Content Security Policy

Last Modified on 10/22/2022 10:09 am CDT

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*

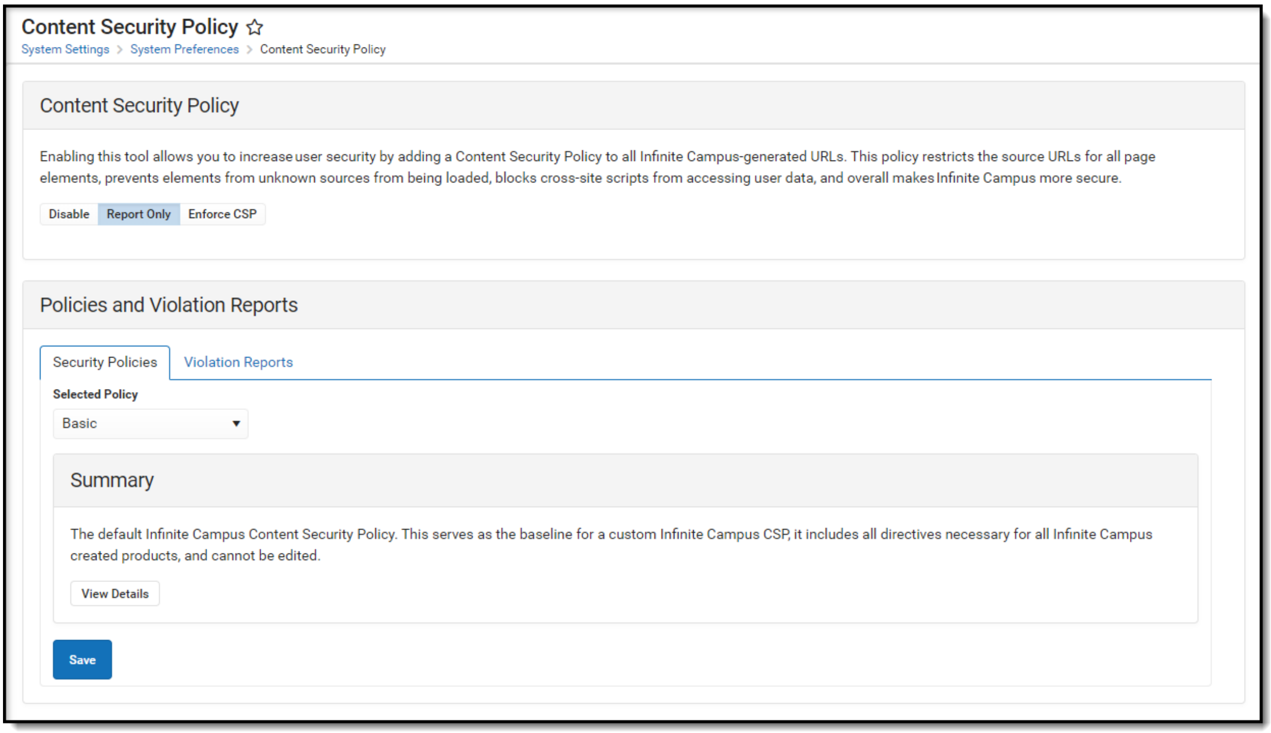
Search Term: *Content Security Policy*

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 Security Policy ☆

System Settings > System Preferences > Content Security Policy

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

Summary

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.

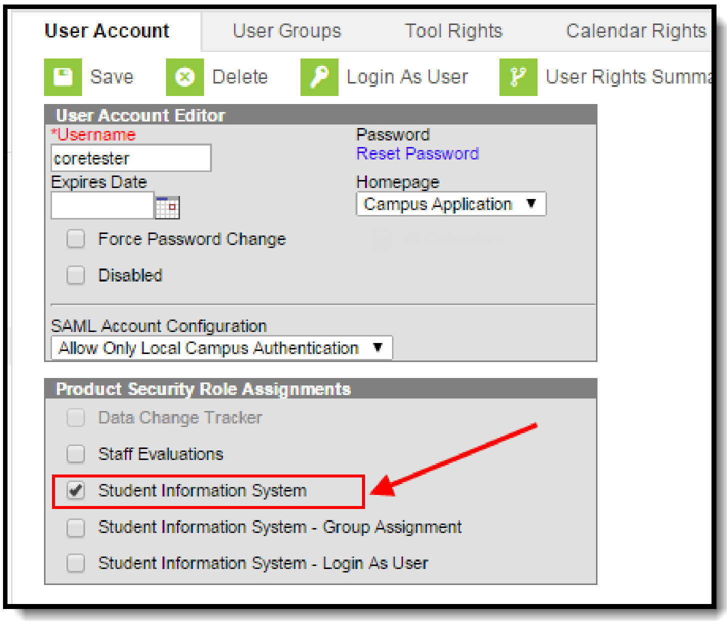
View Details

Save

Image 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 Editor

*Username: coretester

Password: Reset Password

Expires Date:

