style-src	
Campus style-src:	Additions to style-src:
'self' 'unsafe-inline' 'unsafe-eval' www.gstatic.com https://*.bootstrapcdn	m http://*.
frame-src	
Campus frame-src:	Additions to frame-src:
'self' https://*.youtube.com data: http://get.adobe.com https://www.goog	com https://www.google.com
Custom Directives Any desired directives not defined in the campus default CSP can be defined here.	pus does not validate for correct CSP syntax, so make sure you enter your custom directives carefully.
	Previous Cancel Next

Image 7: Adding to the Default CSP

The third editor contains all Campus apps contained within the CSP. Add any additional applications as needed. Once complete, select **Next** (Image 8).



Details Default CSP	Application CSP Portal CSP
Application Content Security Policy	
The Content Security Policy that will be applied to pages with the '/apps' url.	
default-src	
Campus default-src:	Additions to default-src:
'self' https://*.infinitecampus.com https://apis.google.com https://accounts.goog	le.co
script-src	
Campus script-src:	Additions to script-src:
'self' 'unsafe-eval' 'unsafe-inline' https://apis.google.com https://accounts.google.	com
style-src	
Campus style-src:	Additions to style-src:
'self' 'unsafe-inline'	
font-src	
Campus font-src:	Additions to font-src:
'self' data:	
object-src	
Campus object-src:	Additions to object-src:
'none'	
ima-src	
Campus img-src:	Additions to img-src:
'self' blob: data: https://*.infinitecampus.com https://www.biography.com https://	csi.g:
frame-src	
Campus frame-src:	Additions to frame-src:
'self' https://*.infinitecampus.com https://apis.google.com https://accounts.goog	le.co
Custom Directives Any desired directives not defined in the campus default CSP can be defined here. Campus do	ies not validate for correct CSP syntax, so make sure you enter your custom directives carefully.
	Previous Cancel Next

Image 8: Adding to the Application CSP

The fourth editor is all Campus Portal pages included in the CSP. Add any additional pages as needed. Once complete, select **Finish** and then select **Save** near the bottom of the Content Security Policy tool. The policy is now saved and set to Disabled by default. To begin using CSP functionality, Infinite Campus suggest setting it to Report Only and using the Violations Reports to audit any CSP violations prior to enforcing the policy.



Details	Default CSP	Application CSP	Portal CSP
Portal Content Security Policy			
The Content Security Policy that will be applied to pages v	with the '/portal' url.		
default-src			
Campus default-src:		Additions to default-src:	
'self' https://hexea-js-dev-prelive.azurewebsites.net https://	s://hexea-processor-dev-prelive	1	
script-src			
Campus script-src:		Additions to script-src:	
'self' 'unsafe-eval' 'unsafe-inline' https://apis.google.com	https://accounts.google.com		
style-src			
Campus style-src:		Additions to style-src:	
'self' 'unsafe-inline'			
font-src			
Campus font-src:		Additions to font-src:	
'self' data:			
img-src			
Campus img-src:		Additions to img-src:	
'self' https://campus.cusd80.com			
object-src			
Campus object-src:		Additions to object-src:	
'none'			
frame-src			
Campus frame-src:		Additions to frame-src:	
'self' www.vancodev.com https://content.googleapis.com	m		
Custom Directives Any desired directives not defined in the campus default CSP ca	n be defined here. Campus does not	validate for correct CSP syntax, so make sure you enter your	custom directives carefully.
			Previous Cancel Finish

Image 9: Adding to the Portal CSP and Finishing the Custom CSP Process

Enforce, Report, or Disable the Content Security Policy (CSP)

Once you have selected and saved a policy, you need to set whether to have it report violations or be enforced.

By default, **Disabled** is selected. It is best practice to first set the value to Report Only and audit CSP violations prior to enforcing the CSP.

• Disable - Disables the CSP. When selected, no CSP is enforced or reported. This is the default



value selected.

- **Report Only** Enables the CSP but only reports violations and does not enforce the CSP. This option is useful for auditing the Basic or Custom policy to see which violations are occurring. This is especially useful for districts who want to enforce a Custom policy as they can audit and adjust the policy to make sure their custom tools and calls will not break and produce violations once the policy is enforced. Report violations can be reviewed via e Violation Reports tab.
- **Enforce CSP** This option enforces the selected policy (Basic or Custom). All policy violations will be blocked and reported.

Content Security Policy
Enabling this tool allows you to increase user security by adding a Content Security Policy to all Infinite Campus-generated URLs. This policy restricts the source URLs for all page elements, prevents elements from unknown sources from being loaded, blocks cross-site scripts from accessing user data, and overall makes Infinite Campus more secure.

Image 10: Enforcing, Reporting, or Disabling the CSP

Understand Violation Reports

Once a policy has been selected and saved, any violations of the CSP will be reported and detailed in the **Violation Reports** tab (Image 11). For detailed information about a violation, select it from the list.

Review and audit violations to ensure the policy is not blocking or breaking any intended functionality and if using a Custom policy, adjust the policy to account for these violations.

Once you have thoroughly reviewed violations, made any adjustments to the policy as needed, and feel the CSP is ready to be enforced. select Enforce CSP. The CSP is now actively enforcing the policy and any violations are blocked in real time.



Content Security Policy	ated URLs. This policy restricts the source URLs for all page
elements, prevents elements from unknown sources from being loaded, blocks cross-site scripts from accessing user of Disable Report Only Enforce CSP Once you are ready to enable and enforce select Enforce CSP.	data, and overall makes Infinite Campus more secure.
Policies and Violation Reports	
Security Policies Violation Reports	
BLOCKED URI	VIOLATED #
https://www.google.com/uds/api/visualization/1.0/36558b280aac4fa99ed82	style-src 1 >
https://ajax.googleapis.com/ajax/static/modules/gviz/1.0/core/tooltip	style-src 1 >
View All Active Reports	
Violated CSP:	
Basic	
Violations:	
Number of Violations: 1 Last Violation: Apr	ril 2, 2020 7:41 AM
Blocked URI:	
https://www.google.com/uds/api/visualization/1.0/36558b280aac4fa99ed8215e60015cff/ui+en.css	
Violated Directive:	
style-src	
Document Location:	
https://iesite2.infinitecampus.com/campus/olr2/coreOLR/dashboard/olr2dashboard.icml?&nodeID=4475	
https://iesite2.infinitecampus.com/campus/olr2/coreOLR/dashboard/olr2dashboard.icml?&nodeID=4475	
https://iesite2.infinitecampus.com/campus/olr2/coreOLR/dashboard/olr2dashboard.icml?&nodeID=4475	

Image 11: Reviewing CSP Violations