N4L Web Filtering:

Secure Website Inspection and Individualised Filtering Deployment Guide

LAST UPDATED: 4 NOV 2015

VERSION 2.0

Contents

1. Introduction

As the internet has developed there has been an increasing emphasis on security - terms like "SSL" and "HTTPS" are often used. This emphasis on security means that it is not directly possible to read data that flows between a web browser and a web server by any system that sits between the browser and the server.

N4L's In Depth Web Filtering permits users to enter their school network username and password and be given access to specific sites only based on the groups that they are in.

IT Administrators will have the ability to leverage a school's local directory services and a security certificate to provide a filtering policy that allows browsing flexibility in terms of who (which users), when (the time of day) and where (which web sites).

N4L's website can provide further information on N4L's Web Filtering including tutorials.

2. Objective

This document is intended for IT Administrators and Web Filtering Administrators tasked with implementing Secure Website Inspection or Individualised Filtering

The objectives of this document are to:

- Give an overview of the N4L process to get access to inspection certificates
- Explain what HTTPS is and what it does
- Show users how to generate and download the school's inspection certificate
- Provide use cases that could be used to help you decide how to deploy the inspection certificates to all devices in your own school
- Explain the support N4L can provide
- Give the Web Filtering Administrator a *How To* guide on changing filters, rules and policies in the N4L Web Filtering Dashboard once all certificates have been installed

3. Deployment Prerequisites

Before deployment of this service, the school should ensure the chosen implementor has an understanding of:

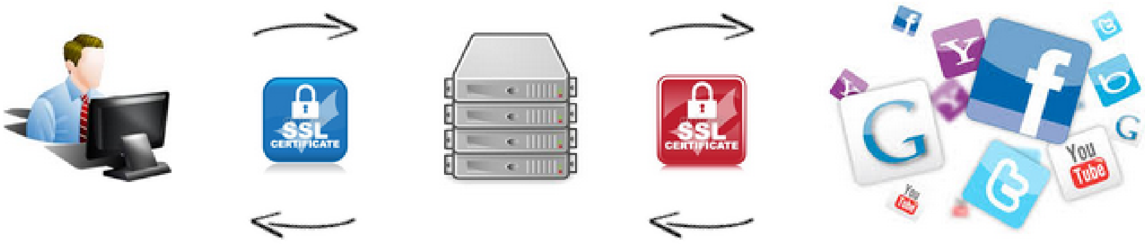
- TCP/IP
- Subnetting
- DHCP Scopes
- Routing & Switching
- Firewalls
- DNS
- Active Directory / LDAP or SAML
- Certificates
- LAN and WLAN troubleshooting

4. Abbreviations and Definitions

Term	Definition/Explanation
CCWS - Cisco Cloud Web Security	N4L uses the Cisco Cloud Web Security (also known as Scansafe) platform to provide web filtering services. Full information on the dashboard and how to use it can be found on the N4L website - http://www.n4l.co.nz/managednetwork/webfiltering/
Directory Integration	Leveraging a school's existing directory service to provide individualised filtering capabilities.
BYOD	Bring Your Own Device
SSL	Secure Sockets Layer
TLS	Transport Layer Security
HTTP	Hypertext transfer Protocol
HTTPS	Hypertext transfer Protocol over SSL or TLS

5. Secure Website Inspection

A key feature of Cisco Cloud Web Security (CCWS) tool is its ability to decrypt and scan the HTTPS traffic passing through CCWS for threats and carry out actions based on your policy settings. If the traffic is deemed safe it is re-encrypted and passed back to your users with a new SSL certificate.



For reasons of privacy Secure Website Inspection can be limited to specific sites or categories. For example you may decide to more closely monitor social networking sites but not monitor any internet banking or online shopping sites.

Any Secure Website Inspection will require that a device wishing to access selected secure web content install a special inspection certificate (Trusted Root Certificate) before access can be granted to the site - ensuring traffic between the end users' browser and N4L filtering service is secure. Individual devices or network segments may be excluded from HTTPS Inspection if required.

The security certificate available for generation and download via the N4L Web Filtering dashboard has been tested to work on Windows, OSX, iOS, Android as well as Chrome based devices.

Considerations to be aware of:

- Filtering secure sites is important, it means you can supply access to secure HTTPS sites for educational purposes, while keeping your school community safe and secure.
- You sign a blanket agreement with N4L related to the searching and filtering of private user data. The school might decide to have additional agreements as part of their IT school policy that the individuals within the school community agree to, ensuring you have agreement from them to search and filter their user data.
- Inspection certificates expire so ensure you track their expiry as part of your school's internal systems and processes.
- If you do not have an internal IT support person you may need to use the IT company that supports your school. Be aware that if they are tasked with managing your certificates to all devices that this may incur a cost each time a certificate expires and needs renewing.
- If you are implementing, or have implemented, BYOD consider that the certificate has to be installed on every device and any new ones as they start to be used.

- The use of a certificate on an Android device will require the device to use a PIN code to securely access the device. Any other lock screen access method is unsupported by Android at this time.
- Some devices require certificates to be changed to a suitable format before they can be installed.

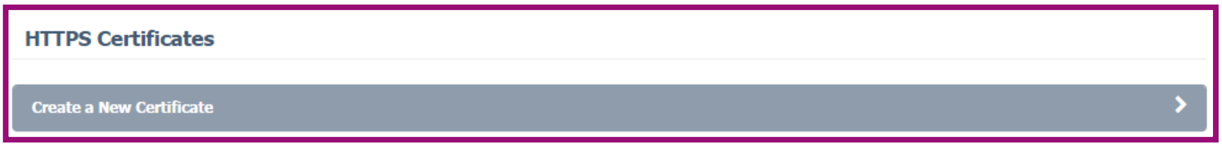
5.1. Overview of the process

1. Once you have decided to implement Secure Website Inspection you will need to nominate a contact person who will manage the inspection certificates and devices. This may be the Web Filtering Administrator if they have a technical background.
2. Certificates are generated and downloaded by either the school or N4L
3. Your allocated IT administrator can then organise to install the certificate onto all devices being used at school.
4. Your Web Filtering Administrator can then make changes to your N4L Web Filtering Dashboard to change the filters, rules and policy to filter secure sites as required.

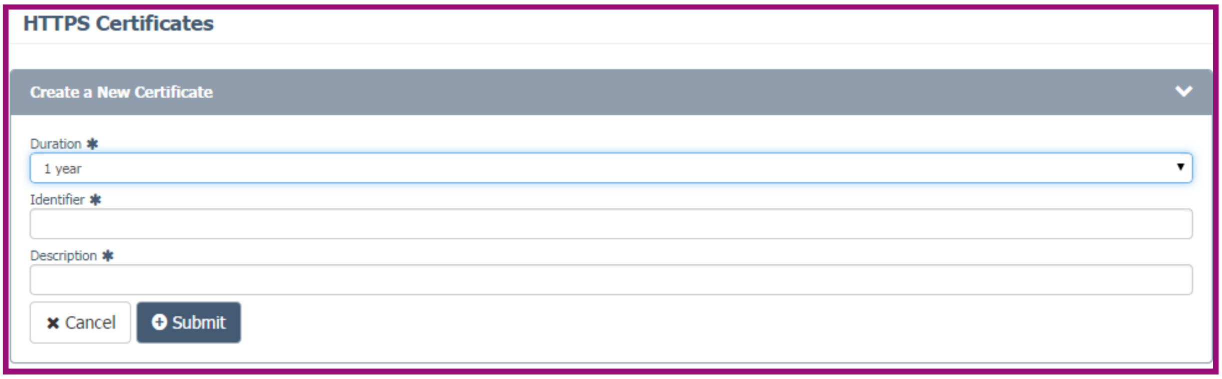
5.2. Creating the Certificate

You can create your own certificate within the school's N4L Web Filtering Dashboard.

1. Log into your N4L Web Filtering Dashboard
2. Click on the **Admin** tab
3. Choose **Certificates** from the **HTTPS Inspection** drop-down menu
4. Click on **Create a New Certificate**



5. Complete all the fields



5.1. Choose the **Duration**: 1, 3 ,5 or 7 years

Note: Shorter length certificates provide a greater level of user security by ensuring certificates do not remain ‘trusted’ on a device for longer than needed (e.g. student or teachers no longer attending a specific school). On the flip side, certificates with a long expiry time reduce admin overhead in that certificates do not need to be renewed and installed across all devices as regularly.

5.2. Add a unique school **Identifier**:
We recommend using the following format to ensure the expiry can be tracked: SCHOOLNAME_HIGH_SCHOOL_From date-To date of expiry. (e.g. Greenwood_High_School_Jan_2014-2021)

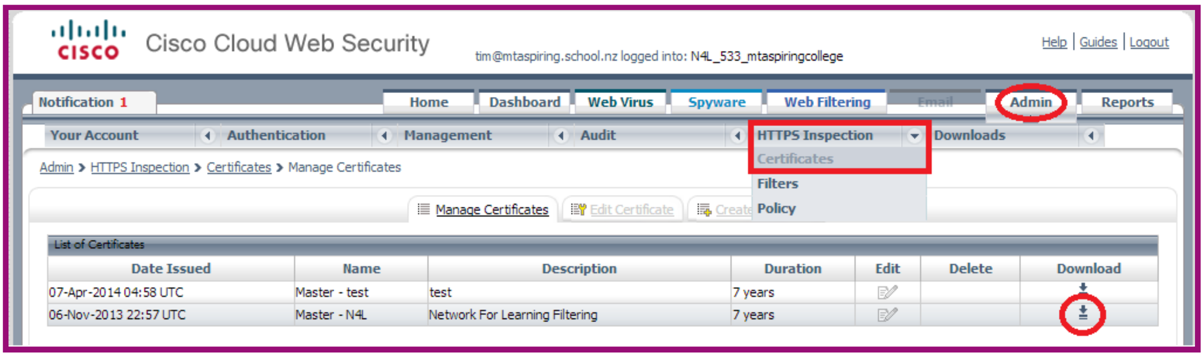
5.3. Add a **Description**:
We recommend using the same name used above to ensure there is no confusion when creating a new certificate at a later date.

5.4. Click **Submit**

5.3. Downloading the Certificate

Once generated, the unique security certificate is available for download from the N4L Web Filtering dashboard.

1. Click on the **Admin** tab
2. Choose **Certificates** from the **HTTPS Inspection** drop-down menu



Cisco Cloud Web Security

tim@mtaspiring.school.nz logged into: N4L_533_mtaspiringcollege

Admin > HTTPS Inspection > Certificates > Manage Certificates

List of Certificates

Date Issued	Name	Description	Duration	Edit	Delete	Download
07-Apr-2014 04:58 UTC	Master - test	test	7 years			
06-Nov-2013 22:57 UTC	Master - N4L	Network For Learning Filtering	7 years			

3. Search the list of certificates and choose the one which has been created specifically for your school.

Note: You’ll be able to identify this by the name of the certificate and the time period it covers (e.g Greenwood_High_School_Jan_2014-2021).

4. Download the certificate using the **Download** link on the right hand side
5. Save it to a location that is widely accessible to your users

What’s next ?

Certificates may be installed on a device by:

- Emailing the certificate to users, or
- Making the certificate available on a suitable network share or website, or
- Providing it on a USB stick, or
- Preferably by rolling it out via local group policies or an equivalent automated process for the devices used in your school

Note: if you do not use a mobile device management platform capable of pushing certificates out to end user devices, the next easiest way to get the certificate to users is often via email.

5.4. Manual Installation of Certificates on Devices

For specific instructions on how to deploy certificates across all the devices within your environment, we highly recommend that you consult with your preferred ICT provider to ensure the correct approach is taken.

If you do not have a current ICT support company, we can help put you in touch with an ICT support company who will be able to assist you with certificate deployment, as well as filtering policy required to effectively filter secure web content.

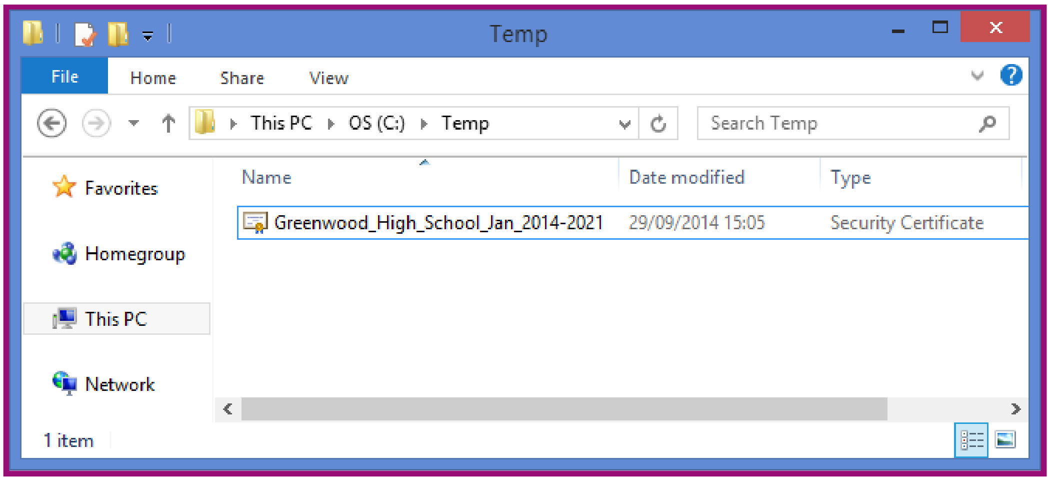
5.4.1. Manually installing certificates on Microsoft Windows

When installing certificates manually onto devices which run Microsoft Windows, some additional steps are required to maintain maximum security, this involves installing the certificate into the correct location and certificate store during the certificate installation wizard.

First make the certificate available to the users.

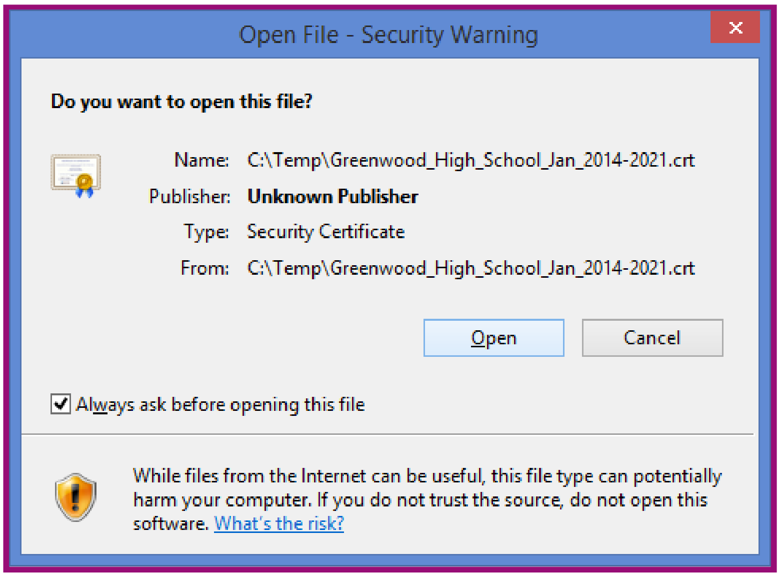
The user will then:

1. Go to where the certificate is saved and either:
    - 1.1. Right click on the certificate and choose install, or
    - 1.2. Click on the certificate, this opens up the certificate and the user can then click on install



Name	Date modified	Type
Greenwood_High_School_Jan_2014-2021	29/09/2014 15:05	Security Certificate

2. This will then show:



Do you want to open this file?

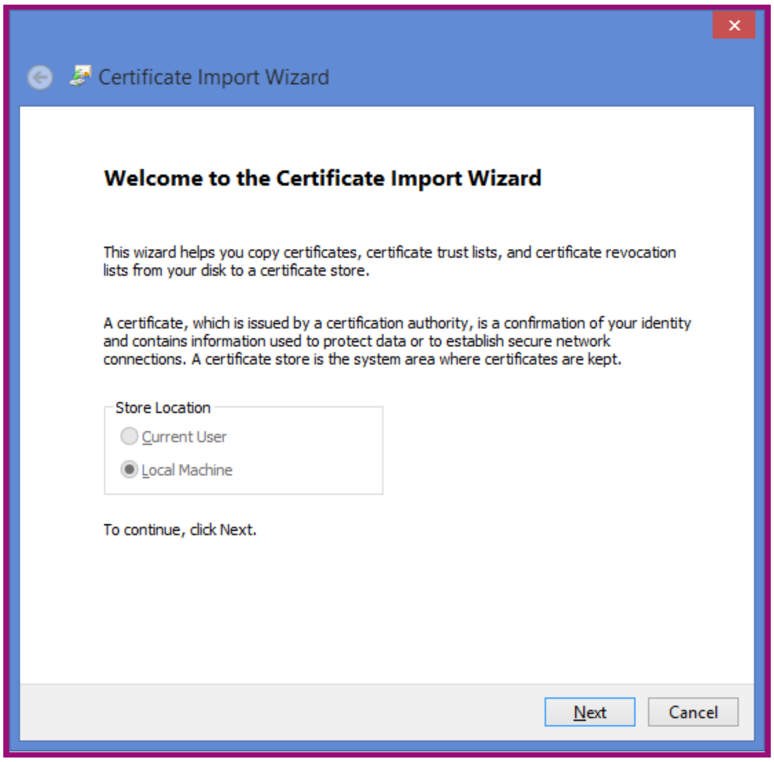
Name: C:\Temp\Greenwood_High_School_Jan_2014-2021.crt
Publisher: **Unknown Publisher**
Type: Security Certificate
From: C:\Temp\Greenwood_High_School_Jan_2014-2021.crt

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

3. Next you need to carefully consider which certificate store to install the certificate into. This will vary depending on how your users use their devices.