Homepage: Campus Application

□ Force Password Change

□ Disabled

SAML Account Configuration: Allow Only Local Campus Authentication

Product Security Role Assignments

□ Data Change Tracker

□ Staff Evaluations

☑ Student Information System

□ Student Information System - Group Assignment

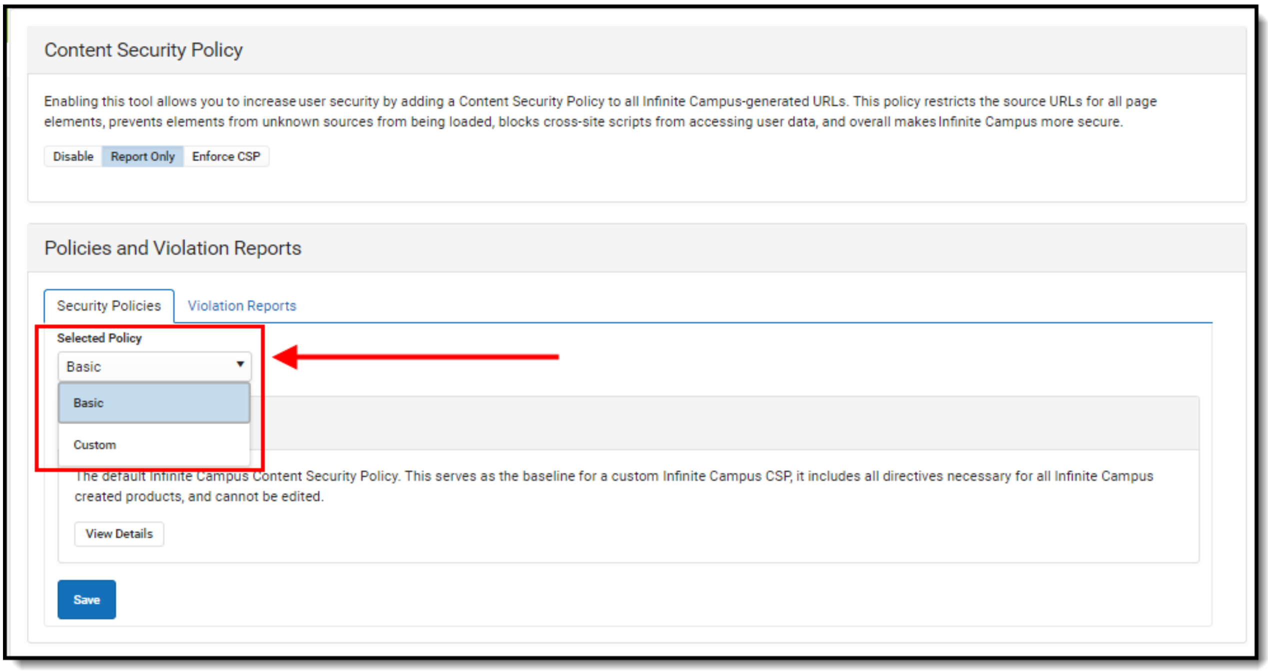
□ Student Information System - Login As User

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.

Policies and Violation Reports

Selected Policy: Basic

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.

