



# Ericom Shield and Forcepoint DLP

*Enabling Data Loss  
Prevention in Isolated  
Web Browsing*

Date: July 2020

## Solution Background and Overview

Ericom Shield offers robust protection against in-bound web borne malware. Ericom and Forcepoint understand that sophisticated insider threats may attempt to use internet gateways, including isolation gateways like Ericom Shield, as a path to exfiltrate sensitive data to unauthorized locations. Ericom Shield supports Forcepoint DLP to ensure that sensitive data cannot be leaked externally by communicating with an upstream Forcepoint proxy chain enabled with DLP. This technote explains how to configure Ericom Shield to use Forcepoint DLP.

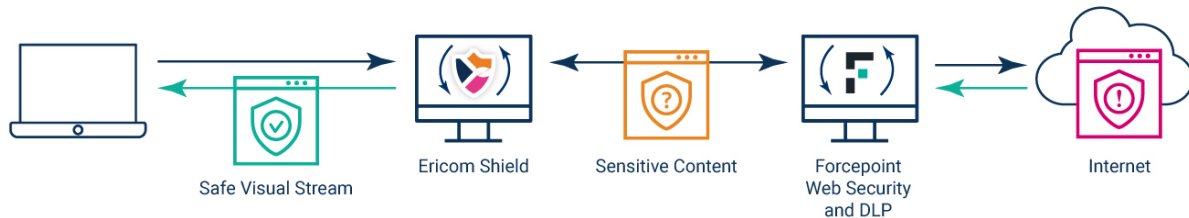
## Solution Technical Details

Supported software name and versions

- Ericom Shield 20.x
- Forcepoint Data Loss Prevention (DLP)

Before beginning the configuration, ensure that Ericom Shield can browse successfully to the Internet and that Forcepoint DLP is functioning correctly.

### Data flow overview and architectural diagram

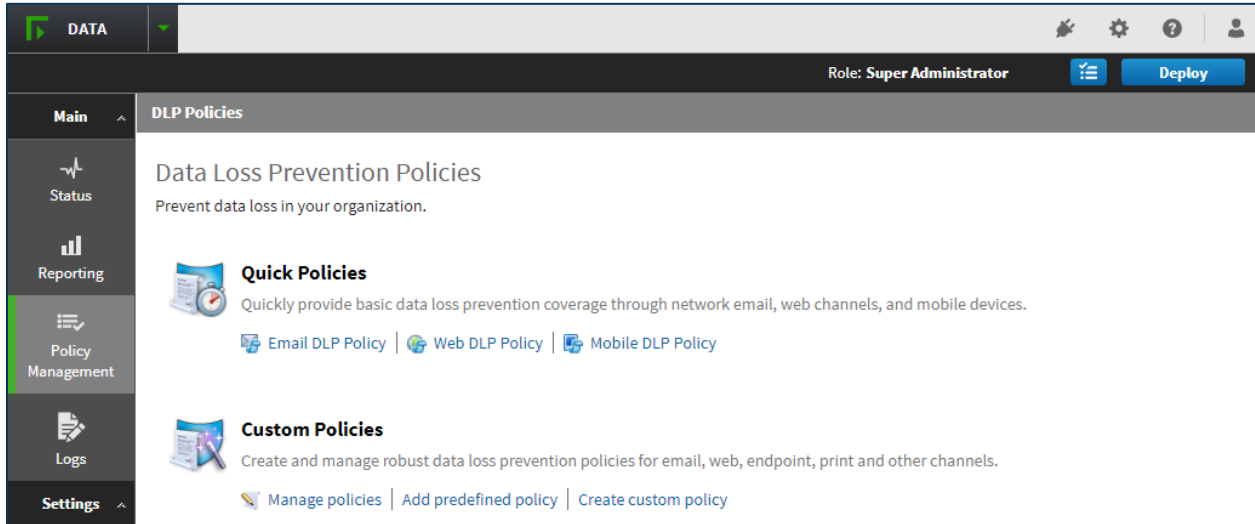


The data flow of this design is as follows:

- 1) User requests a URL that is sent to Ericom Shield for isolation protection
- 2) Ericom Shield attempts to navigate to the requested URL via Forcepoint proxy with DLP enabled
- 3) Ericom Shield opens the content in disposable Linux containers and sends a safe visual stream of pixels to the end user's browser
- 4) If the user exfiltrates data from the browser container, Forcepoint DLP will intercept it and apply configured action on the request