Store Name	Use Case
Local Machine Store	For PCs used by multiple users
Current User Store	For PCs used by one staff member/student only, or where only one user may have consented to having their secure traffic inspected.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

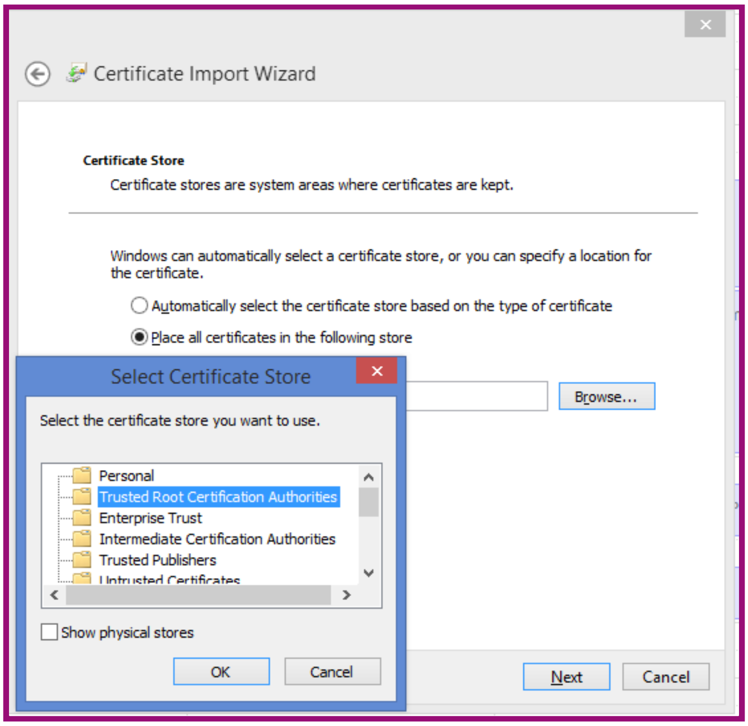
Store Location

○ Current User

● Local Machine

To continue, click Next.

4. Once you have selected the User or Local Machine store, install the certificate into the **Trusted Root Certification Authorities** store to ensure correct operation as shown in the example below.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Select Certificate Store

Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates

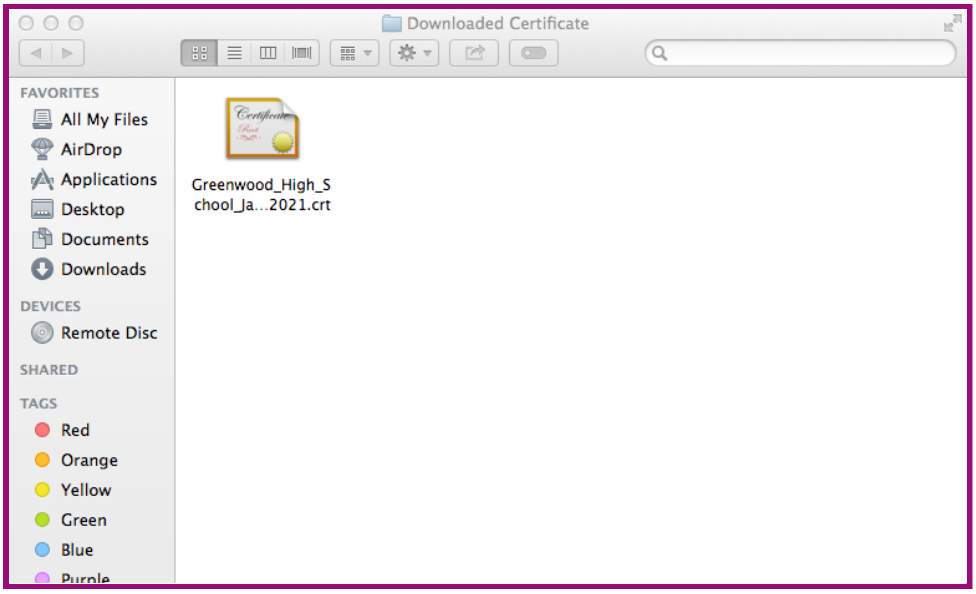
□ Show physical stores

5.4.2. Manually installing certificates on Apple OSX

When installing certificates manually onto devices which run Apple OSX some additional steps are required to maintain maximum security. This involves installing the certificate into the correct location depending on whether the device is shared amongst multiple users, or used by only a single user.

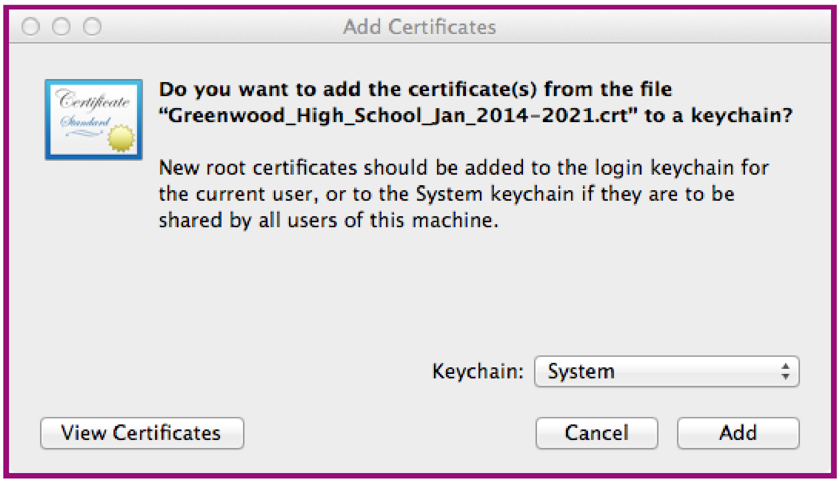
First make the certificate available to the users.

1. The user will then:
   1.1. Double click on the certificate file and follow the wizard to add the certificate to the Keychain.



   1.2. Here you have two options:

Store Name	Use Case
System Keychain	For devices used by multiple users
Local User KeyChain	For devices used by one staff member/student only, or where only one user may have consented to having their secure traffic inspected.



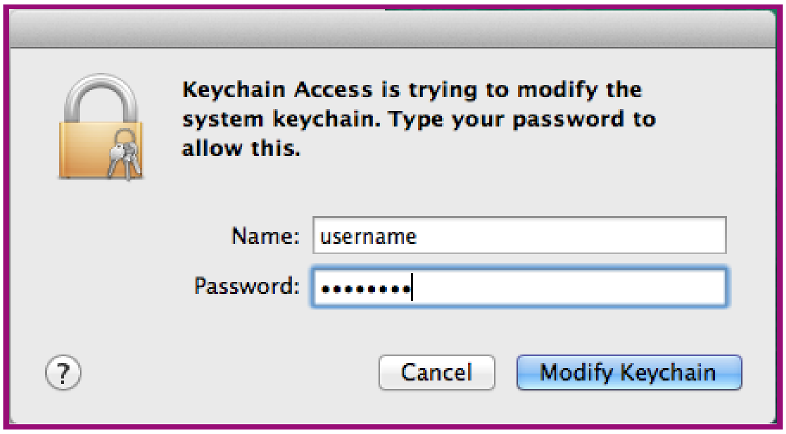
Add Certificates

Do you want to add the certificate(s) from the file "Greenwood_High_School_Jan_2014-2021.crt" to a keychain?

New root certificates should be added to the login keychain for the current user, or to the System keychain if they are to be shared by all users of this machine.

Keychain: System

1.3. Enter your credentials to allow access to the Keychain store

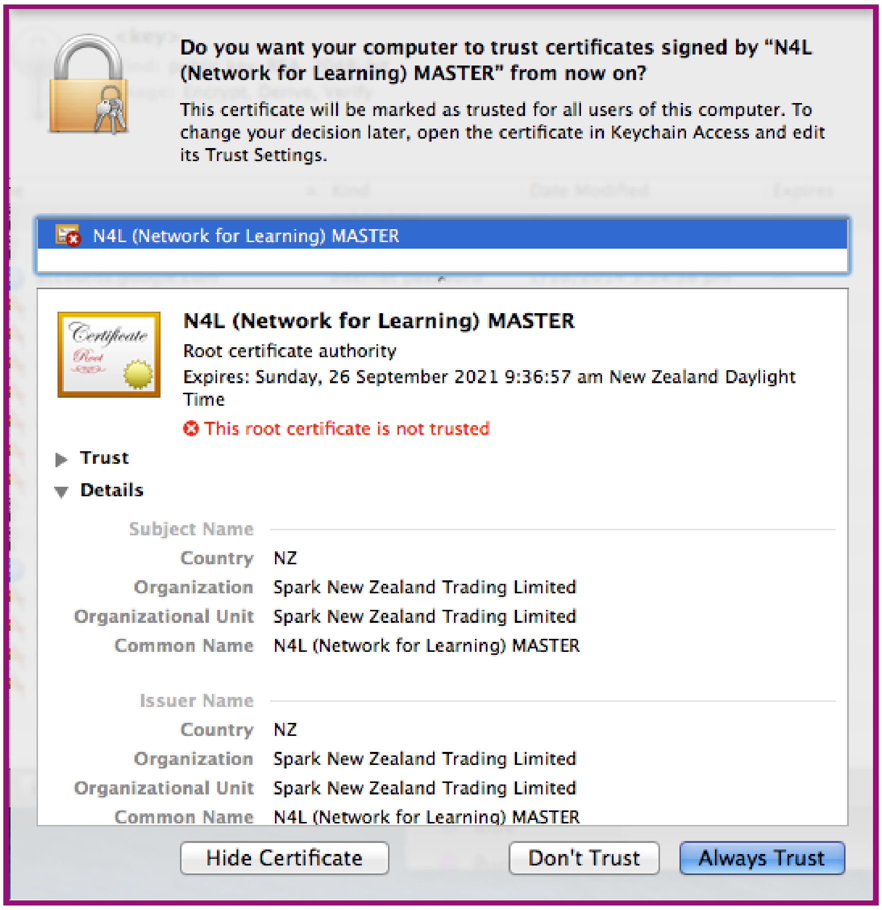


Keychain Access is trying to modify the system keychain. Type your password to allow this.

Name: username

Password: ••••••••

1.4. Check the certificate is valid, and that it is the most recent one (based on the expiry date).



Do you want your computer to trust certificates signed by "N4L (Network for Learning) MASTER" from now on?

This certificate will be marked as trusted for all users of this computer. To change your decision later, open the certificate in Keychain Access and edit its Trust Settings.

N4L (Network for Learning) MASTER

N4L (Network for Learning) MASTER

Root certificate authority

Expires: Sunday, 26 September 2021 9:36:57 am New Zealand Daylight Time

This root certificate is not trusted

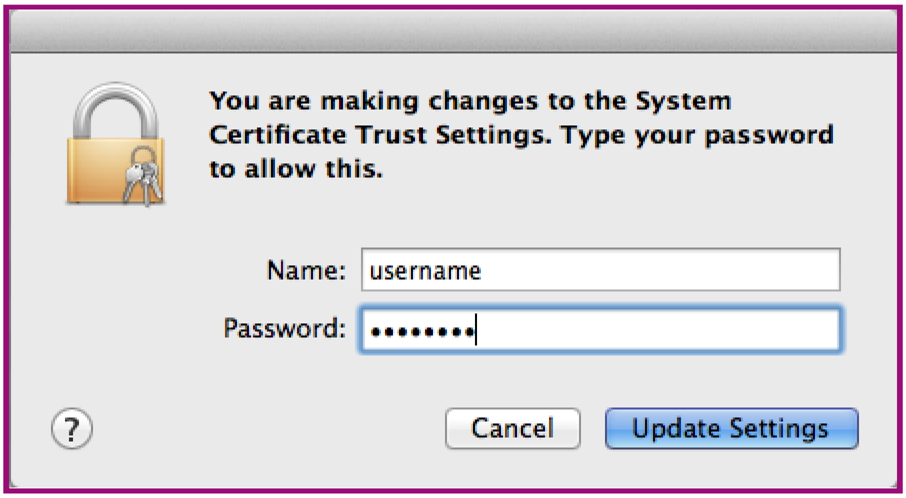
▶ Trust

▼ Details

Subject Name	
Country	NZ
Organization	Spark New Zealand Trading Limited
Organizational Unit	Spark New Zealand Trading Limited
Common Name	N4L (Network for Learning) MASTER

Issuer Name	
Country	NZ
Organization	Spark New Zealand Trading Limited
Organizational Unit	Spark New Zealand Trading Limited
Common Name	N4L (Network for Learning) MASTER

1.5. Again, you'll be asked for credentials to allow the N4L filtering certificate to be added to the System Certificate Trust Settings.

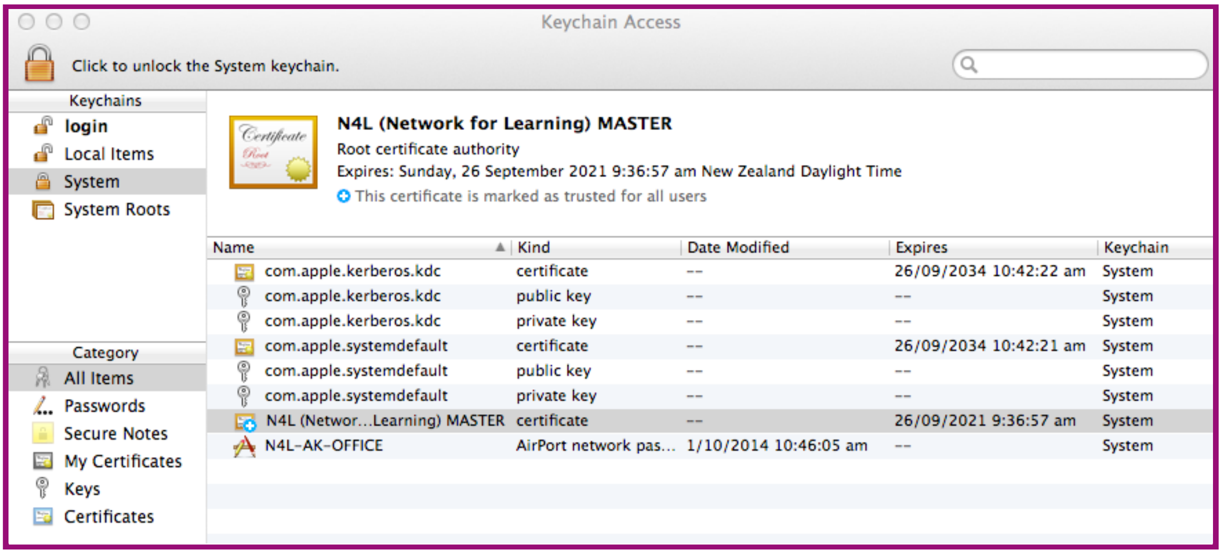


You are making changes to the System Certificate Trust Settings. Type your password to allow this.

Name: username

Password: ••••••••

1.6. You'll be able to see the certificate in the Keychain which you added it into (in this case the System Keychain), which in turn shows it's trusted by all users.