Image 3: Selecting a Policy

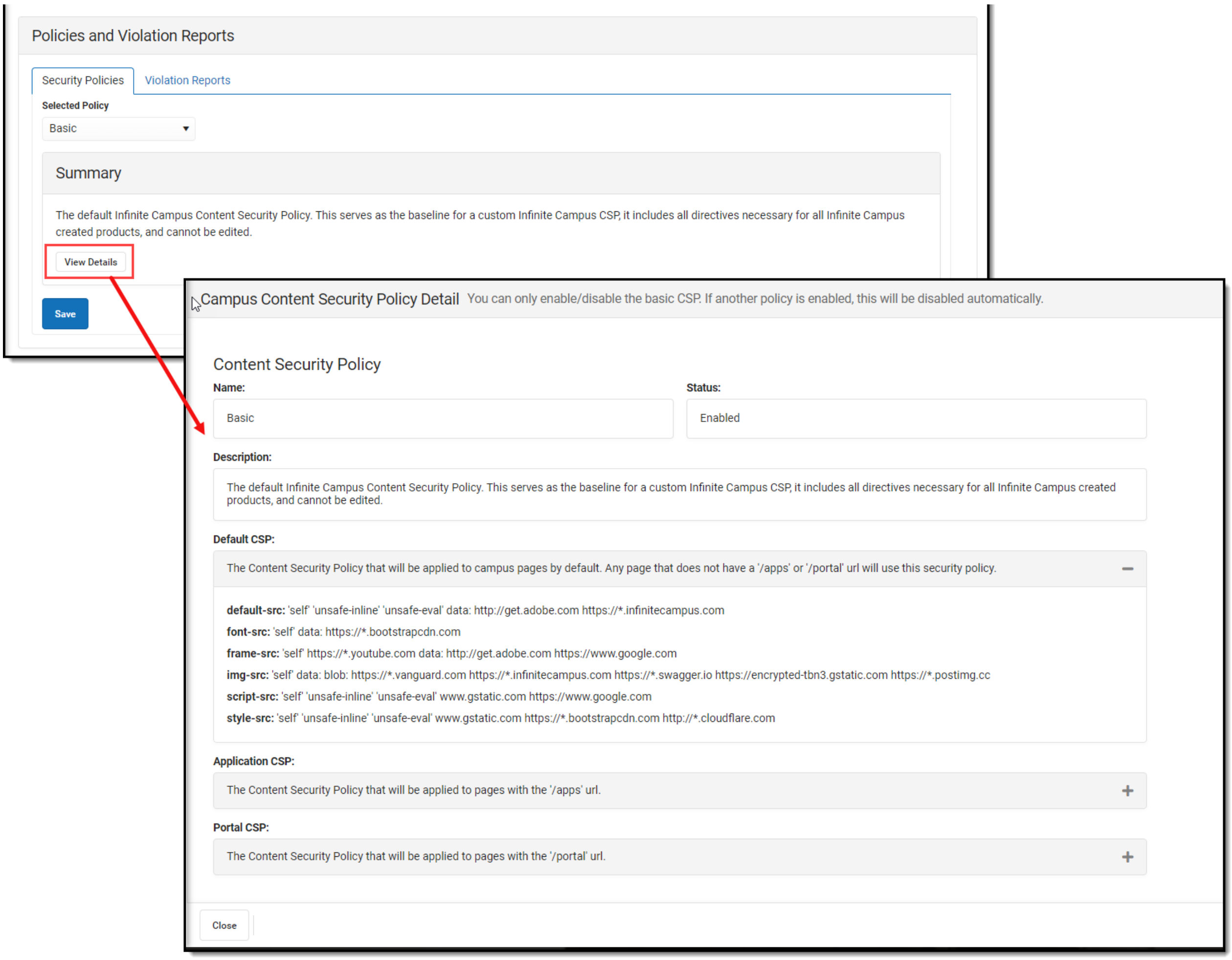
Basic Policy

The **Basic** policy is the default policy which includes all directives necessary for all Infinite Campus-created 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.
2. 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.



Policies and Violation Reports

Selected Policy: Basic

Summary

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.

Campus Content Security Policy Detail You can only enable/disable the basic CSP. If another policy is enabled, this will be disabled automatically.

Content Security Policy

Name: Basic

Status: Enabled

Description: 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.

Default 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-src: 'self' 'unsafe-inline' 'unsafe-eval' data: http://get.adobe.com https://*.infinitecampus.com

font-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://*.infinitecampus.com https://*.swagger.io https://encrypted-tbn3.gstatic.com https://*.postimg.cc

script-src: 'self' 'unsafe-inline' 'unsafe-eval' www.gstatic.com https://www.google.com

style-src: 'self' 'unsafe-inline' 'unsafe-eval' www.gstatic.com https://*.bootstrapcdn.com http://*.cloudflare.com

Application CSP:

The Content Security Policy that will be applied to pages with the '/apps' url.

Portal CSP:

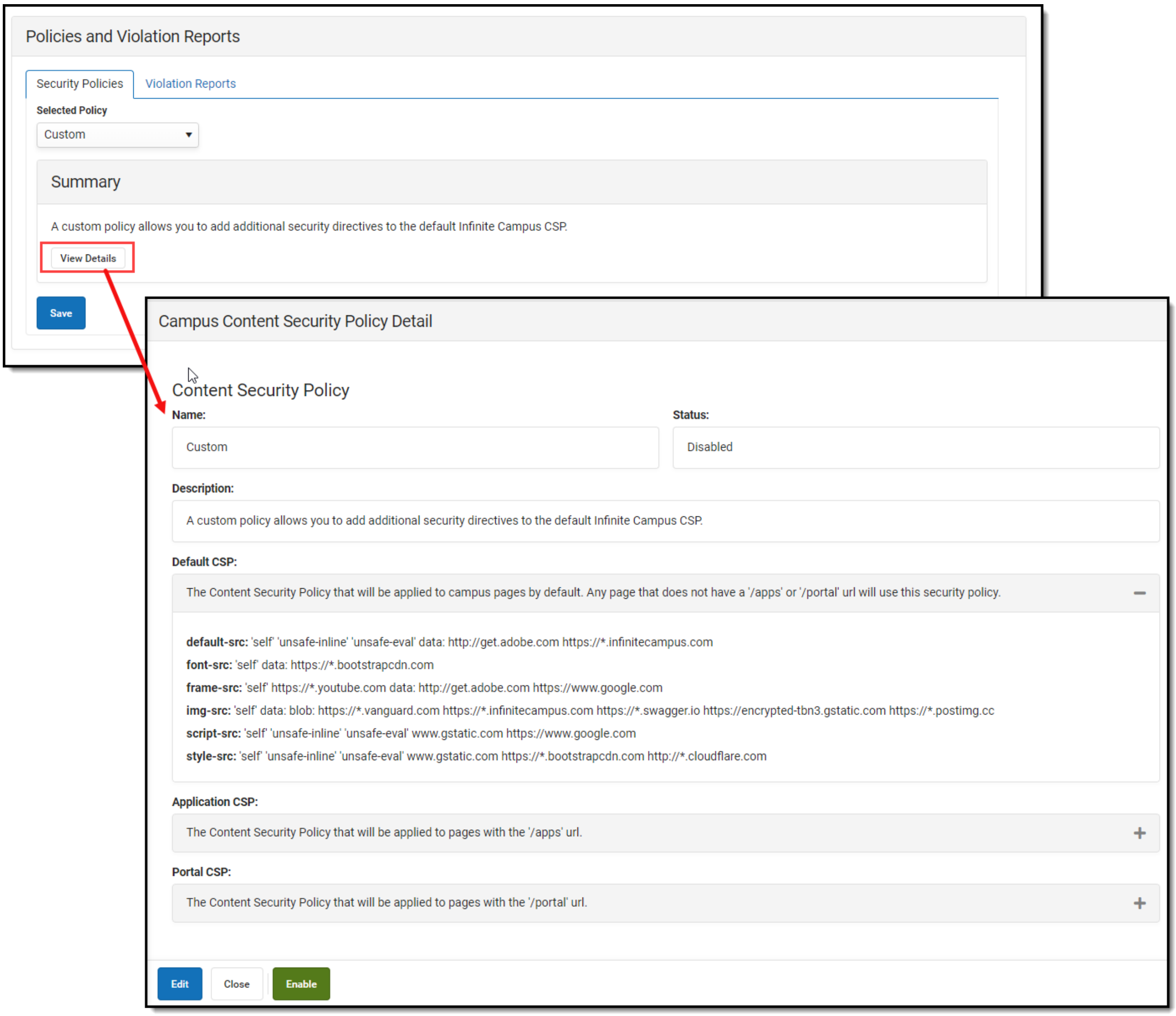
The Content Security Policy that will be applied to pages with the '/portal' url.

