

Whitelisting and Browser Requirements

ACLP Site Whitelisting

The following items should be whitelisted so users can access and take training on the SANS Advanced Cybersecurity Learning Platform (ACLP).

ACLP Domains

learn.sans.org (443, 8443)

learn.sans.org (443)

report.sans.org (443)

jasport.sans.org (8443)

cc.sans.org (80, 443)

transfer.sans.org (443)

access.sans.org (443)

login.sans.org (443)

ACLP Email IP Addresses

54.240.58.80

54.240.58.81

54.240.58.82

Phishing Whitelisting

Clients who have Phishing will also need to whitelist an additional domain and IP address.

Phishing Image Domain

ybpbox.com (80, 443)

Phishing Email IP Address

This is the IP for all mail delivery within the SANS Phishing solution:

52.34.244.186 (mail.phishing.sans.org)

Additional Information

- Whitelisting <https://learn.sans.org> (URL) or learn.sans.org (domain) will prevent popup blockers and ensure delivery of notification images.
- SANS hosts video files on Amazon CloudFront. If you are not blocking external media or internet sites, no action will need to be taken. If you do block external media, you may need to allow Amazon CloudFront. The Cloudfront addresses are:

<https://d2hvigoj32t43z.cloudfront.net> <https://d1c5ja4blaaees.cloudfront.net>

- If you fall back to Flash, the courseware is downloading a lightweight swf file from: Vjs.zencdn.net
- Reporting uses ports 443, 8443 – ensure these are open to access the reporting platform
- Training is video-based and requires users to play audio and interact with the site via mouse or keyboard. *Our training content is Section 508 compliant for assistive technologies.*
- Standard video quality typically requires 0.5Mb/s. *A lower quality video is available for clients with bandwidth constraints.*

Whitelisting and Browser Requirements

Email Addresses

Notification “From” Address

The ACLP can automatically email notifications to inform users of their training assignment and status. These emails can be configured to be sent from the address of your choosing. We recommend using a domain owned by your organization. The ACLP uses Amazon Web Services (AWS) Simple Email Service (SES) to have a secure platform for all outgoing emails. *For more information about Amazon SES Email Authentication, visit: <http://docs.aws.amazon.com/ses/latest/DeveloperGuide/spf.html>*

To configure the email address displayed on your notifications, you will need to provide the email address or domain on the Account Settings page of your Administrator Dashboard. Once submitted, Amazon SES will send two separate verification emails to the email address from no-reply-aws@amazon.com. You will need to click the link provided in the emails to verify your email address.

NOTE: Gmail addresses can sometimes consider notifications to be spoof. If you are not receiving notifications from a Gmail address, try using no-reply@aclp.org to test.

For more spoofing details, visit: <https://community.mimecast.com/docs/DOC-1369#550>

SPAM Filter Registration

Register the following email addresses to your SPAM filter to ensure the successful delivery of the applicable items:

Email Address	Sends
no-reply-aws@amazon.com	Notification email address verification
Your sending email address	Notifications
access@sans.org	Password reset
no-reply@sans.org	User Import confirmation or failure notifications
adv_rep_notifications@sans.org	Scheduled Reports

Whitelisting and Browser Requirements

Supported Browsers

The SANS ACLP supports the following desktop browsers. If you are not using one of these browsers (or versions) to interact with the system, please download or upgrade to a supported version. If you elect not to upgrade your desktop browser, your experience may not be optimal.

NOTE: Interactive videos are not mobile compatible.

Computer			
			
42+	37+	9 - 11	7 8.0.5
Mobile			
			
7x	8.3	4.5	5.1
Tablet			
			
7.1.1	8.3	7.1	8.3

NOTE: The SANS ACLP may not work properly with beta or pre-release versions of these browsers. Download the latest commercial version for the best experience.

Whitelisting and Browser Requirements

Internet Explorer Security Settings

- For IE11 users, we recommend selecting “Enable Font Downloads” to ensure proper display of images, such as the completion checkmark for completed modules on the Learner Dashboard.
- Compatibility Mode must be turned OFF.
- To play HTML5 videos in the Internet Zone, you need to use the default settings or make sure the following registry key value 2701 under.
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 is set to 0.

The default value is 0 = Allow

If set to 3 = Disallow

This key is read by the URL Action Flag that can be taken in a URL Security Zones.