N4L (Network for Learning) MASTER
Root certificate authority
Expires: Sunday, 26 September 2021 9:36:57 am New Zealand Daylight Time
This certificate is marked as trusted for all users

Name	Kind	Date Modified	Expires	Keychain
com.apple.kerberos.kdc	certificate	--	26/09/2034 10:42:22 am	System
com.apple.kerberos.kdc	public key	--	--	System
com.apple.kerberos.kdc	private key	--	--	System
com.apple.systemdefault	certificate	--	26/09/2034 10:42:21 am	System
com.apple.systemdefault	public key	--	--	System
com.apple.systemdefault	private key	--	--	System
N4L (Networ...Learning) MASTER	certificate	--	26/09/2021 9:36:57 am	System
N4L-AK-OFFICE	AirPort network pas...	1/10/2014 10:46:05 am	--	System

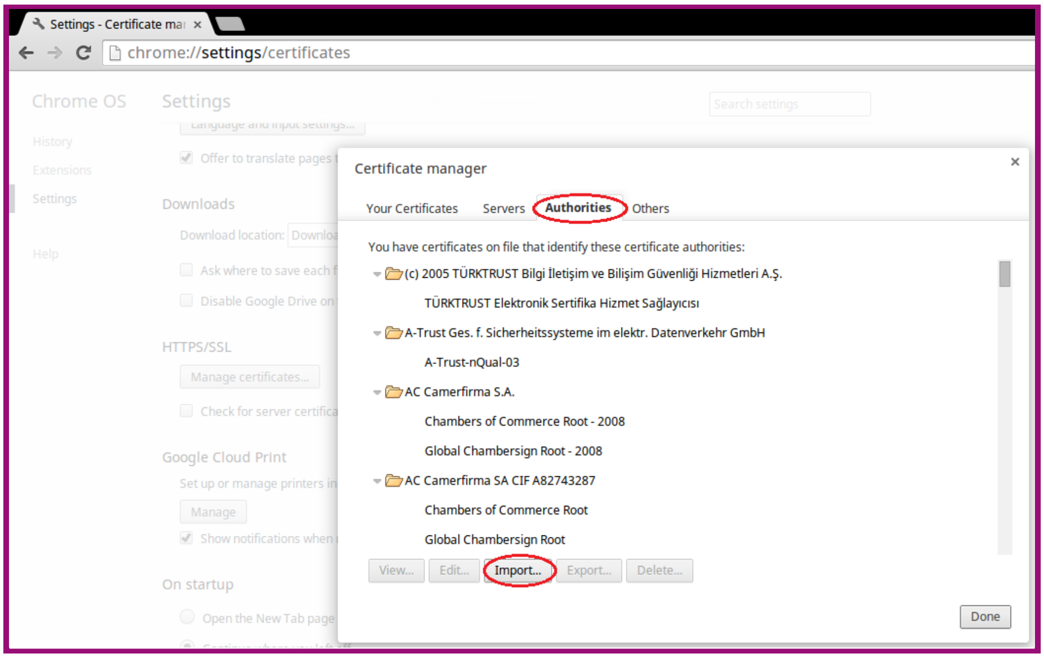
5.4.3. Manually installing certificates on Chrome OS

Installing certificates manually onto Google Chromebooks is a fairly quick task to complete.

1. Make the certificate available to the users through Email, USB stick or Intranet link

2. The user will then: Open up Chrome and go to chrome://settings/certificates to launch the certificate manager.

3. Locate the Authorities tab and click Import to begin importing the certificate created in section three of this doc.

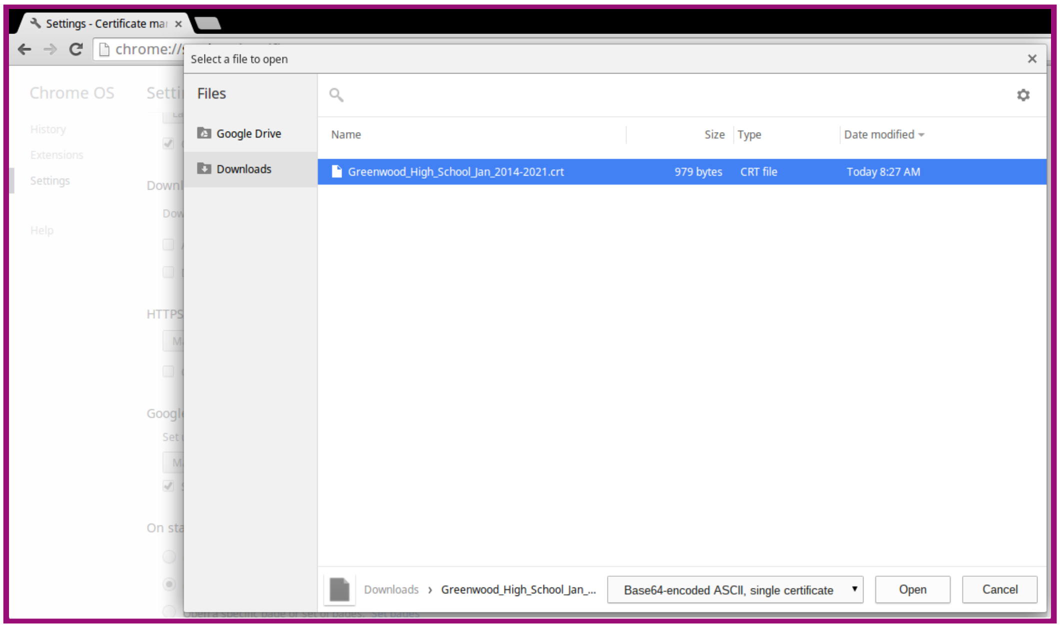


Certificate manager

You have certificates on file that identify these certificate authorities:

- (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
  - TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı
- A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
  - A-Trust-nQual-03
- AC Camerfirma S.A.
  - Chambers of Commerce Root - 2008
  - Global Chambersign Root - 2008
- AC Camerfirma SA CIF A82743287
  - Chambers of Commerce Root
  - Global Chambersign Root

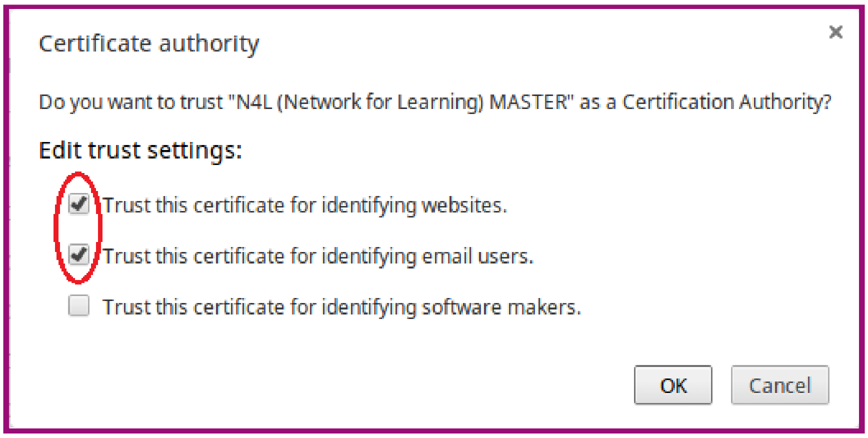
3. Locate the filtering certificate which has been disseminated.


Settings - Certificate ma
chrome://
Chrome OS
History
Extensions
Settings
Help
Files
Google Drive
Downloads
Downloads › Greenwood_High_School_Jan_...
Base64-encoded ASCII, single certificate
Open
Cancel

Select a file to open

Name	Size	Type	Date modified
Greenwood_High_School_Jan_2014-2021.crt	979 bytes	CRT file	Today 8:27 AM

4. Click trust the filtering certificate for identifying email and websites.



Certificate authority

Do you want to trust "N4L (Network for Learning) MASTER" as a Certification Authority?

Edit trust settings:

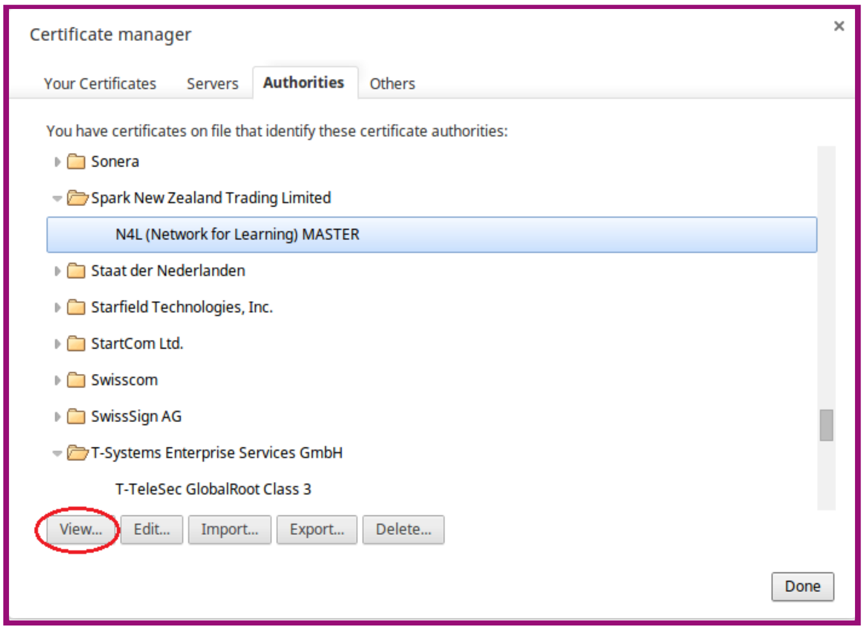
☑ Trust this certificate for identifying websites.

☑ Trust this certificate for identifying email users.

□ Trust this certificate for identifying software makers.

5. Once installed you'll be able see the filtering certificate in the list of trusted authorities.

5.1. By clicking on **View** you'll be able to see the specific details of the filtering certificate.



Certificate manager

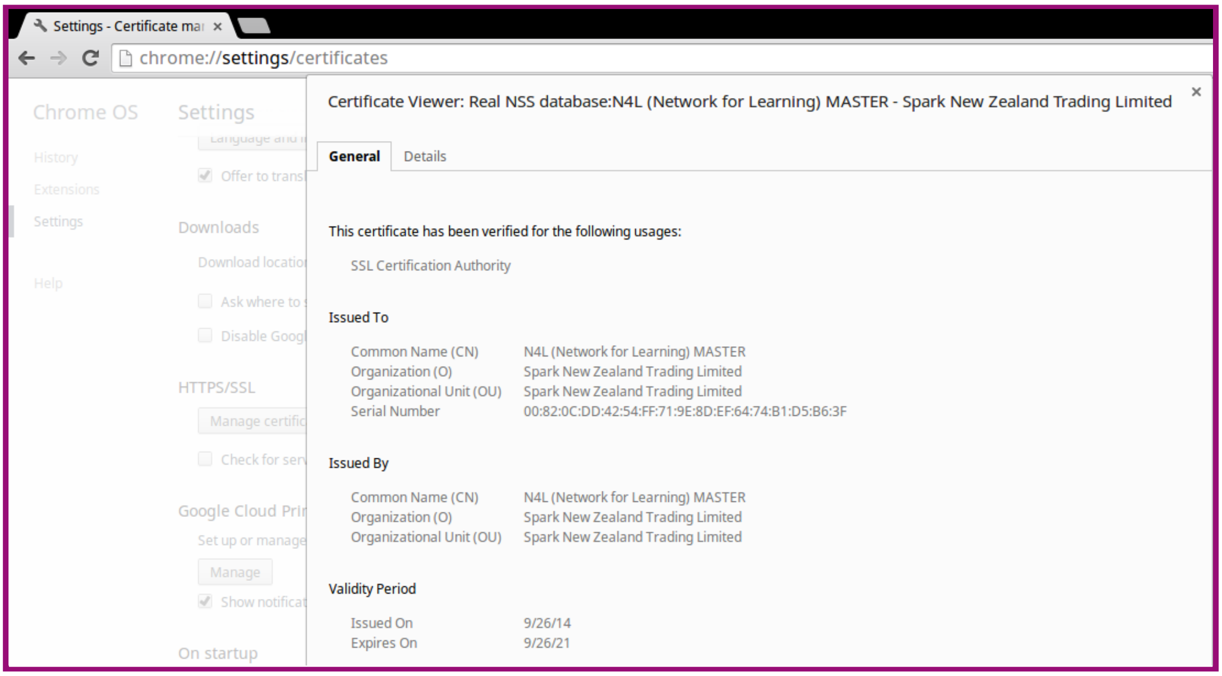
You have certificates on file that identify these certificate authorities:

- Sonera
- Spark New Zealand Trading Limited
  - N4L (Network for Learning) MASTER
- Staat der Nederlanden
- Starfield Technologies, Inc.
- StartCom Ltd.
- Swisscom
- SwissSign AG
- T-Systems Enterprise Services GmbH
  - T-TeleSec GlobalRoot Class 3

6. Here you can validate that the certificate is the correct one by:

6.1 Looking at who the certificate was issued by; and

6.2 Looking at the validity period



Certificate Viewer: Real NSS database:N4L (Network for Learning) MASTER - Spark New Zealand Trading Limited

General Details

This certificate has been verified for the following usages:

SSL Certification Authority

Issued To

Common Name (CN)	N4L (Network for Learning) MASTER
Organization (O)	Spark New Zealand Trading Limited
Organizational Unit (OU)	Spark New Zealand Trading Limited
Serial Number	00:82:0C:DD:42:54:FF:71:9E:8D:EF:64:74:B1:D5:B6:3F

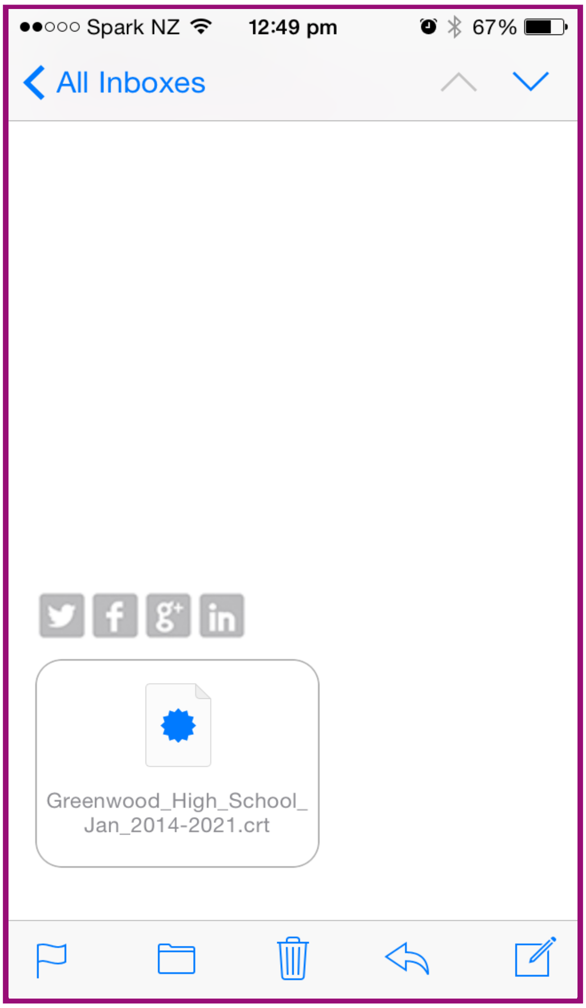
Issued By

Common Name (CN)	N4L (Network for Learning) MASTER
Organization (O)	Spark New Zealand Trading Limited
Organizational Unit (OU)	Spark New Zealand Trading Limited

Validity Period

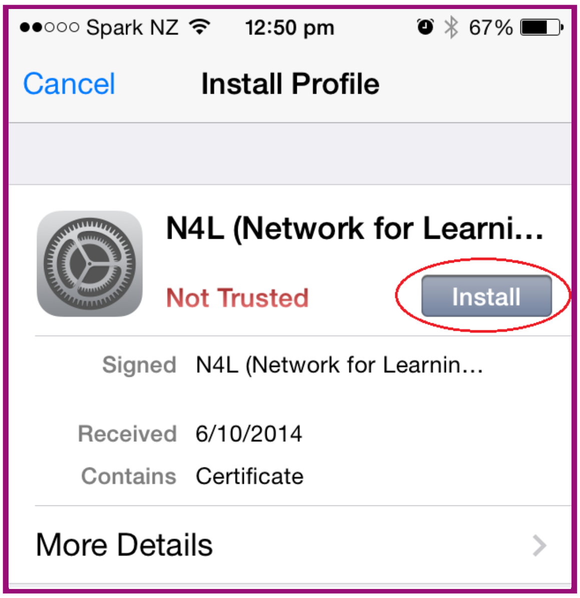
Issued On	9/26/14
Expires On	9/26/21

5.4.4. Manually installing certification on iOS



If you do not have access to an Mobile Device Management (MDM) platform another way to distribute the filtering security certificate to iOS devices is via email.

1. Open the attached filtering certificate to begin the setup wizard



●●○○○ Spark NZ 12:50 pm 67%

Cancel Install Profile

N4L (Network for Learni…

Not Trusted Install

Signed N4L (Network for Learnin…

Received 6/10/2014

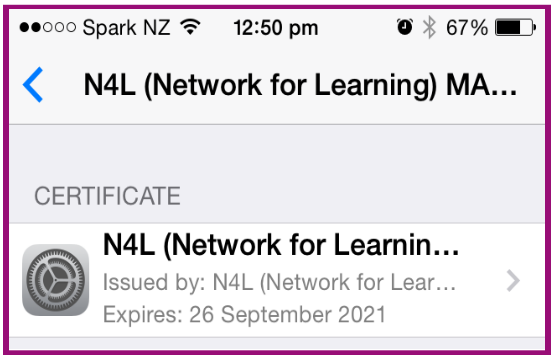
Contains Certificate

More Details

2. Here you are advised of who has signed the filtering certificate and the details can be checked before installing the certificate as needed.