Image 4: Selecting and Viewing the Basic Policy

Custom Policy

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).



Policies and Violation Reports

Selected Policy: Custom

Summary

A custom policy allows you to add additional security directives to the default Infinite Campus CSP.

Campus Content Security Policy Detail

Content Security Policy

Name: Custom

Status: Disabled

Description: A custom policy allows you to add additional security directives to the default Infinite Campus CSP.

Default 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-src: 'self' 'unsafe-inline' 'unsafe-eval' data: http://get.adobe.com https://*.infinitecampus.com
font-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://*.infinitecampus.com https://*.swagger.io https://encrypted-tbn3.gstatic.com https://*.postimg.cc
script-src: 'self' 'unsafe-inline' 'unsafe-eval' www.gstatic.com https://www.google.com
style-src: 'self' 'unsafe-inline' 'unsafe-eval' www.gstatic.com https://*.bootstrapcdn.com http://*.cloudflare.com

Application CSP:

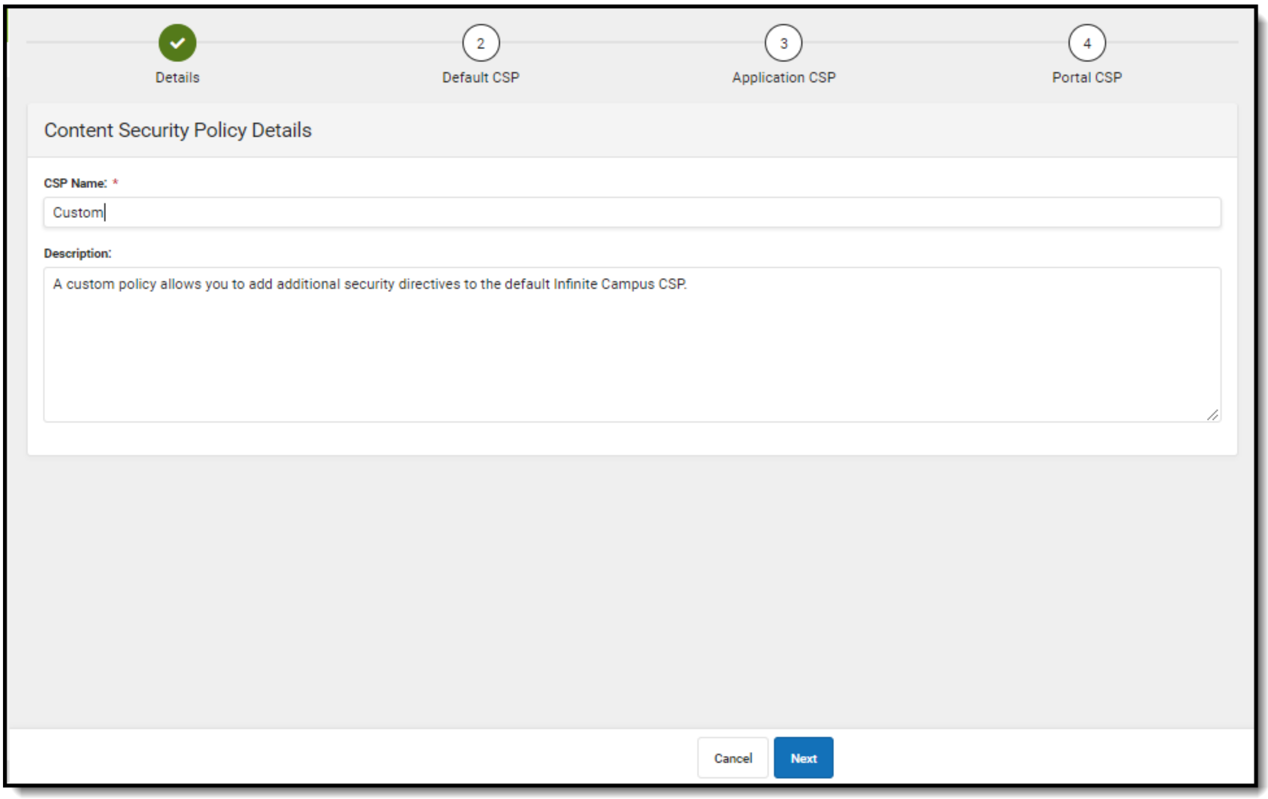
The Content Security Policy that will be applied to pages with the '/apps' url.

