How to Enable CORS Validation

Nx Support
2 months ago · Updated

By default, the Media Server uses a **Standard** security level with a permissive Cross-Origin Resource Sharing (CORS) policy. This ensures broad compatibility with third-party integrations and embedded clients.

However, this carries a security trade-off: a malicious web page visited by an authenticated user could potentially access session data. **Enabling strict CORS validation** restricts the server to prevent this class of attack.

Security Levels

When configuring the Media Server, you can choose between two security levels:

- **Standard (Default):** Permissive; the server reflects any `Origin` header. This is compatible with all integrations but disables strict CORS protection.

- **High (Strict):** Restrictive; the `Origin` header is validated. This prevents unauthorized cross-origin session access but may impact some third-party integrations.

New Installations

You can enable CORS protection during the initial setup wizard by selecting **High** in the **Advanced Site Settings**.

- **Via WebAdmin:** During "Setup New Site," select **Advanced Site Settings** and set the **Security level** dropdown to **High**.
- **Via Desktop Client:** In the "Get Started" dialog, select **Advanced system settings** and set the **Security Level** to **High**.

Existing Installations (API Method)

For systems already in production, you can toggle strict CORS validation by updating the `supportedOrigins` site setting via the **WebAdmin** or the **REST API**.

WebAdmin method

1. Navigate to the hidden Advanced settings of the **WebAdmin** via: `https://<serverIp>:7001/#/settings/advanced`
2. Scroll down till you find the **HTTP header: Origin** `supportedOrigins` setting.
3. Enter `null` to Enable Strict CORS Validation or `*` to Disable Strict CORS Validation:

Enabled Strict CORS Validation:

Disabled Strict CORS Validation:

REST API method

1. Enable Strict CORS Validation

To activate strict protection, send a `PATCH` request to set the supported origins to **null**. This prevents the server from reflecting untrusted origins in the `Access-Control-Allow-Origin` header.

Request: `PATCH /rest/v4/site/settings`

Body:

```
{
  "supportedOrigins": "null"
}
```

2. Disable Strict CORS Validation (Revert)

To return to the standard permissive behavior, set the value to a wildcard (*****).

Request: `PATCH /rest/v4/site/settings`

Body:

```
{
  "supportedOrigins": "*"
}
```

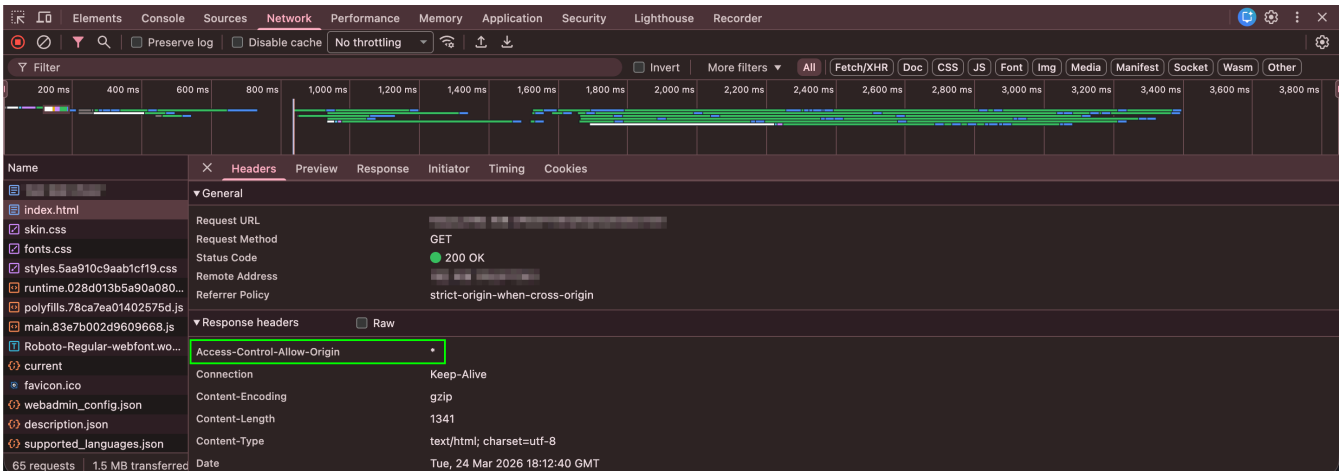
NOTE: Before sending the `PATCH` request to `/rest/v4/site/settings`, you must obtain a **fresh bearer token** by authenticating via the `/rest/v4/login/sessions` endpoint.