3. Click on **Install,** and

4. Enter your password to confirm you accept installing the filtering certificate on the device.



●●○○○ Spark NZ 12:50 pm 67%

N4L (Network for Learning) MA…

CERTIFICATE

N4L (Network for Learnin…

Issued by: N4L (Network for Lear…

Expires: 26 September 2021

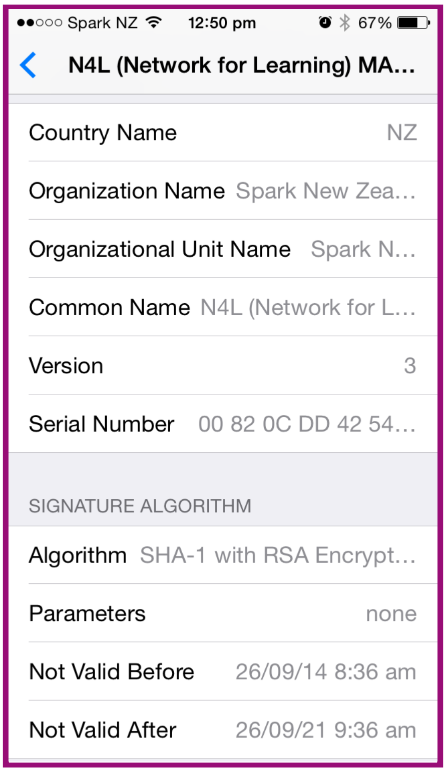
5. Here you validate that the certificate is the correct by:

5.1. Clicking on 'more details'

5.2. Click on the certificate.

5.3. Look at who the certificate was issued by

5.4. Look at the validity period



●●○○○ Spark NZ 12:50 pm 67%

N4L (Network for Learning) MA…

Country Name NZ

Organization Name Spark New Zea…

Organizational Unit Name Spark N…

Common Name N4L (Network for L…

Version 3

Serial Number 00 82 0C DD 42 54…

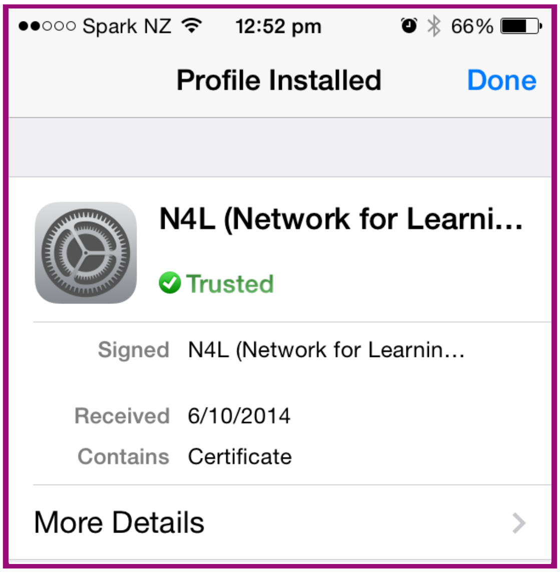
SIGNATURE ALGORITHM

Algorithm SHA-1 with RSA Encrypt…

Parameters none

Not Valid Before 26/09/14 8:36 am

Not Valid After 26/09/21 9:36 am



●●○○○ Spark NZ 12:52 pm 66%

Profile Installed Done

N4L (Network for Learni…

✓ Trusted

Signed N4L (Network for Learnin…

Received 6/10/2014

Contains Certificate

More Details >

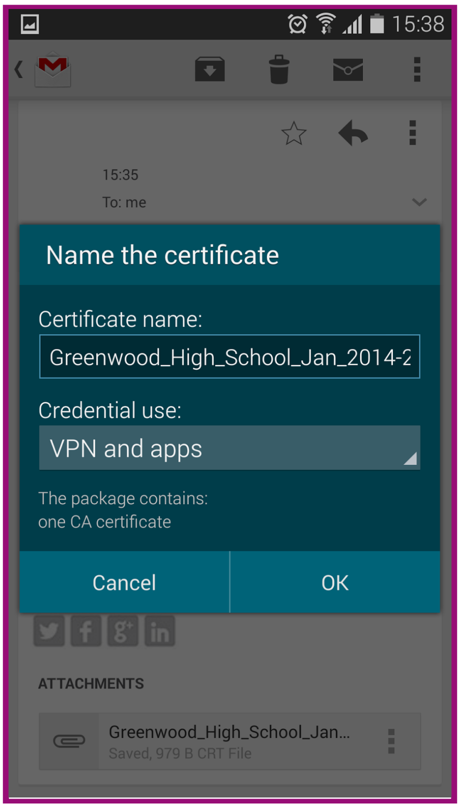
6. After the filtering certificate has been successfully installed you'll see the certificate now listed as 'Trusted'

5.4.5. Manually installing certification on Android

If you do not have access to an Mobile Device Management (MDM) platform another way to distribute the filtering security certificate to Android devices is via email.

1. The filtering certificate can either be:

- Emailed to all users; or
- The user may email the certificate found on a common file share to themselves for installation.



15:38

15:35

To: me

Name the certificate

Certificate name:

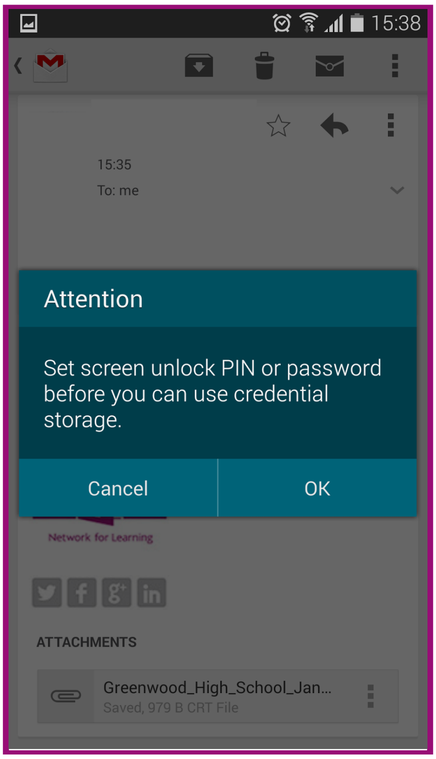
Greenwood_High_School_Jan_2014-2

Credential use:

VPN and apps

The package contains:
one CA certificate

In the example to the left the certificate has been received in the email client and the attachment has been opened to begin the certificate installation process.



15:38

15:35

To: me

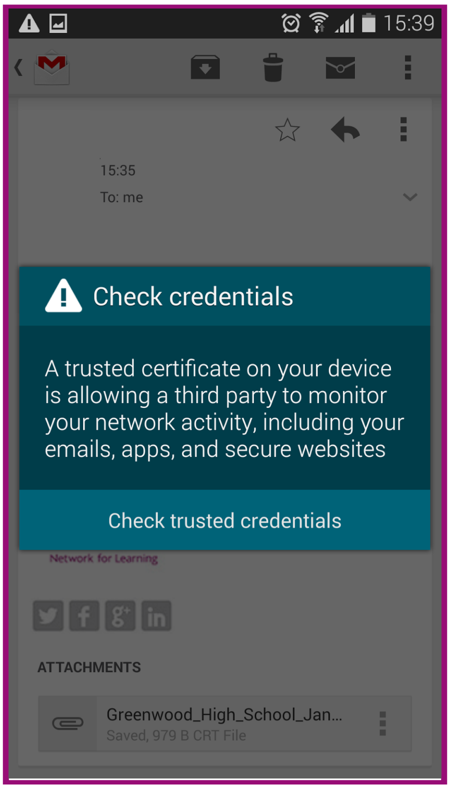
Attention

Set screen unlock PIN or password before you can use credential storage.

2. Depending on the lock screen security settings on the Android device you may be prompted to change your lock screen method to use a pin code or a password.

Swipe or Pattern locking methods are not considered secure enough for the Android credential store and are thus not supported.

Research has shown that some workarounds are available for various versions of Android but the use of such workarounds is not recommended.



15:39

15:35

To: me

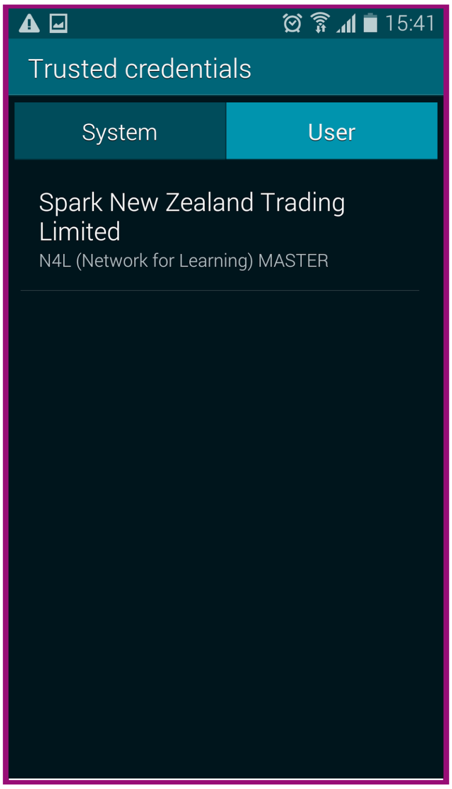
Check credentials

A trusted certificate on your device is allowing a third party to monitor your network activity, including your emails, apps, and secure websites

Greenwood_High_School_Jan...
Saved, 979 B CRT File

3. After meeting the lockscreen password complexity requirements you will be warned that installing a security certificate onto your device may allow a 3rd party to monitor network traffic.

This 3rd party being referenced to is the N4L filtering platform - it is required to monitor and filter secure network content and to facilitate any future user level filtering capabilities.

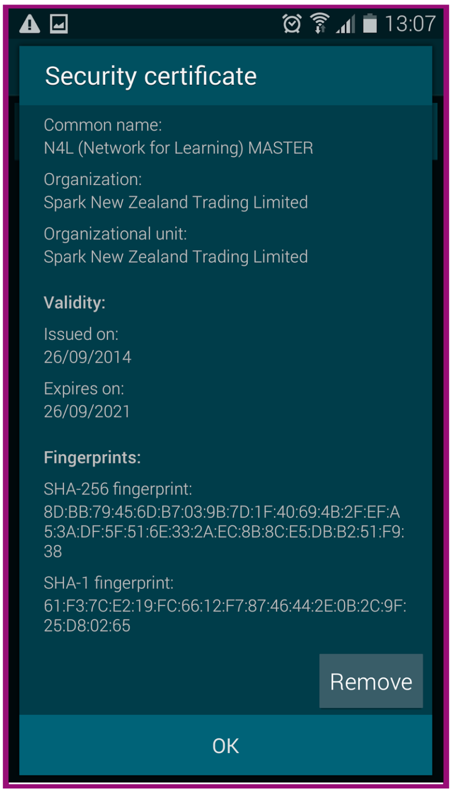


15:41

Trusted credentials

Spark New Zealand Trading Limited
N4L (Network for Learning) MASTER

4. When prompted to check the trusted credentials ensure that the certificate installed is the correct one for your school as created in the self-service filtering dashboard or provided to you by N4L as shown in the example to the left.



Security certificate

Common name:
N4L (Network for Learning) MASTER

Organization:
Spark New Zealand Trading Limited

Organizational unit:
Spark New Zealand Trading Limited

Validity:

Issued on:
26/09/2014

Expires on:
26/09/2021

Fingerprints:

SHA-256 fingerprint:
8D:BB:79:45:6D:B7:03:9B:7D:1F:40:69:4B:2F:EF:A5:3A:DF:5F:51:6E:33:2A:EC:8B:8C:E5:DB:B2:51:F9:38

SHA-1 fingerprint:
61:F3:7C:E2:19:FC:66:12:F7:87:46:44:2E:0B:2C:9F:25:D8:02:65

5. By viewing the full certificate details we can verify that the certificate is not only the correct one for your school, but also the current one based on the issued and expiry date.

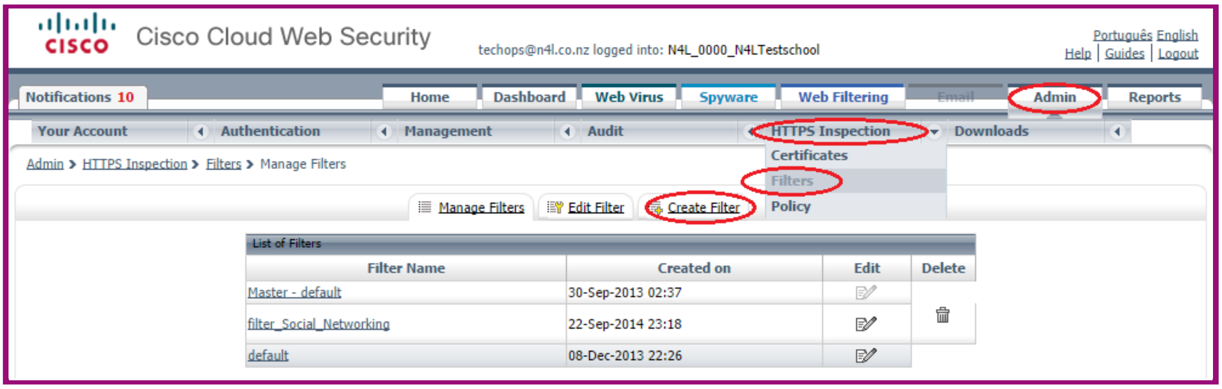
5.5. Implementing Secure Website Inspection

Please ensure you have completed all the basic web filtering training that is available on the N4L website, or have sufficient web filtering experience, prior to following these instructions.

5.5.1. Secure Website Inspection Filters

Secure Website Inspection filters are grouped separately within the Web Filtering Dashboard and can be found by:

1. Clicking on **Admin**
2. Choosing **Filters** from the **HTTPS Inspection** drop-down menu



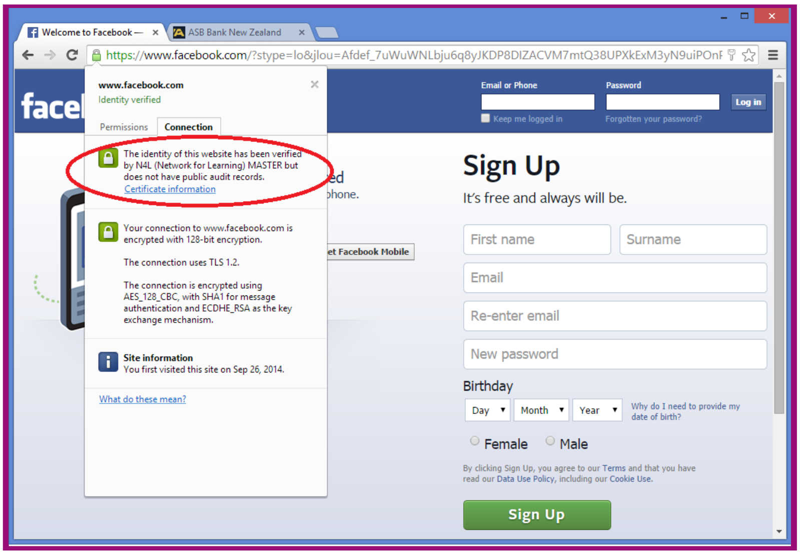
List of Filters

Filter Name	Created on	Edit	Delete
Master - default	30-Sep-2013 02:37		
filter_Social_Networking	22-Sep-2014 23:18		
default	08-Dec-2013 22:26		

Note: Secure Website Inspection filters and policy function differently to Web Filtering filters and policy.

Secure Website Inspection filters determine whether the filtering security certificate created earlier is **presented** to the user for the chosen categories, domains and applications, this is what allows CCWS to view the content of secure websites. Web Filtering filters and rules must be created separately to take filtering actions such as allow, block, anonymize, warn or authenticate.

In the example below we have chosen to enable Secure Website Inspection for Facebook, and this can be verified by looking at the certificate information.


Welcome to Facebook —
ASB Bank New Zealand
https://www.facebook.com/?stype=lo&jlou=Afdef_7uWuWNLbju6q8yJKDP8DIZACVM7mtQ38UPXkExM3yN9uiPOnF
Email or Phone
Password
Log in
Keep me logged in
Forgotten your password?
Permissions
Connection
et Facebook Mobile
Sign Up
It's free and always will be.
First name
Surname
Email
Re-enter email
New password
Birthday
Day
Month
Year
Why do I need to provide my date of birth?
Female
Male
By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.
Sign Up

www.facebook.com
Identity verified

The identity of this website has been verified by N4L (Network for Learning) MASTER but does not have public audit records.
Certificate information

Your connection to www.facebook.com is encrypted with 128-bit encryption.