Portal CSP:

The Content Security Policy that will be applied to pages with the '/portal' url.

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).



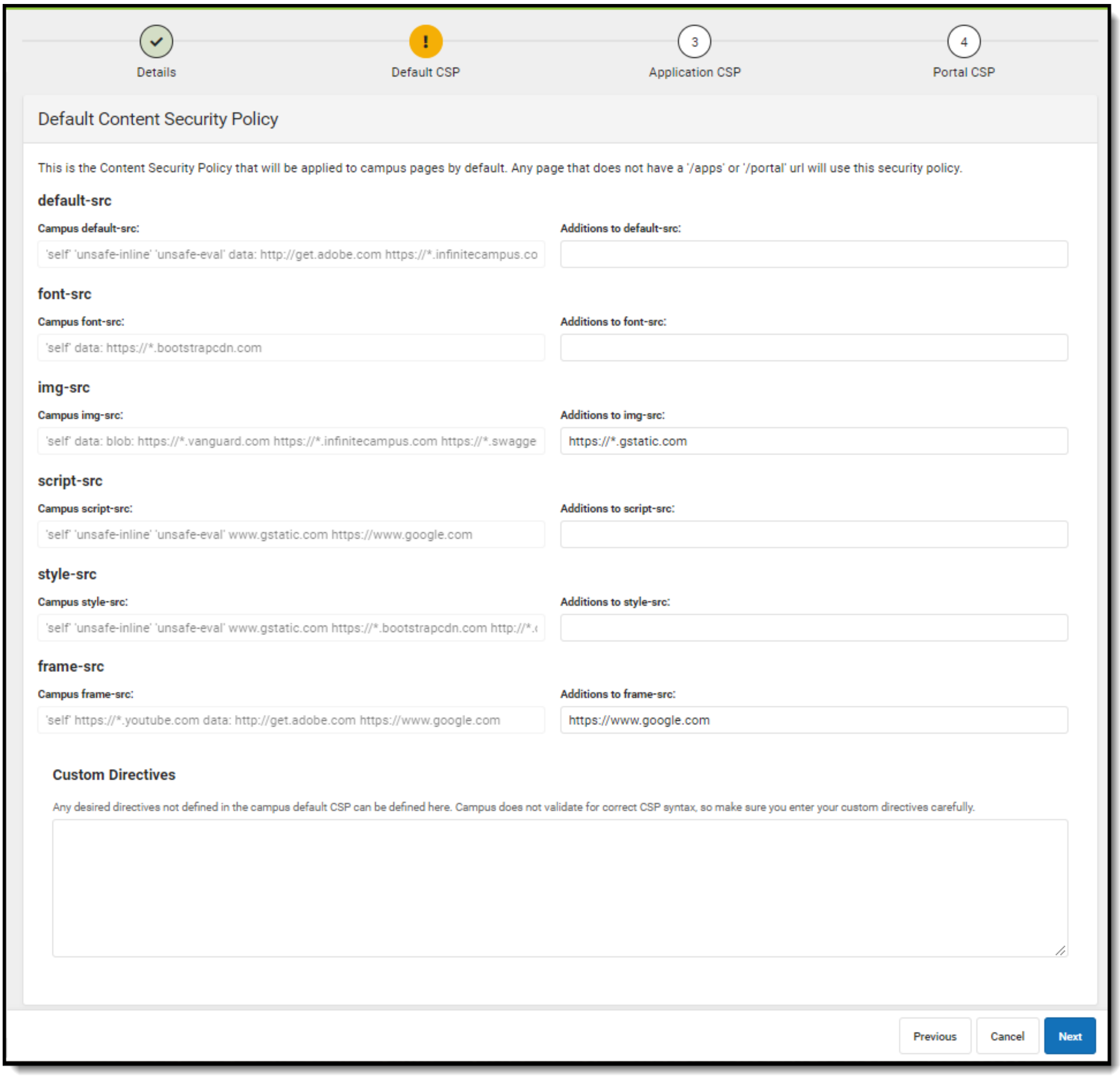
Content Security Policy Details

CSP Name: * Custom

Description: A custom policy allows you to add additional security directives to the default Infinite Campus CSP.

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).



Default Content Security Policy

This is 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-src

Campus default-src: 'self' 'unsafe-inline' 'unsafe-eval' data: http://get.adobe.com https://*.infinitecampus.co

Additions to default-src:

font-src

Campus font-src: 'self' data: https://*.bootstrapcdn.com

Additions to font-src:

img-src

Campus img-src: 'self' data: blob: https://*.vanguard.com https://*.infinitecampus.com https://*.swagge

Additions to img-src: https://*.gstatic.com

script-src

Campus script-src: 'self' 'unsafe-inline' 'unsafe-eval' www.gstatic.com https://www.google.com

Additions to script-src:

style-src

Campus style-src: 'self' 'unsafe-inline' 'unsafe-eval' www.gstatic.com https://*.bootstrapcdn.com http://*.