Verification

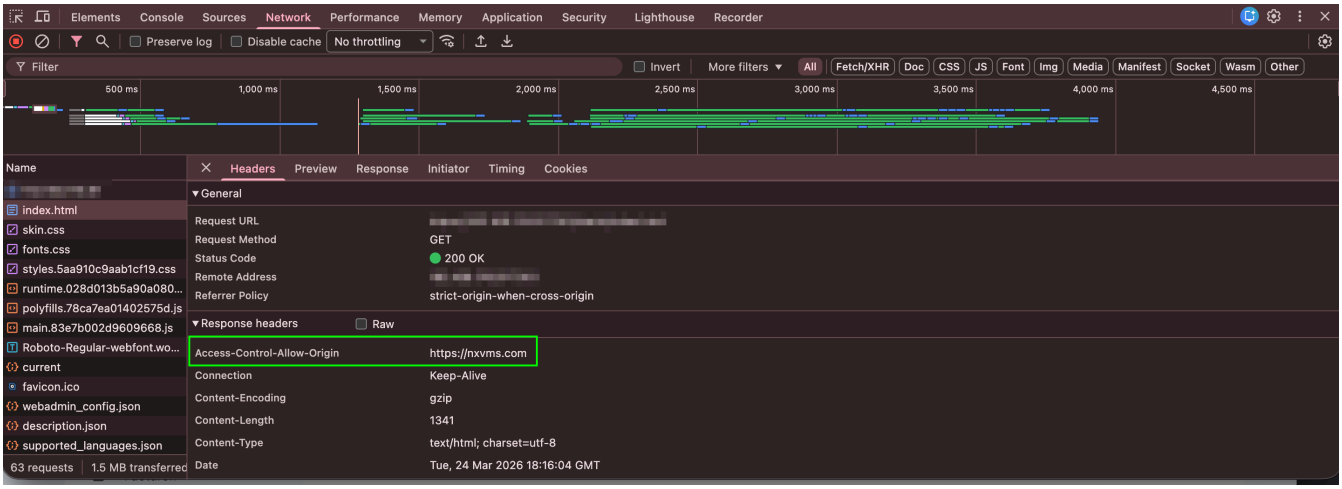
To verify the change using your browser, follow these steps:

1. Open the **WebAdmin** page
2. **Open Developer Tools**: Press **F12** (or **Ctrl+Shift+I**) and select the **Network** tab.
3. Refresh the **WebAdmin** page.
4. **Inspect the Call**: for example the `index.html` page
5. **Check Response Headers**: Look for the **Headers** (or **Response**) sub-tab and locate `Access-Control-Allow-Origin`.

CORS validation disabled:



CORS validation enabled:



Compatibility Considerations

Before applying the **High** security level or setting `supportedOrigins` to `null`:

- **Audit Integrations:** Identify any web-based dashboards or embedded clients that call the API from a different domain.
- **Test in Staging:** Ensure that legitimate cross-origin requests are not blocked.
- **Explicit Allowlist:** If you have a specific trusted domain that requires access, contact your administrator to configure a specific origin instead of using `null`.

Related to

cors

Was this article helpful?

Yes No

0 out of 0 found this helpful

Have more questions? Submit a request

Return to top

Related articles

Controlling Uniview Camera White Lights via a Do HTTP(S) request

Understanding the Remote Access Tool (RAT) Configuration

How to change software logging level and how to get logs

Integrating WisenetRoadAI with the VMS

Access the Nx Witness User Manual

Comments

0 comments

Article is closed for comments.