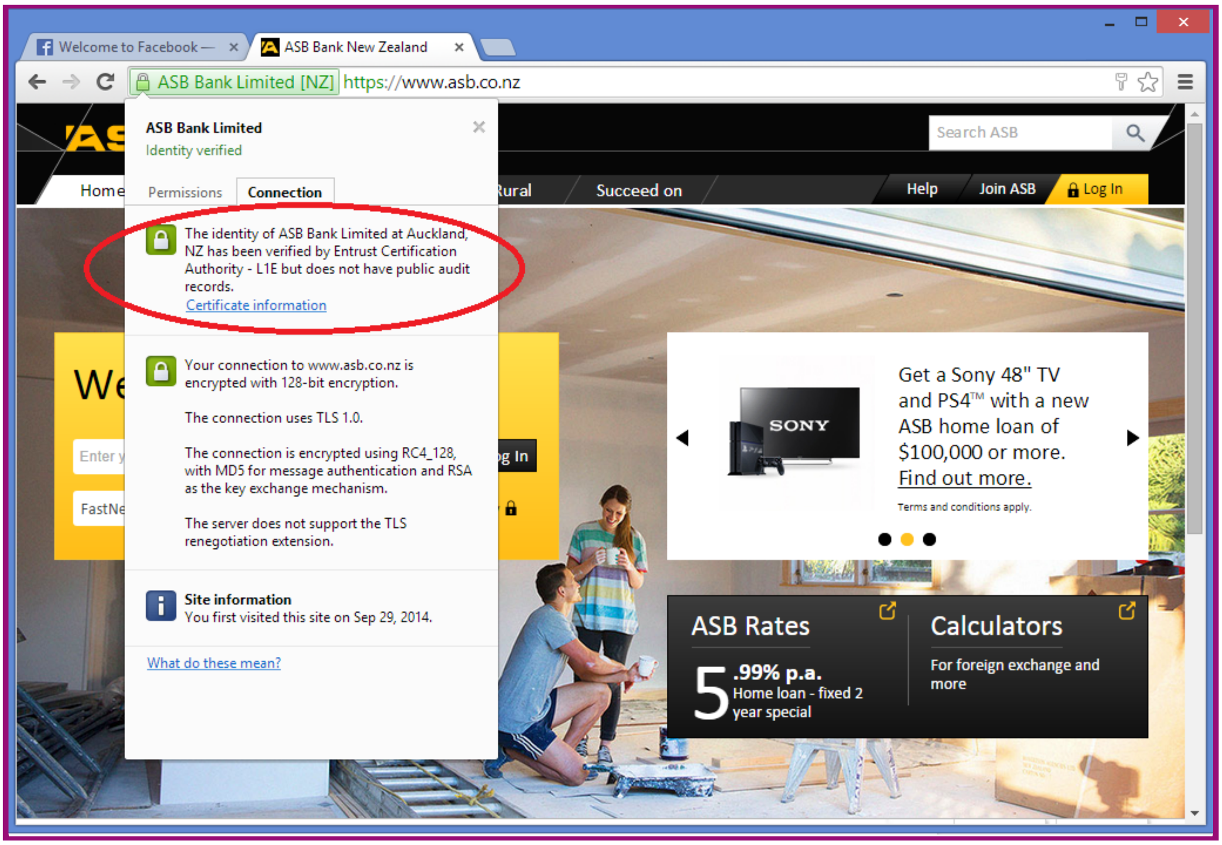
The connection uses TLS 1.2.

The connection is encrypted using AES_128_CBC, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.

Site information
You first visited this site on Sep 26, 2014.

What do these mean?

Similarly in this next example we have chosen **not** to inspect the secure website https://www.asb.co.nz for obvious reasons. It is your responsibility to ensure you have sufficient authorisation to inspect your users web traffic at your School.



The identity of ASB Bank Limited at Auckland, NZ has been verified by Entrust Certification Authority - L1E but does not have public audit records.

Your connection to www.asb.co.nz is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using RC4_128, with MD5 for message authentication and RSA as the key exchange mechanism.

The server does not support the TLS renegotiation extension.

You first visited this site on Sep 29, 2014.

5.5.2. Creating Secure Website Inspection filters

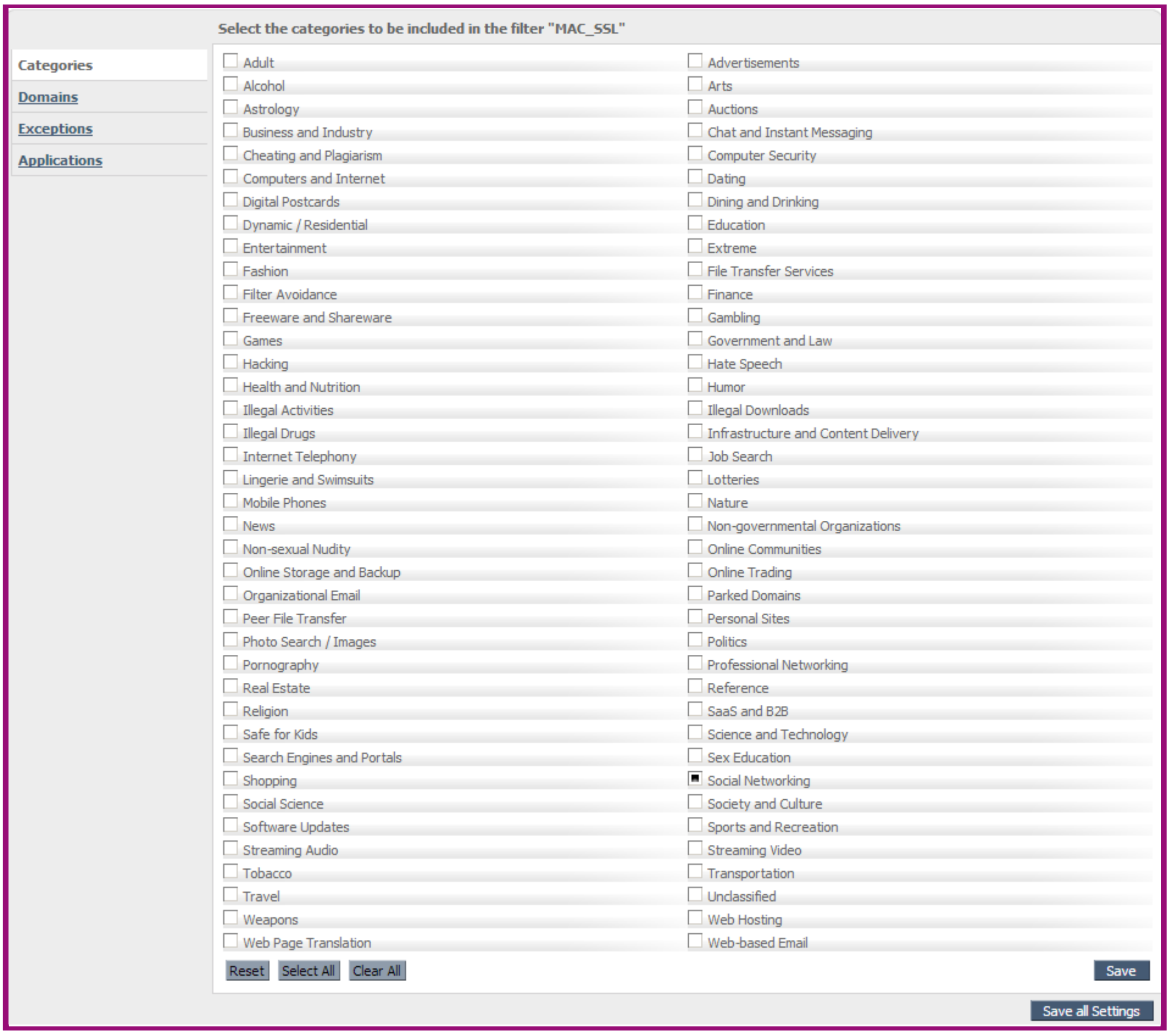
1. Click on **Admin**
2. Choose **Filters** from the **HTTPS Inspection** dropdown menu
3. Click on the **Create Filter** tab
4. Select the categories (as seen below) that HTTPS inspection will be applied to.

Note: Any sites covered by any of the selected categories will require the inspection certificate to be installed correctly to access the site/service without the browser detecting a untrusted connection.

The example below shows that only sites in the **Social Networking** category will be inspected, however in reality you would most likely have a number of categories filtered. It is also advisable to <u>not</u> enable HTTPS inspection for categories such as Government and Law, Online Shopping, Online Trading or Lotteries etc where highly sensitive information may be exchanged.

- Create more filters for every additional category; or
- Create a single filter covering multiple categories

Note: HTTPS sites for other globally blocked categories (e.g. the "Pornography' category) are automatically blocked.

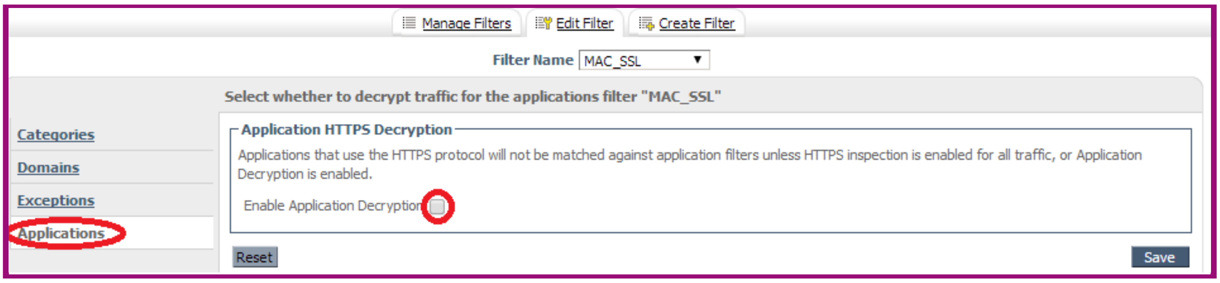


Select the categories to be included in the filter "MAC_SSL"

Categories
Domains
Exceptions
Applications

- □ Adult
- □ Alcohol
- □ Astrology
- □ Business and Industry
- □ Cheating and Plagiarism
- □ Computers and Internet
- □ Digital Postcards
- □ Dynamic / Residential
- □ Entertainment
- □ Fashion
- □ Filter Avoidance
- □ Freeware and Shareware
- □ Games
- □ Hacking
- □ Health and Nutrition
- □ Illegal Activities
- □ Illegal Drugs
- □ Internet Telephony
- □ Lingerie and Swimsuits
- □ Mobile Phones
- □ News
- □ Non-sexual Nudity
- □ Online Storage and Backup
- □ Organizational Email
- □ Peer File Transfer
- □ Photo Search / Images
- □ Pornography
- □ Real Estate
- □ Religion
- □ Safe for Kids
- □ Search Engines and Portals
- □ Shopping
- □ Social Science
- □ Software Updates
- □ Streaming Audio
- □ Tobacco
- □ Travel
- □ Weapons
- □ Web Page Translation
- □ Advertisements
- □ Arts
- □ Auctions
- □ Chat and Instant Messaging
- □ Computer Security
- □ Dating
- □ Dining and Drinking
- □ Education
- □ Extreme
- □ File Transfer Services
- □ Finance
- □ Gambling
- □ Government and Law
- □ Hate Speech
- □ Humor
- □ Illegal Downloads
- □ Infrastructure and Content Delivery
- □ Job Search
- □ Lotteries
- □ Nature
- □ Non-governmental Organizations
- □ Online Communities
- □ Online Trading
- □ Parked Domains
- □ Personal Sites
- □ Politics
- □ Professional Networking
- □ Reference
- □ SaaS and B2B
- □ Science and Technology
- □ Sex Education
- ■ Social Networking
- □ Society and Culture
- □ Sports and Recreation
- □ Streaming Video
- □ Transportation
- □ Unclassified
- □ Web Hosting
- □ Web-based Email

5. If required, domains or IP ranges can be added to the Secure Website Inspection filter using the **Domains** links.
6. If needed, specific Domains or IP ranges can also be excluded from Secure Website Inspection within a category by adding these to the **Exception** fields (e.g. this could be used to inspect all social networking sites with the exception of Yammer).
7. You can also force web and mobile applications to use the certificate by checking the **Enable Application Decryption** box using the **Applications** link. This allows very granular levels of Web filtering such as blocking Facebook games but allowing Facebook messaging, or allowing viewing YouTube but preventing video's from being uploaded.



Filter Name MAC_SSL

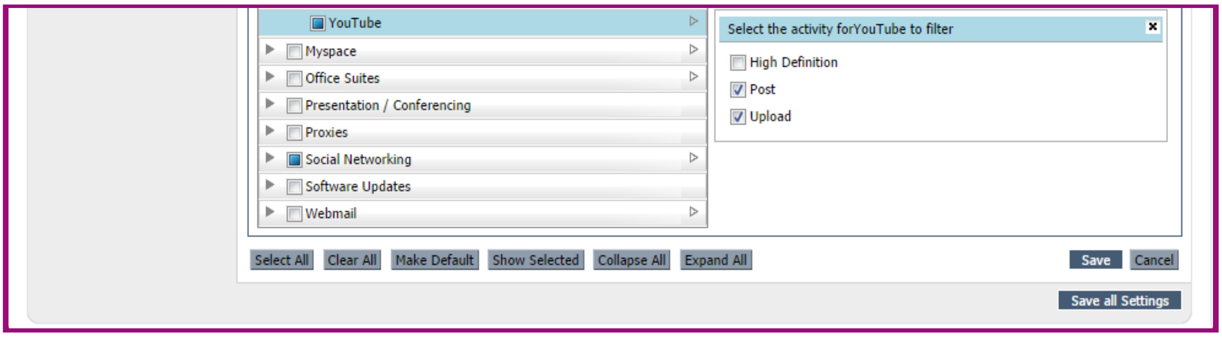
Select whether to decrypt traffic for the applications filter "MAC_SSL"

Application HTTPS Decryption

Applications that use the HTTPS protocol will not be matched against application filters unless HTTPS inspection is enabled for all traffic, or Application Decryption is enabled.

Enable Application Decryption □

8. Click **Save all Settings** and proceed to create appropriate application based filters under the Web Filtering section of the Web Filtering Dashboard.



■ YouTube

□ Myspace

□ Office Suites

□ Presentation / Conferencing

□ Proxies

■ Social Networking

□ Software Updates

□ Webmail

Select the activity forYouTube to filter

□ High Definition

☑ Post

☑ Upload

Note: If you have not yet completed them, training videos on how to create filters and policy in the N4L Web Filtering dashboard can be found on the N4L website.

5.5.3. Creating a new Secure Website Inspection Rule

To inspect secure traffic based on a previously created filter:

1. Click on Create Rule

2. Provide a Name for your rule

3. Select the correct certificate we created earlier for your school from the dropdown list (see next page). This step is especially important as if you do not select the certificate to be installed on end user devices, users will receive HTTPS security error messages in their browsers informing them of an untrusted intermediary potentially inspecting their traffic.

4. Define your Group

   4.1. Choose a group created earlier from the drop-down list or select none to apply to all users.

   4.2. Click on Add

5. Define your Filter by ensuring you choose the relevant Secure Website Inspection filter created for your school beforehand from the pull-down list

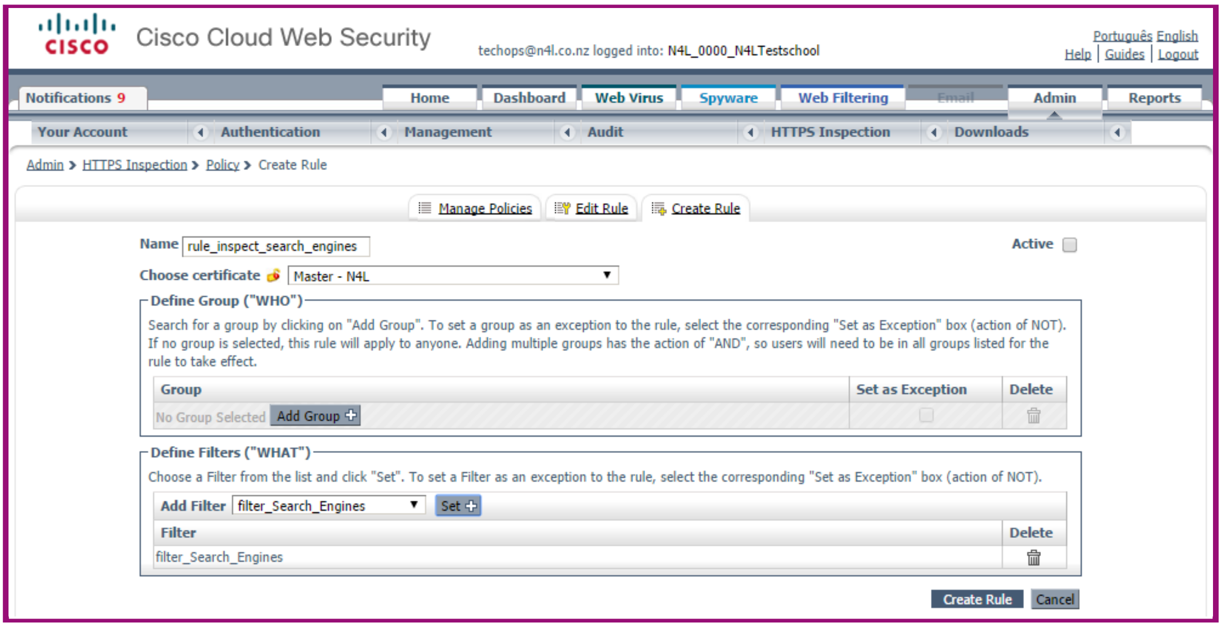
   5.1. Click on Add

Note: You can add multiple filters to a single rule as required.