Additions to style-src:

frame-src

Campus frame-src: 'self' https://*.youtube.com data: http://get.adobe.com https://www.google.com

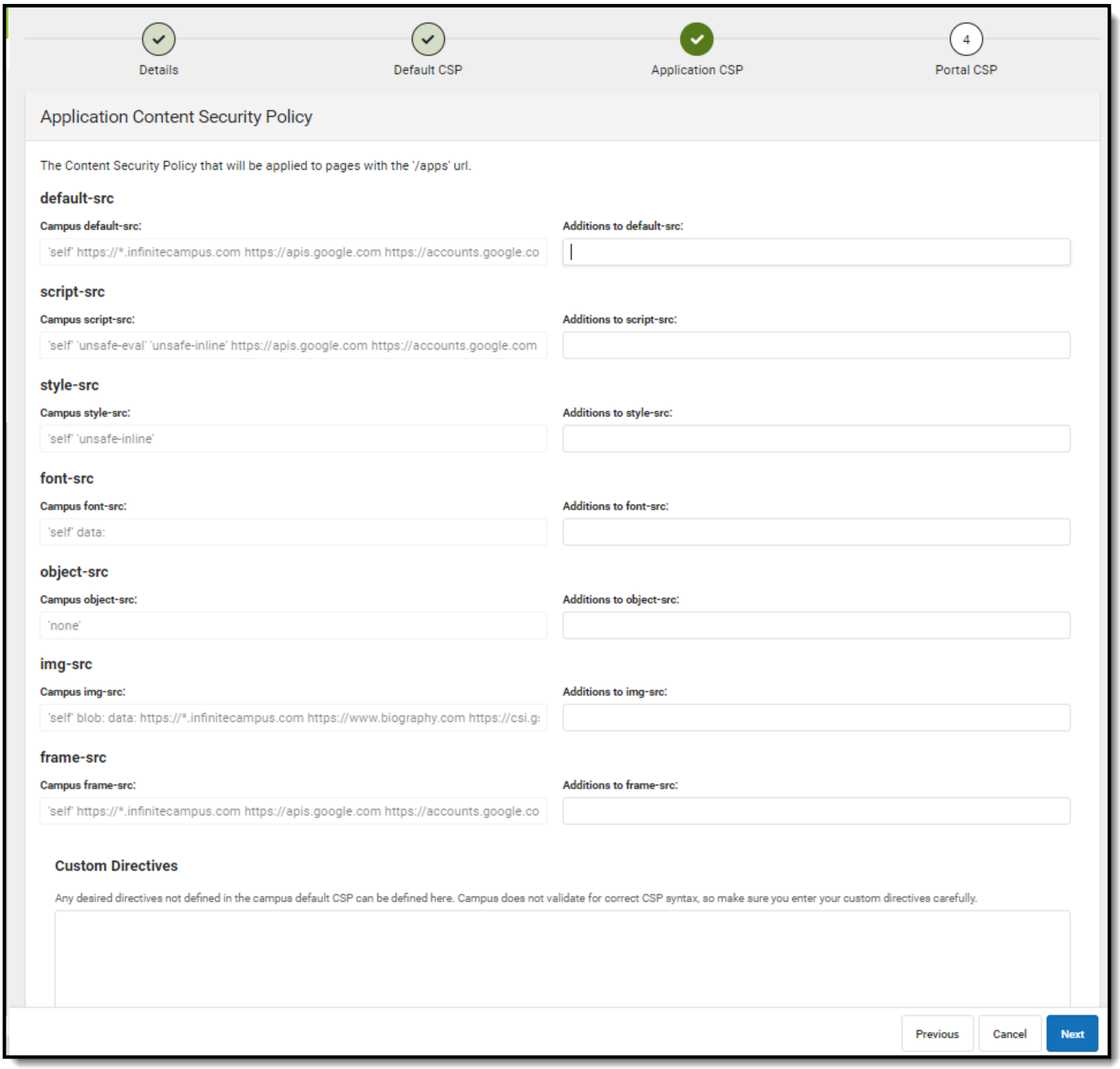
Additions to frame-src: https://www.google.com

Custom Directives

Any desired directives not defined in the campus default CSP can be defined here. Campus does not validate for correct CSP syntax, so make sure you enter your custom directives carefully.

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).



Application Content Security Policy

The Content Security Policy that will be applied to pages with the '/apps' url.

default-src

Campus default-src: 'self' https://*.infinitecampus.com https://apis.google.com https://accounts.google.co

Additions to default-src:

script-src

Campus script-src: 'self' 'unsafe-eval' 'unsafe-inline' https://apis.google.com https://accounts.google.com

Additions to script-src:

style-src

Campus style-src: 'self' 'unsafe-inline'

Additions to style-src:

font-src

Campus font-src: 'self' data:

Additions to font-src:

object-src

Campus object-src: 'none'

Additions to object-src:

img-src

Campus img-src: 'self' blob: data: https://*.infinitecampus.com https://www.biography.com https://csi.g

Additions to img-src:

frame-src

Campus frame-src: 'self' https://*.infinitecampus.com https://apis.google.com https://accounts.google.co