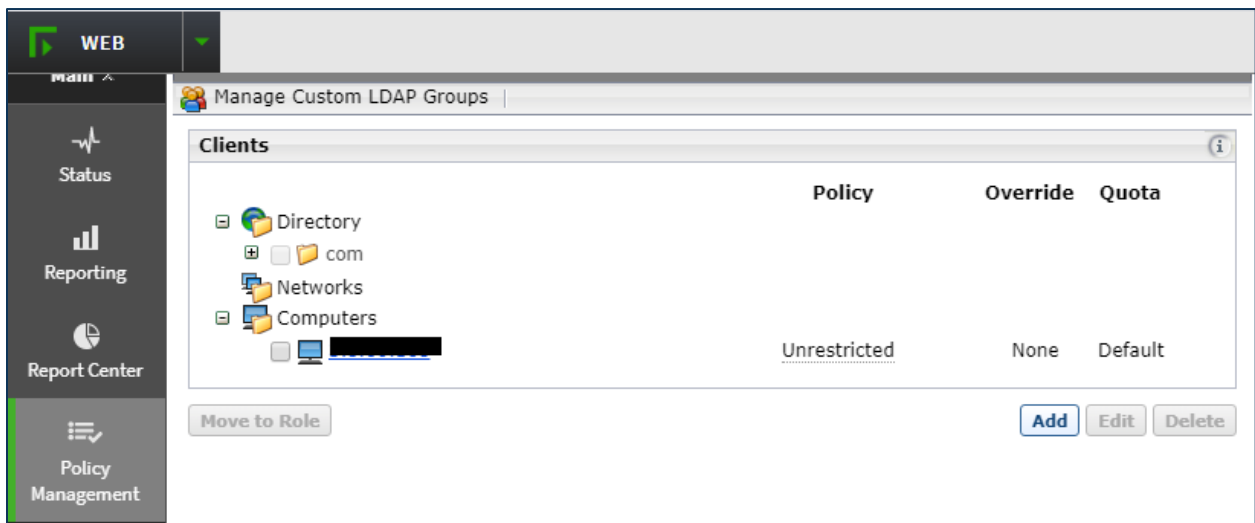
## Forcepoint DLP Configuration

Configure Forcepoint DLP as desired, no proprietary configuration is required for use with Ericom Shield.

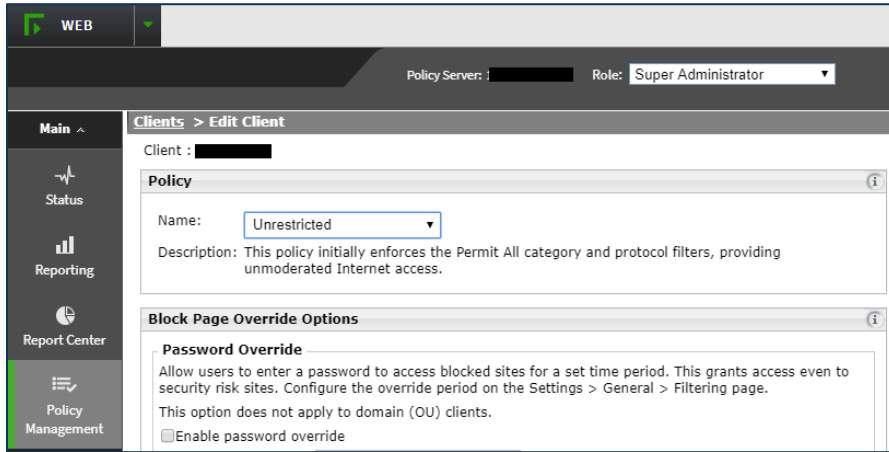


## Forcepoint Web Security Policy configuration

Add a "Client" to Forcepoint Web Security with the Ericom Shield address:



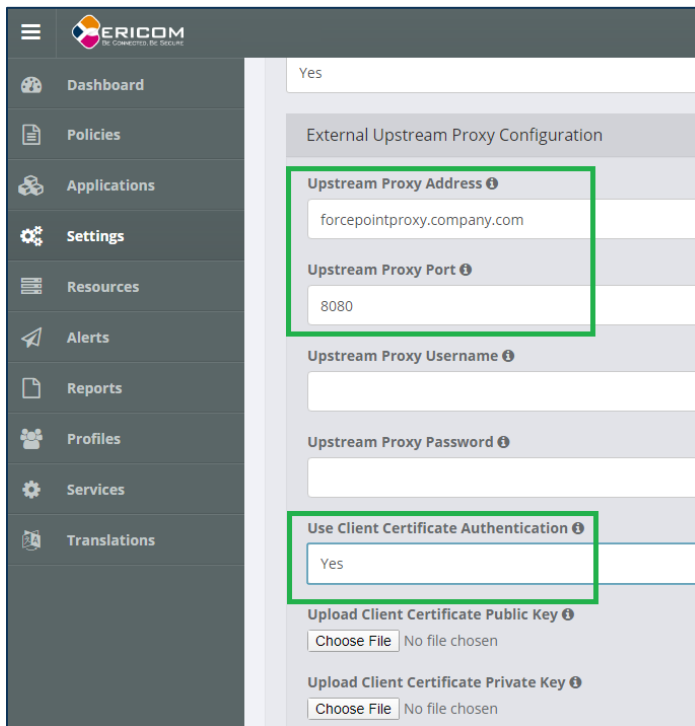
Assign this Client to **Unrestricted** so Ericom Shield can browse the Internet.



A custom policy other than **Unrestricted** may also be used to set conditions on how Ericom Shield will browse the Internet.

## Ericom Shield Configuration

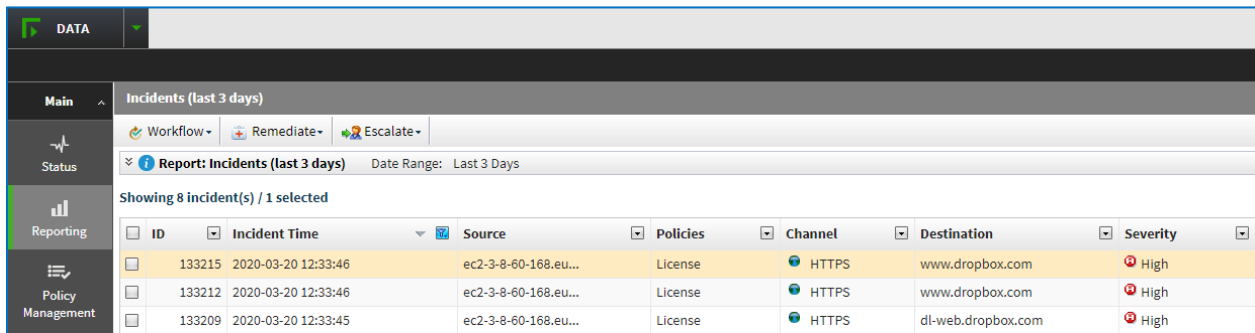
Configure Ericom Shield to use Forcepoint DLP system as the **Upstream** proxy.



Optional: Add the public and private keys that are used by Forcepoint. Add the proxy username and password to authenticate into Forcepoint, if this is required.

## Testing DLP

Upload a file to a website being isolated by Ericom Shield that will trigger a Forcepoint DLP condition. After the operation completes, go to the Forcepoint DLP Reporting section to view the event. In the example below, the report for the “Incidents (last 3 days)” is used. A file was uploaded to dropbox.com that triggered the DLP condition.



The screenshot shows the 'Incidents (last 3 days)' report in the Ericom DLP Reporting section. The interface includes a sidebar with navigation options like 'Main', 'Status', 'Reporting', and 'Policy Management'. The main area displays a table of incidents with columns for ID, Incident Time, Source, Policies, Channel, Destination, and Severity. Three incidents are listed, all with a severity of 'High' and originating from 'ec2-3-8-60-168.eu...'. The destinations are 'www.dropbox.com' and 'dl-web.dropbox.com'.

ID	Incident Time	Source	Policies	Channel	Destination	Severity
133215	2020-03-20 12:33:46	ec2-3-8-60-168.eu...	License	HTTPS	www.dropbox.com	High
133212	2020-03-20 12:33:46	ec2-3-8-60-168.eu...	License	HTTPS	www.dropbox.com	High
133209	2020-03-20 12:33:45	ec2-3-8-60-168.eu...	License	HTTPS	dl-web.dropbox.com	High

## About Ericom

Ericom Software provides businesses with secure access to the web and corporate applications, in the cloud and on-premises, from any device or location. Leveraging innovative isolation capabilities and multiple secure access technologies, Ericom’s solutions ensure that devices and applications are protected from cybersecurity threats, and users can connect to only the specific resources they are authorized to access.