6. Click Create Rule to save

7. Remember to mark the rule as Active to enable it, should you wish to do this at this stage.

8. Once the rule is defined it should be moved to the relevant position in the policy list and enabled if you haven't done so already. It may take several minutes for changes to take effect.



Name: rule_inspect_search_engines

Active □

Choose certificate: Master - N4L

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "AND", so users will need to be in all groups listed for the rule to take effect.

Group	Set as Exception	Delete
No Group Selected Add Group	□	🗑

Define Filters ("WHAT")

Choose a Filter from the list and click "Set". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter: filter_Search_Engines Set

Filter	Delete
filter_Search_Engines	🗑

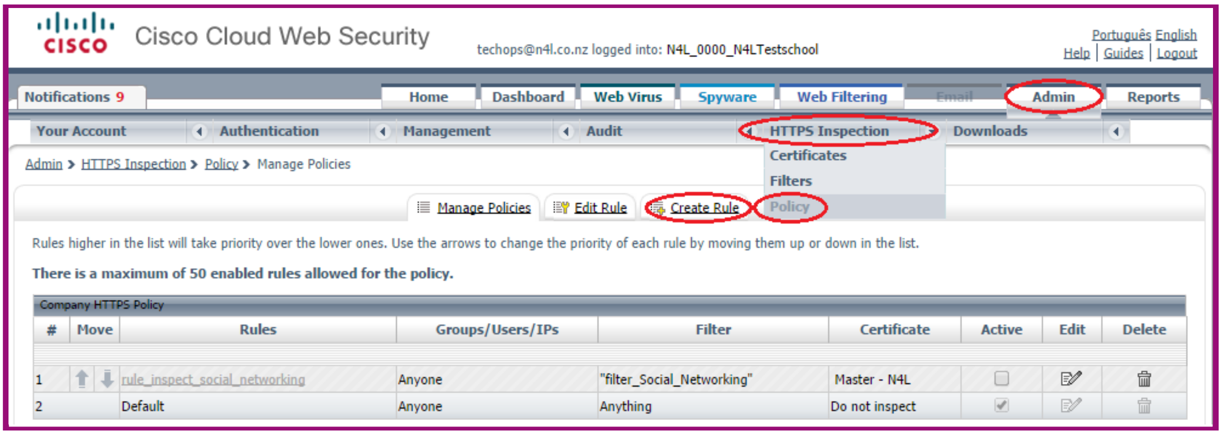
5.5.4. Secure Website Inspection Policy

Secure Website Inspection policy consists of rules which reference one or more filters each.

To view these rules within the N4L Web Filtering dashboard:

1. Click on **Admin**
2. Choose **Policy** from the **HTTPS Inspection** drop-down menu.

From here you can manage and easily create additional rules as required to build up your Secure Website Inspection policy. In many cases a single rule will suffice, however additional rules can provide greater flexibility and aid any troubleshooting.



Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.

There is a maximum of 50 enabled rules allowed for the policy.

Company HTTPS Policy

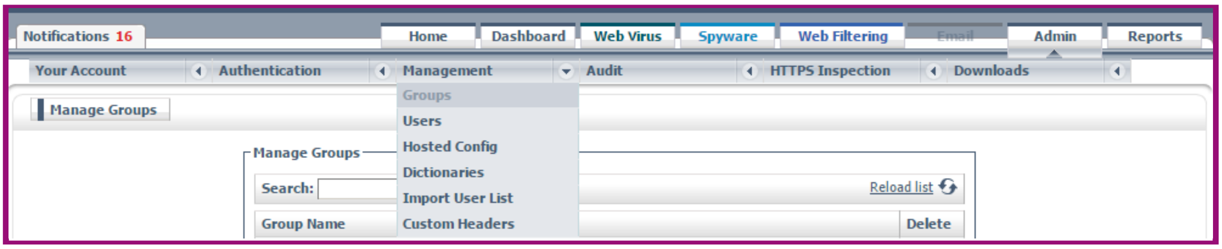
#	Move	Rules	Groups/Users/IPs	Filter	Certificate	Active	Edit	Delete
1	↑ ↓	rule_inspect_social_networking	Anyone	"filter_Social_Networking"	Master - N4L	□	✎	🗑
2		Default	Anyone	Anything	Do not inspect	☑	✎	🗑

5.5.5. Inspection Groups

As with Web Filtering filters, your filtering action can be applied to subset of your users by segmenting your schools local area network. For example filtering rules could be customised to provide different levels of filtering for Teachers, Students, Guests or servers by creating an appropriate IP Groups which are referenced within the filtering dashboard. **Directory based groups are not supported in Secure Website Inspection policy**. Directory based groups are supported within Web Filtering Policy.

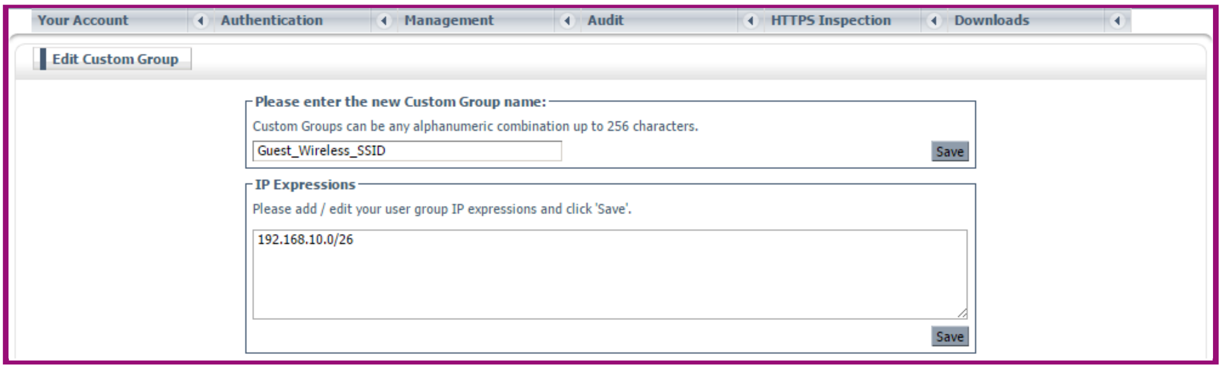
Inspection groups can be created by:

1. Clicking on **Admin**
2. Choosing **Groups** from the **Management** dropdown menu



3. Click **Add Custom Group**

4. Provide a name for the group to be identified by
5. Click **Edit** to configure the newly created custom group
6. Enter your LAN IP address range for the group accordingly and click **Save**



Please enter the new Custom Group name:

Custom Groups can be any alphanumeric combination up to 256 characters.

Guest_Wireless_SSID

IP Expressions

Please add / edit your user group IP expressions and click 'Save'.

192.168.10.0/26

5.6. Browsing with Secure Website Inspection enabled

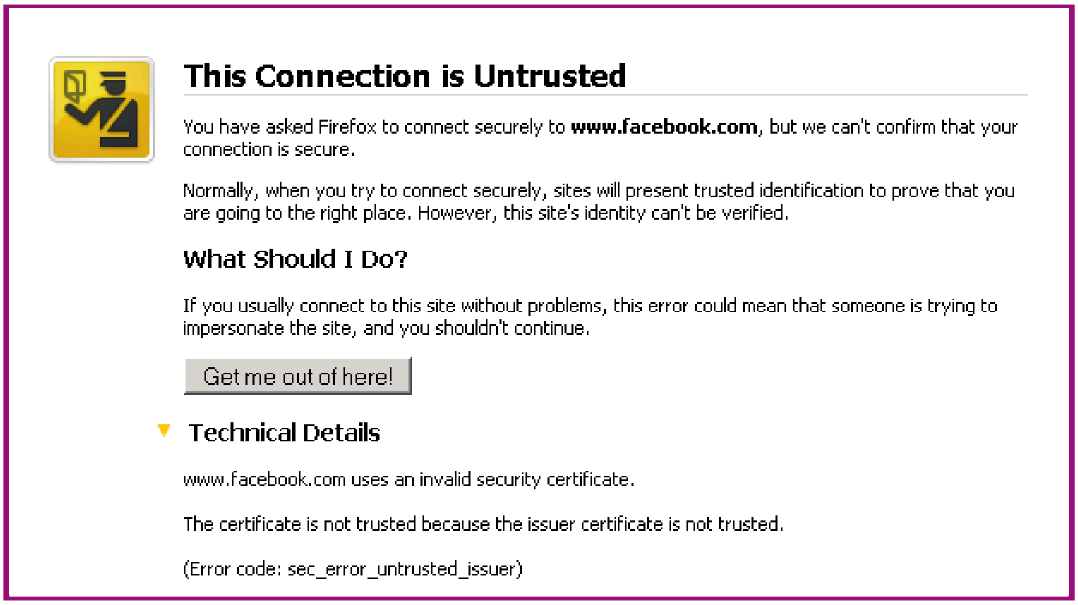
If an attempt to browse is made to a site subject to Secure Website Inspection, and no valid inspection certificate has been installed then the browser will return an HTTPS certificate warning message.

Different browsers will return different messages.

Once the security certificate is installed the browser will trust the secure connection to the filtering platform and the requested content will be displayed without any warnings - unless there is a rule to block it, in which case a familiar "N4L Blocked Site" message will be displayed.

Below are several examples of error messages presented by different browsers when Secure Website Inspection has been enabled and the inspection certificate has **not** been installed,

Firefox – browsing to https://www.facebook.com



This Connection is Untrusted

You have asked Firefox to connect securely to **www.facebook.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

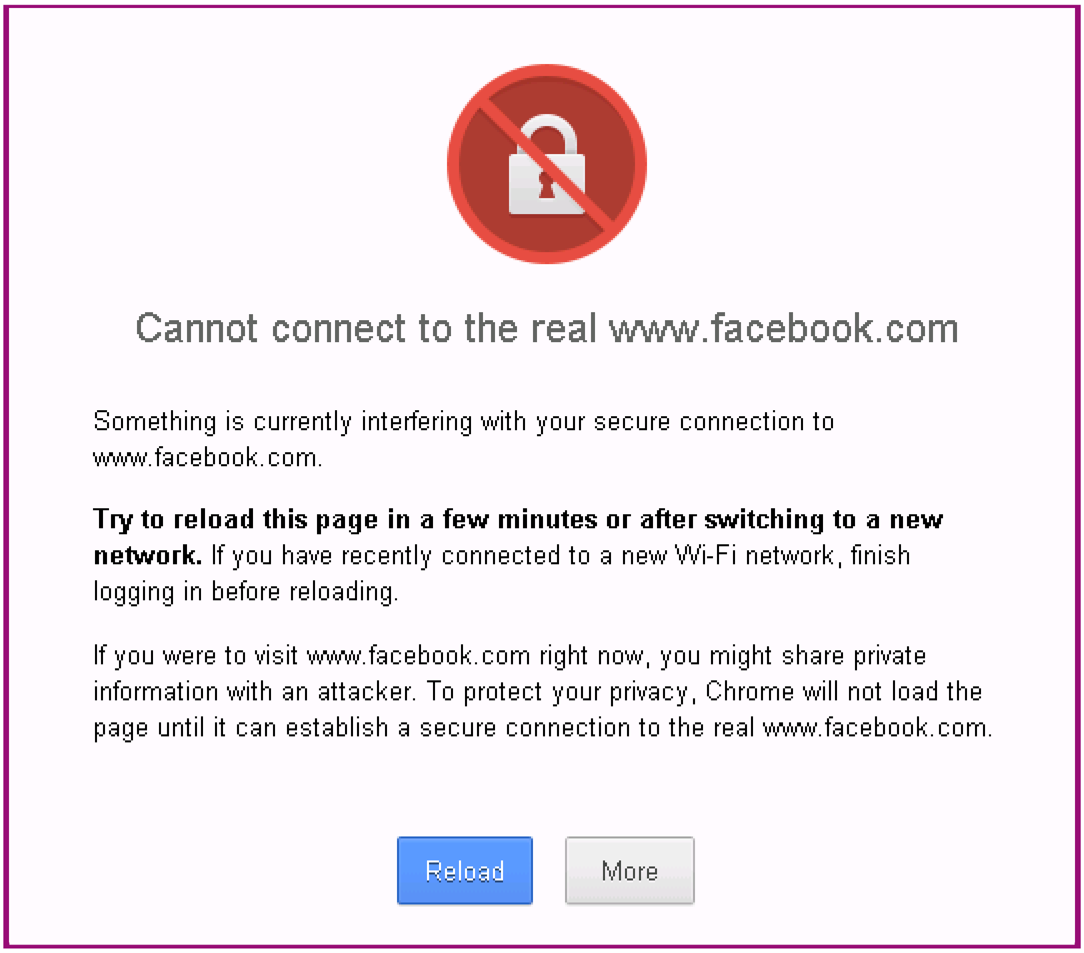
▼ Technical Details

www.facebook.com uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is not trusted.

(Error code: sec_error_untrusted_issuer)

Chrome – browsing to https://www.facebook.com



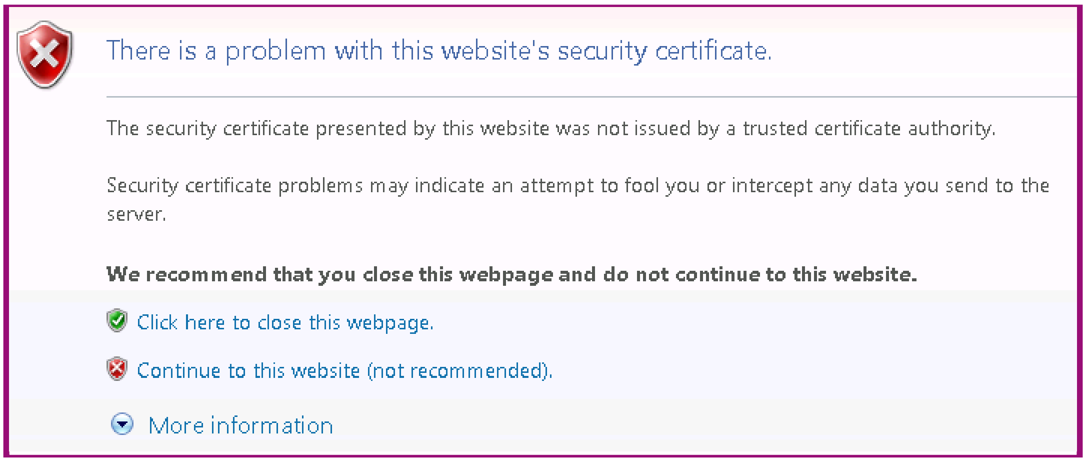
Cannot connect to the real www.facebook.com

Something is currently interfering with your secure connection to www.facebook.com.

Try to reload this page in a few minutes or after switching to a new network. If you have recently connected to a new Wi-Fi network, finish logging in before reloading.

If you were to visit www.facebook.com right now, you might share private information with an attacker. To protect your privacy, Chrome will not load the page until it can establish a secure connection to the real www.facebook.com.

Internet Explorer – browsing to https://www.facebook.com



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

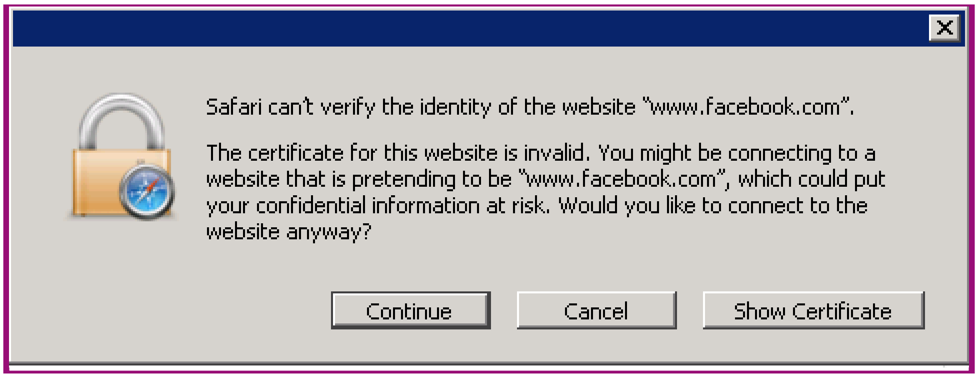
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

Clicking on “Continue to this website (not recommended)” will cause this message to continue to be displayed.