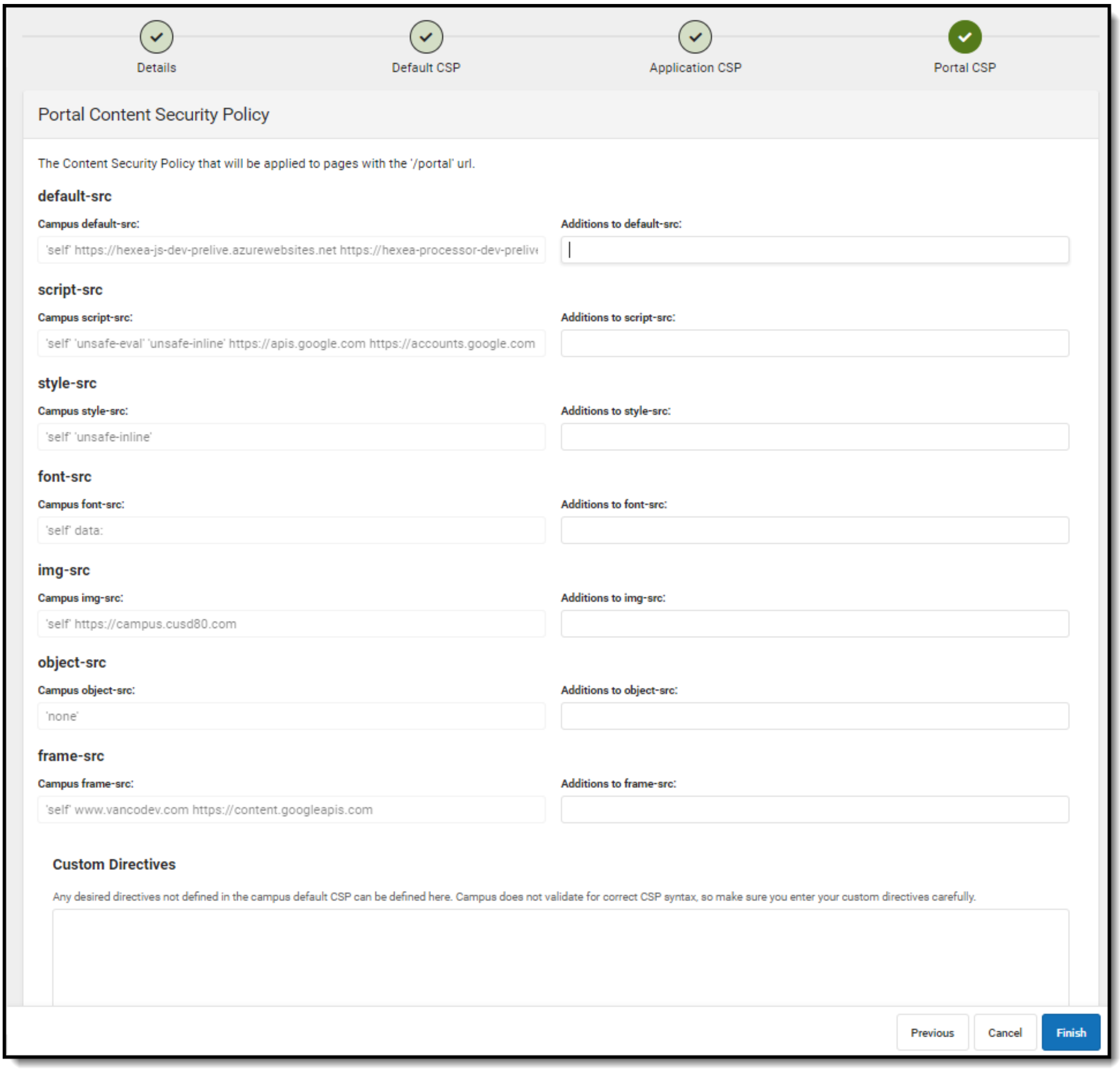
Additions to frame-src:

Custom Directives

Any desired directives not defined in the campus default CSP can be defined here. Campus does not validate for correct CSP syntax, so make sure you enter your custom directives carefully.

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.



Portal Content Security Policy

The Content Security Policy that will be applied to pages with the '/portal' url.

default-src

Campus default-src: 'self' https://hexea-js-dev-prelive.azurewebsites.net https://hexea-processor-dev-prelive

Additions to default-src:

script-src

Campus script-src: 'self' 'unsafe-eval' 'unsafe-inline' https://apis.google.com https://accounts.google.com

Additions to script-src:

style-src

Campus style-src: 'self' 'unsafe-inline'

Additions to style-src:

font-src

Campus font-src: 'self' data:

Additions to font-src:

img-src

Campus img-src: 'self' https://campus.cusd80.com

Additions to img-src:

object-src

Campus object-src: 'none'

Additions to object-src:

frame-src

Campus frame-src: 'self' www.vancodev.com https://content.googleapis.com

Additions to frame-src:

Custom Directives

Any desired directives not defined in the campus default CSP can be defined here. Campus does not validate for correct CSP syntax, so make sure you enter your custom directives carefully.