Safari (Windows) – browsing to https://www.facebook.com

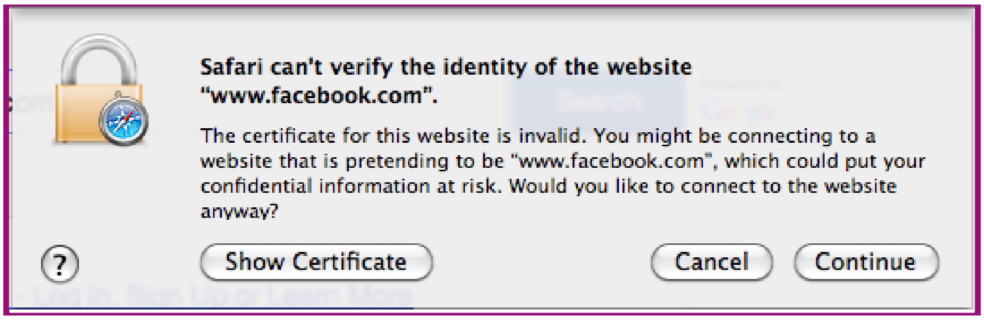


Safari can't verify the identity of the website "www.facebook.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "www.facebook.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

Safari (Windows) will allow the user to override the warning and continue to the page. All Scansafe filtering rules will still be correctly applied, however overriding security warnings should always be avoided.

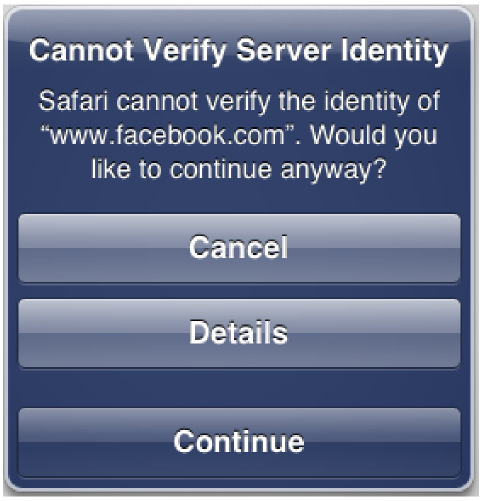
Safari (OSX) – browsing to https://www.facebook.com



Safari can't verify the identity of the website "www.facebook.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "www.facebook.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

Safari (iOS) – browsing to https://www.facebook.com

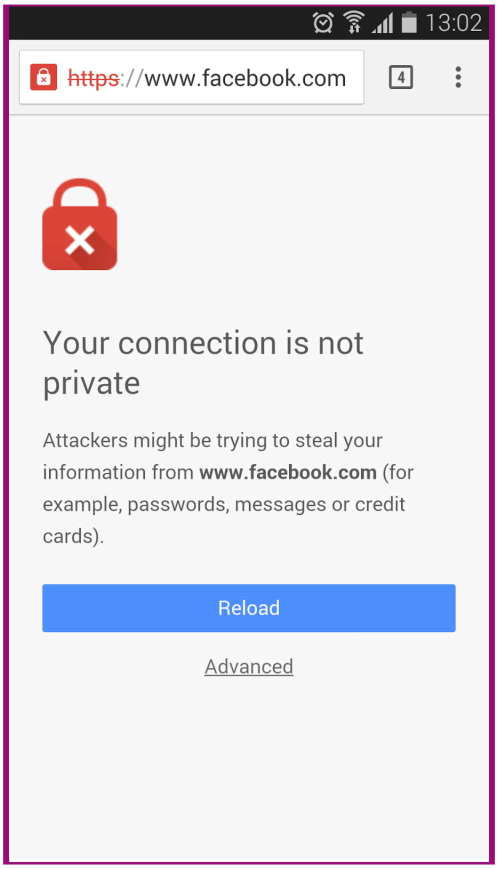


Cannot Verify Server Identity

Safari cannot verify the identity of "www.facebook.com". Would you like to continue anyway?

Unlike with Windows, both the OSX and iOS versions will not allow you to proceed to the web page by pressing "Continue". The inspection certificate must be installed first.

Chrome (Android 4.4.2) - Browsing to https://www.facebook.com

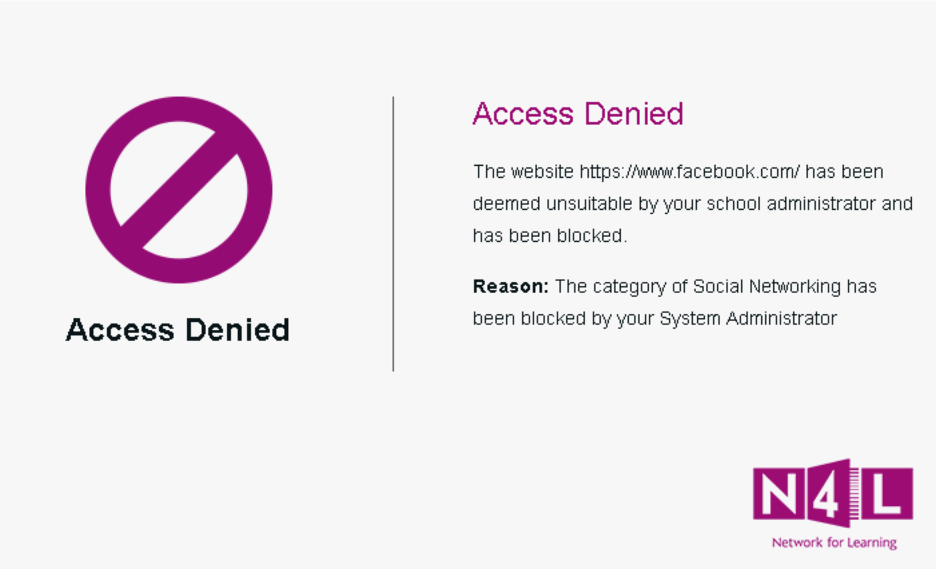


Your connection is not private

Attackers might be trying to steal your information from **www.facebook.com** (for example, passwords, messages or credit cards).

For any browsers:

Once the inspection certificate is installed, and if the user is not permitted to reach for example https://www.facebook.com due to Web Filtering rules then the appropriate "N4L Access Denied" message is displayed.

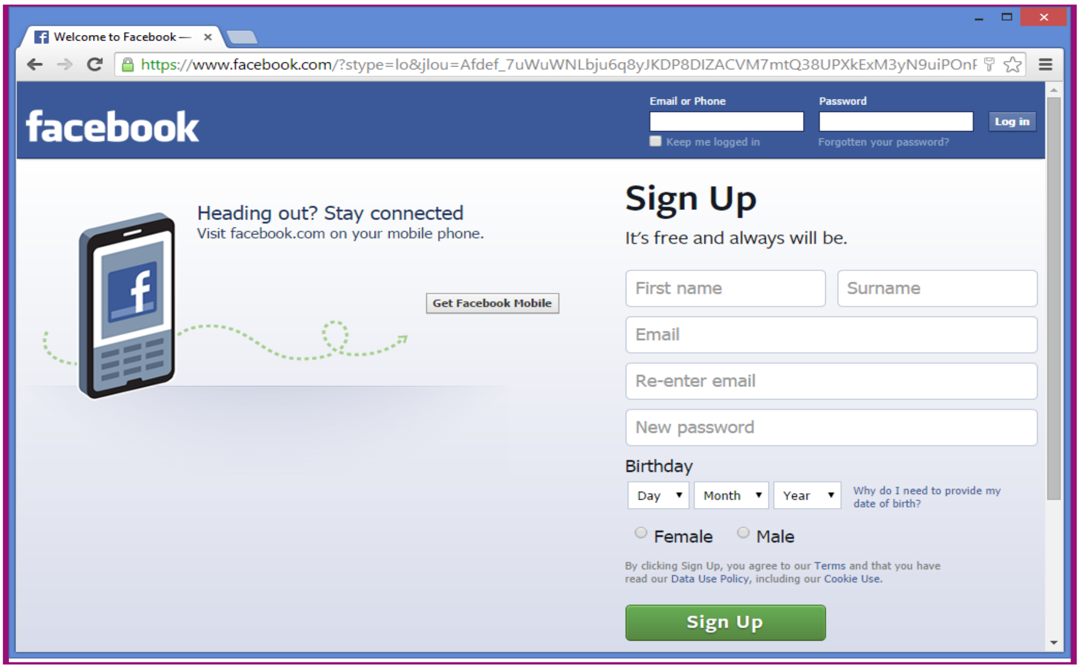


Access Denied

The website https://www.facebook.com/ has been deemed unsuitable by your school administrator and has been blocked.

Reason: The category of Social Networking has been blocked by your System Administrator

Any browser: Once the N4L Security Certificate is installed, and if the user is permitted to reach e.g https://www.facebook.com then the requested page will be displayed without any SSL security error messages as seen below.



https://www.facebook.com/?stype=lo&jlou=Afdef_7uWuWNLbju6q8yJKDP8DIZACVM7mtQ38UPXkExM3yN9uiPOnF

Heading out? Stay connected

Visit facebook.com on your mobile phone.

Sign Up

It's free and always will be.

By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.

5.7. Secure Website Filtering for Chrome Devices

Google Chrome devices employ additional security measures to ensure user data is not intercepted. Google advises that to ensure correct functioning of Chrome devices that any Secure Website Inspection bypasses the following URLs.

accounts.youtube.com	omahaproxy.appspot.com
accounts.youtube.com	safebrowsing-cache.google.com
clients1.google.com	m.safebrowsing-cache.google.com
clients2.google.com	safebrowsing.google.com
clients3.google.com	ssl.gstatic.com
clients4.google.com	tools.google.com
cros-omahaproxy.appspot.com	pack.google.com
dl.google.com	www.gstatic.com
dl-ssl.google.com	gweb-gettingstartedguide.appspot.com
www.googleapis.com	storage.googleapis.com
m.google.com	commondatastorage.googleapis.com
accounts.gstatic.com (added August 2015)	

Source: https://support.google.com/chrome/a/answer/3504942

5.7.1. Creating a filter and rule for Chrome devices

The domains listed above can be excluded from Secure Website Inspection by:

1. Clicking on **Admin**
2. Choosing **Filter** from the **HTTPS Inspection** drop-down menu.
3. Choose an appropriate **filter name** for you to identify it later
4. Click **Domains** and enter the list found above into the domains field.
5. Click **Save** to save the filter
6. Choose **Policy** from the **HTTPS Inspection** drop-down menu.
7. Click on **Create Rule**
8. Choose an appropriate **rule name** for you to identify it later
9. Select **Do not inspect** from the certificate drop-down menu
10. Add the filter created above from the filters drop-down list and click **Set**
11. Click **Create Rule**
12. Move the newly created rule to the top of the policy list and tick the **Active** checkbox

Note: Depending on your Web Filtering policy, it may also be necessary to allow / whitelist the aforementioned URLs to ensure proper Chromebook usage in general.

5.8. Managing expiry of certificates

When certificates are generated (please see section 6 for details), the school chooses the **Duration** of 1, 3 ,5 or 7 years.

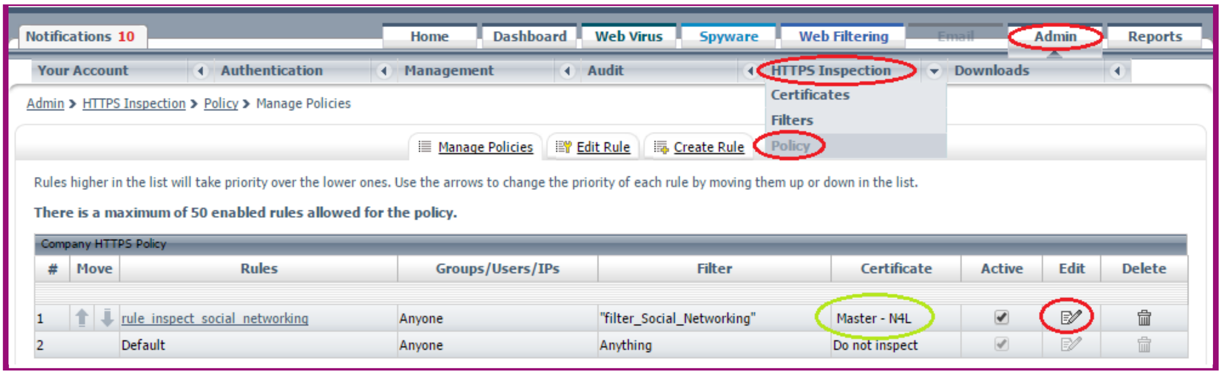
Please make note N4L does not manage the expiry of certificates, therefore note the expiry date of your certificate and put a process in place in which:

1. A reminder is generated before expiry
2. A new certificate is generated before expiry (either you manage or contact N4L to assist with the creation of a new certificate)
3. The new certificate is deployed to all devices
4. Update the school's Secure Website Inspection policy (either you manage or contact N4L to for assistance).

Once a new certificate has been generated for your school, and the new certificate has been rolled out to all devices requiring filtering, the necessary changes can be made within the Web Filtering Dashboard.

To update the Secure Website Inspection policy login to the Web Filtering Dashboard

Click on Admin - > HTTPS Inspection -> Policy
Click on Edit to modify any existing rules which reference the soon to be expiring certificate



Admin > HTTPS Inspection > Policy > Manage Policies

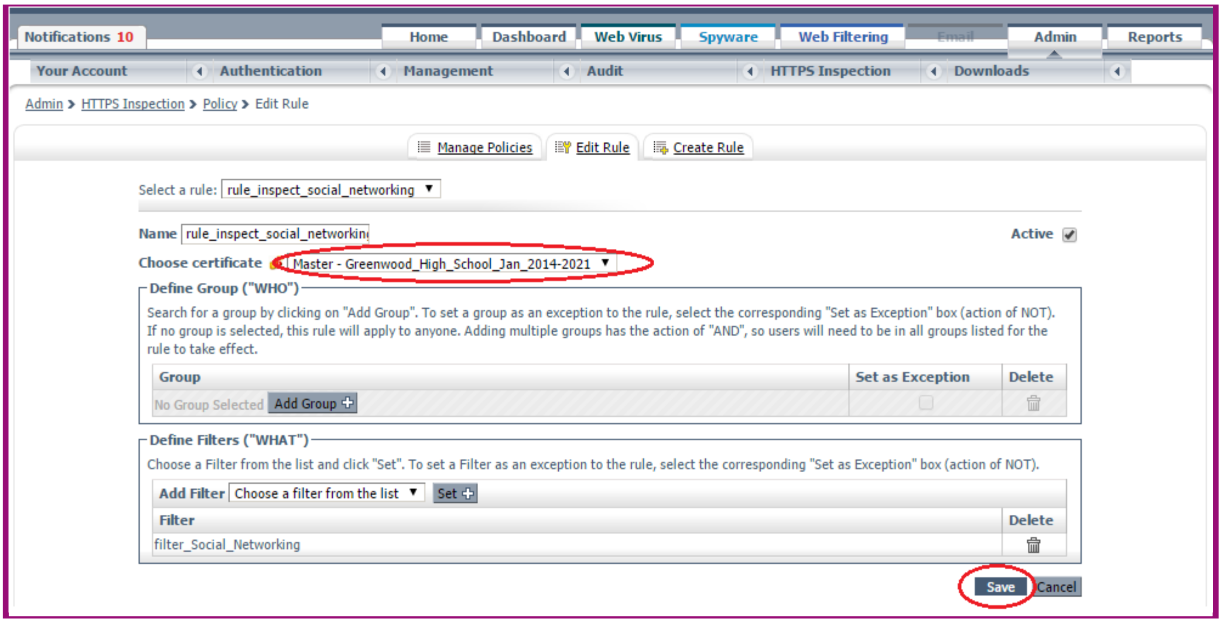
Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.

There is a maximum of 50 enabled rules allowed for the policy.

Company HTTPS Policy

#	Move	Rules	Groups/Users/IPs	Filter	Certificate	Active	Edit	Delete
1	↑ ↓	rule_inspect_social_networking	Anyone	"filter_Social_Networking"	Master - N4L	☑	✎	🗑
2		Default	Anyone	Anything	Do not inspect	☑	✎	🗑

Next select the newly created certificate from the drop-down list and save the changes.