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

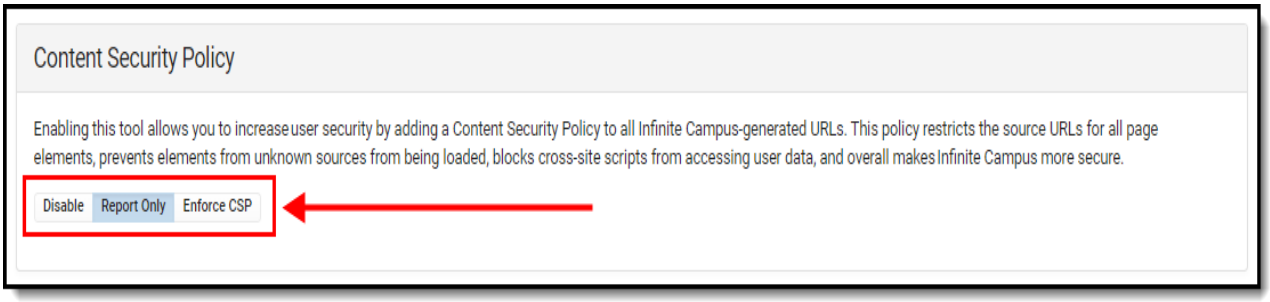
Enforce, Report, or Disable the Content Security Policy (CSP)

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.

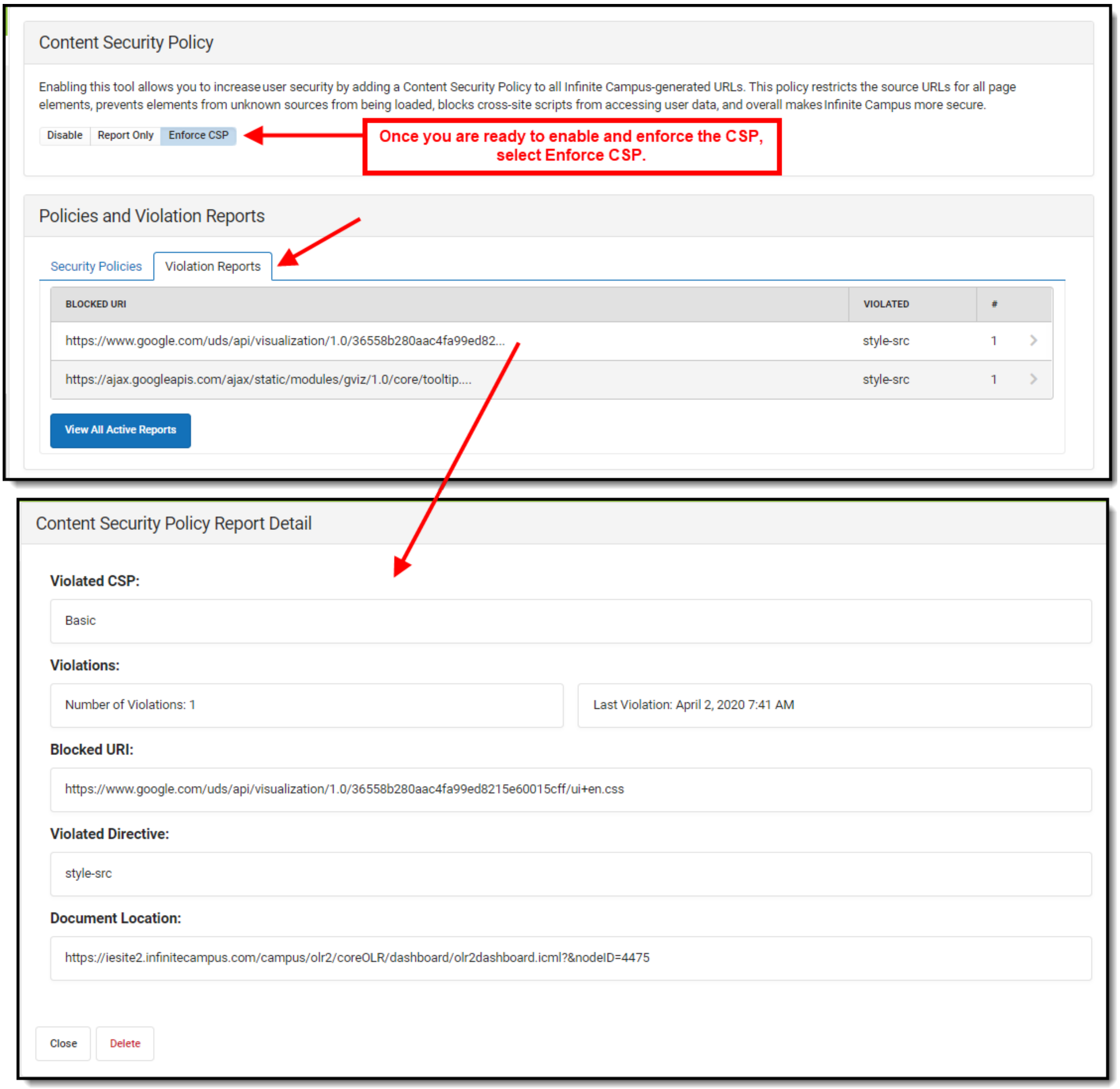
Image 10: Enforcing, Reporting, or Disabling the CSP

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

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.

Once you are ready to enable and enforce the CSP, select Enforce CSP.

Policies and 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

Content Security Policy Report Detail

Violated CSP: Basic

Violations: Number of Violations: 1 | Last Violation: April 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

Image 11: Reviewing CSP Violations