Admin > HTTPS Inspection > Policy > Edit Rule

Select a rule: rule_inspect_social_networking ▼

Name rule_inspect_social_networkin Active ☑

Choose certificate Master - Greenwood_High_School_Jan_2014-2021 ▼

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "AND", so users will need to be in all groups listed for the rule to take effect.

Group	Set as Exception	Delete
No Group Selected Add Group +	□	🗑

Define Filters ("WHAT")

Choose a Filter from the list and click "Set". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter Choose a filter from the list ▼ Set +

Filter	Delete
filter_Social_Networking	🗑

Save Cancel

From now on when users browse to sites defined within the Secure Website Inspection rule they will be presented with the new filtering certificate.

6. Individualised Filtering

The integration of a Directory Service allows schools to leverage their existing systems to gain more from the N4L Web Filtering dashboard, rather than just a “one-size fits all” filtering solution.

Individualised Filtering allows schools to define different levels of access for different groups of users, or even individual users.

Scenarios can include:

- Allowing different browsing rules for different groups of users
- Disallowing internet browsing for a defined group of users
- Disallowing browsing at specific times for a defined group of users

Once implemented, users not already logged in will be required to authenticate their browsing session by logging in with their school network credentials.

As user based filtering requires cookies to maintain session states, only browser based web access is supported. If a “User Agent” e.g Desktop or Mobile Application does not support cookies then additional rules will be required to cater for such cases.

Almost any directory service which supports AD/LDAP or SAML can be added to the N4L Web Filtering Dashboard. LDAP Acceptance testing has been completed using Windows (Active Directory) and Novell network directories. SAML acceptance testing has been performed using SimpleSAMLphp, OpenAM and ADFS. Encryption for both protocols is supported and recommended.

6.1. Overview of the process

Once you have placed your request for Individualised Filtering with N4L you will need to do the following:

1. The school will supply N4L with a contact person that will manage the schools directory service. This may be your Web Filtering Administrator if they have a technical background.
2. N4L will open up the relevant ports on the Managed N4L Router/Firewall to allow the CCWS platform to connect to your schools directory service as required.
3. The allocated IT Administrator will:
   - Contact N4L to ensure relevant details have been supplied for the Firewall Rules to be implemented (if not already done)
   - Create an inspection certificate for your school in the Web Filtering dashboard
   - Create an LDAP/SAML Connection
   - Create User groups
   - Create an EasyID login screen for user authentication (AD/LDAP only)
4. The IT Administrator and the Web Filtering Administrator can then make changes to the N4L Web Filtering Dashboard to change the filters, rules to filter by user group as required.

6.2. Individualised Filtering Prerequisites

6.2.1. Inspection Certificate

For LDAP or SAML to be successfully integrated into N4l's Platform, you will need to created an Inspection Certificate and deploy this to your devices. To do this, please refer to Section 3 of this document, or Click Here

6.2.2. Firewall Rules (Not Required for SAML)

A school must permit inbound read-only access on TCP port 389 for LDAP or TCP port 636 for secure LDAP to the LDAP server from the following public IP addresses:

- 80.254.145.4
- 202.177.218.34
- 210.55.186.224
- 210.55.186.225
- 108.171.130.224
- 108.171.130.225
- 108.171.133.224
- 108.172.133.225
- 46.255.41.27
- 46.255.41.28
- 108.171.134.225
- 108.171.134.224

The N4L Helpdesk can arrange the necessary inbound firewall rules and restrict access to just the public IP addresses listed above. To request changes for your school email support@n4l.co.nz.

6.2.3. User Groups

The N4L Web Filtering dashboard can use different groups to define a set of users:

- The group can be an existing group; or
- One specifically made for the purpose of filtering

Notes:

- Users can be a member of more than one group
- All users that need to authenticate must be a member of at least one group
- In order to make use of user groups within the filtering dashboard, groups must first be setup to reference an LDAP or SAML group.

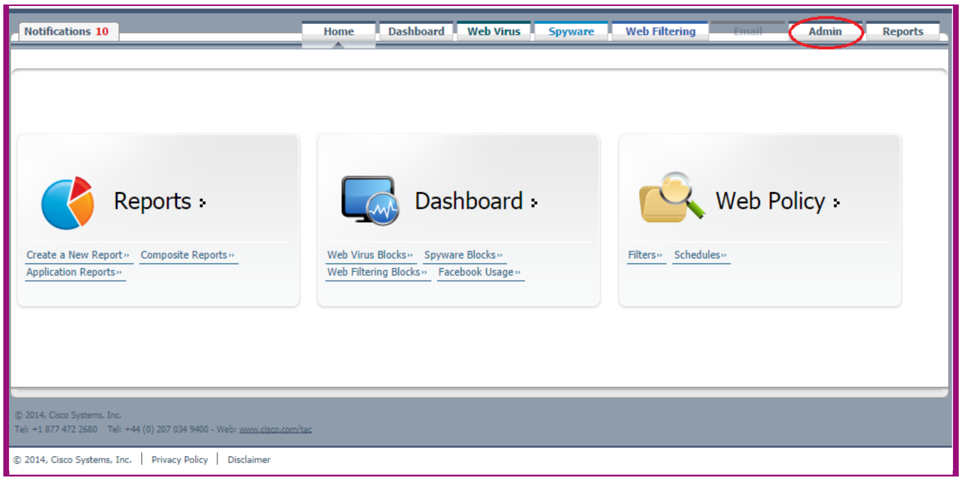
6.2.4. Rollback Plan

Before you enable your directory service integrated filtering rules, be sure to keep any existing filtering rules in a disabled state should you need rollback due to any difficulties.

6.3. Setting up Individualised Filtering

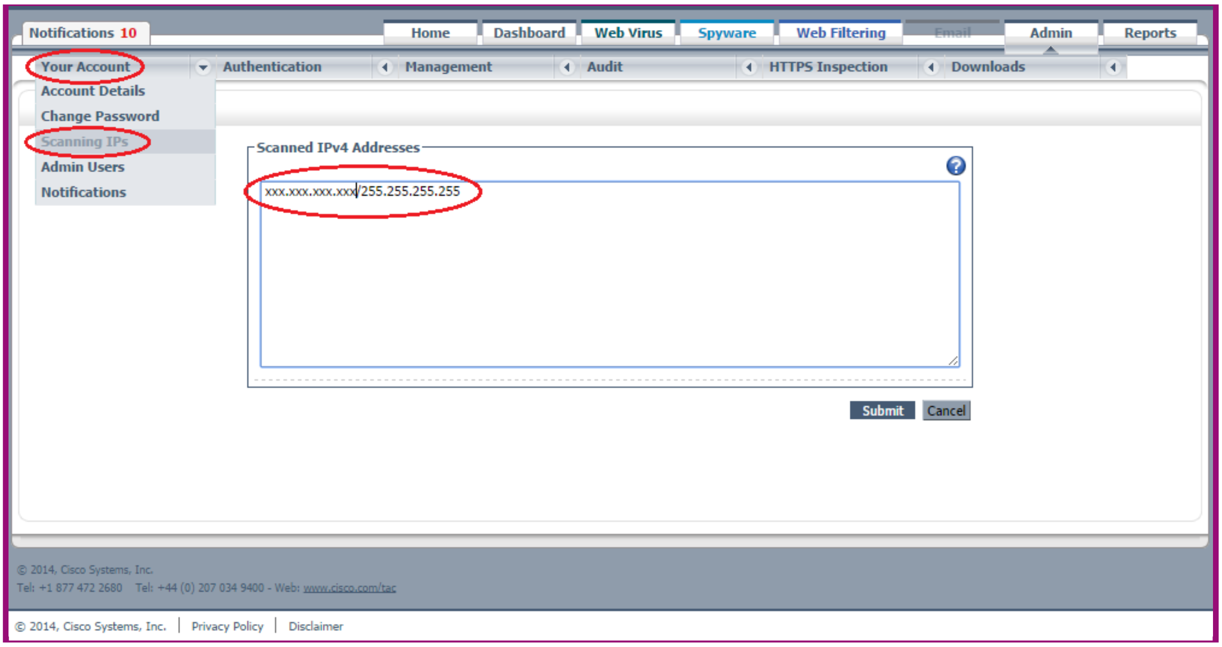
6.3.1. Creating an LDAP Connection (AD/LDAP only)

1. Log in to your N4L Web Filtering dashboard
2. Click on the **Admin** tab



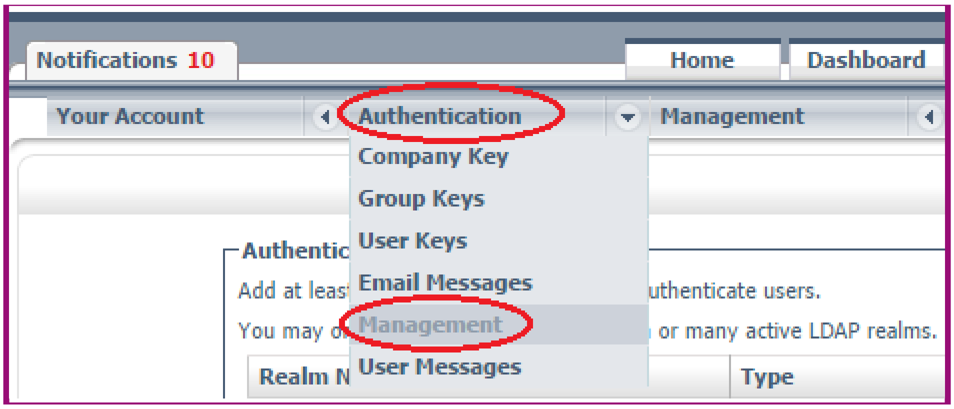
3. The first task is to define the IP address of the LDAP server as a **Scanning IP** to your dashboard
   3.1.1. Choose **Scanning IPs** from the **Your Account** dropdown menu
4. Type in the public IP address of the LDAP server(s), including the network mask
5. Click **Submit**

This information is used to configure the CCWS “Tower” firewalls to permit access from CCWS to the LDAP server(s) in the range defined by the Scanning IP entry.



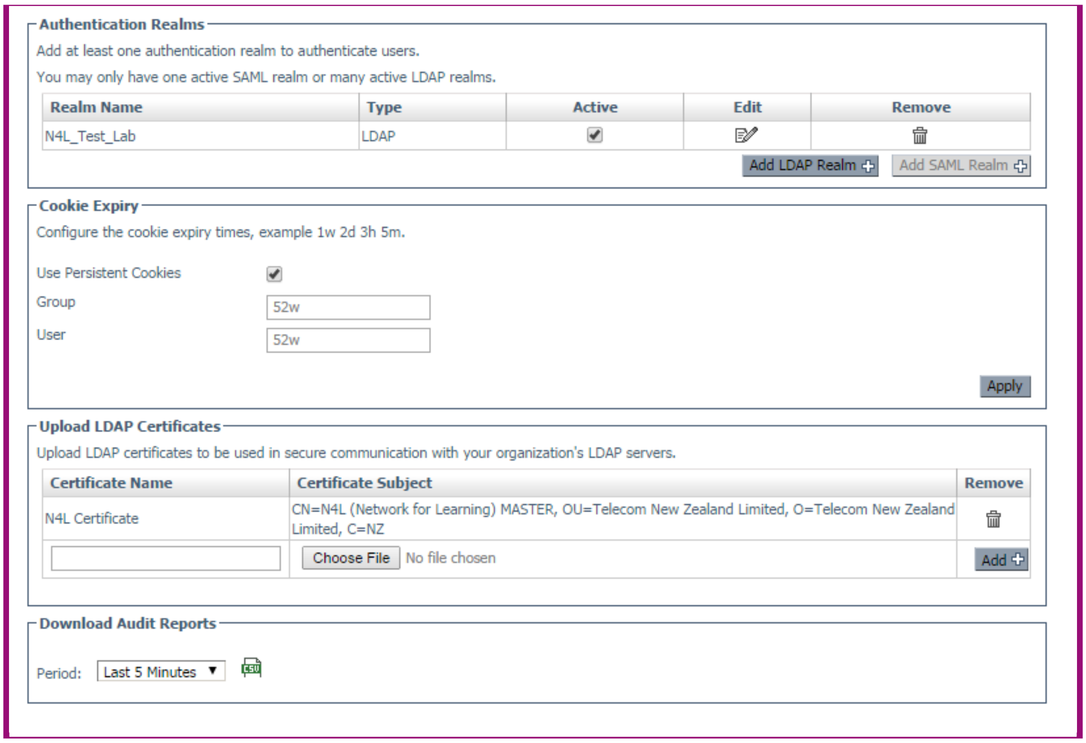
Scanned IPv4 Addresses: xxx.xxx.xxx.xxx/255.255.255.255

6. Choose **Management** from the **Authentication** dropdown menu



Here there are four sections:

- Upload LDAP Certificates (see step 7)
- Authentication Realms (see step 8)
- Cookie Expiry (see step 9)
- Download Audit report (see step 10)



Authentication Realms

Add at least one authentication realm to authenticate users.

You may only have one active SAML realm or many active LDAP realms.

Realm Name	Type	Active	Edit	Remove
N4L_Test_Lab	LDAP	☑	✎	🗑

Cookie Expiry

Configure the cookie expiry times, example 1w 2d 3h 5m.

Use Persistent Cookies ☑

Group 52w

User 52w

Upload LDAP Certificates

Upload LDAP certificates to be used in secure communication with your organization's LDAP servers.

Certificate Name	Certificate Subject	Remove
N4L Certificate	CN=N4L (Network for Learning) MASTER, OU=Telecom New Zealand Limited, O=Telecom New Zealand Limited, C=NZ	🗑
	Choose File No file chosen	Add

Download Audit Reports

Period: Last 5 Minutes ▼

Note: While LDAP and LDAPS connections are secured by a firewall, user credentials transmitted when using LDAP are transmitted between the CCWS platform and your LDAP server in plain text. It is recommended to make use of LDAPS where possible. LDAPS uses an SSL/TLS connection between the CCWS platform and your LDAP server to ensure user credentials remain secure at all times.

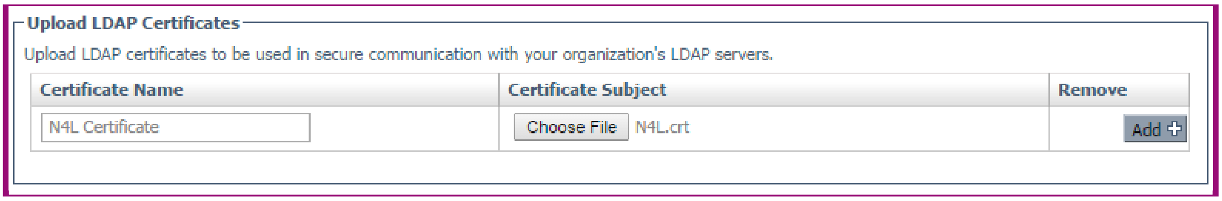
The following guide can be followed for help on creating a suitable certificate within a Microsoft environment:

http://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx .

In a Unix environment the same process would need to be followed, which involves creating a self-signed certificate and the necessary configuration adjustments to your LDAP directory to enable LDAPS.

If you do not wish to make use of LDAPS you may skip step 7.

7. In the **Upload LDAP Certificates** section:
   - 7.1. Provide a name for your LDAPS certificate
   - 7.2. Click **Choose File** to locate your certificate
   - 7.3. Click **Add** to upload the certificate to the N4L Web Filtering dashboard

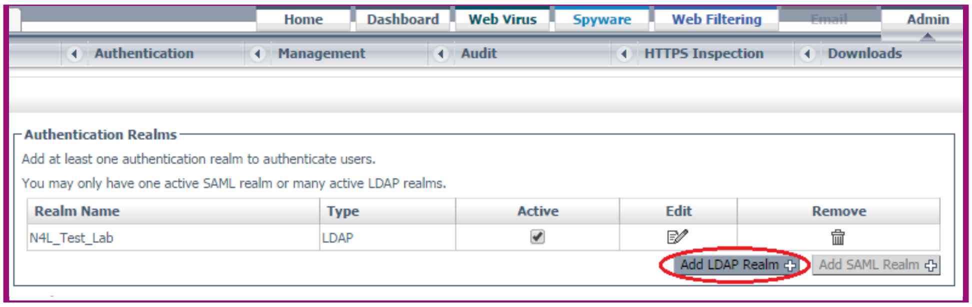


Upload LDAP Certificates

Upload LDAP certificates to be used in secure communication with your organization's LDAP servers.

Certificate Name	Certificate Subject	Remove
N4L Certificate	Choose File N4L.crt	Add ✚

8. In the **Authentication Realms** section:
   - 8.1. Select **Add LDAP Realm** or choose to edit an existing realm



Authentication Realms

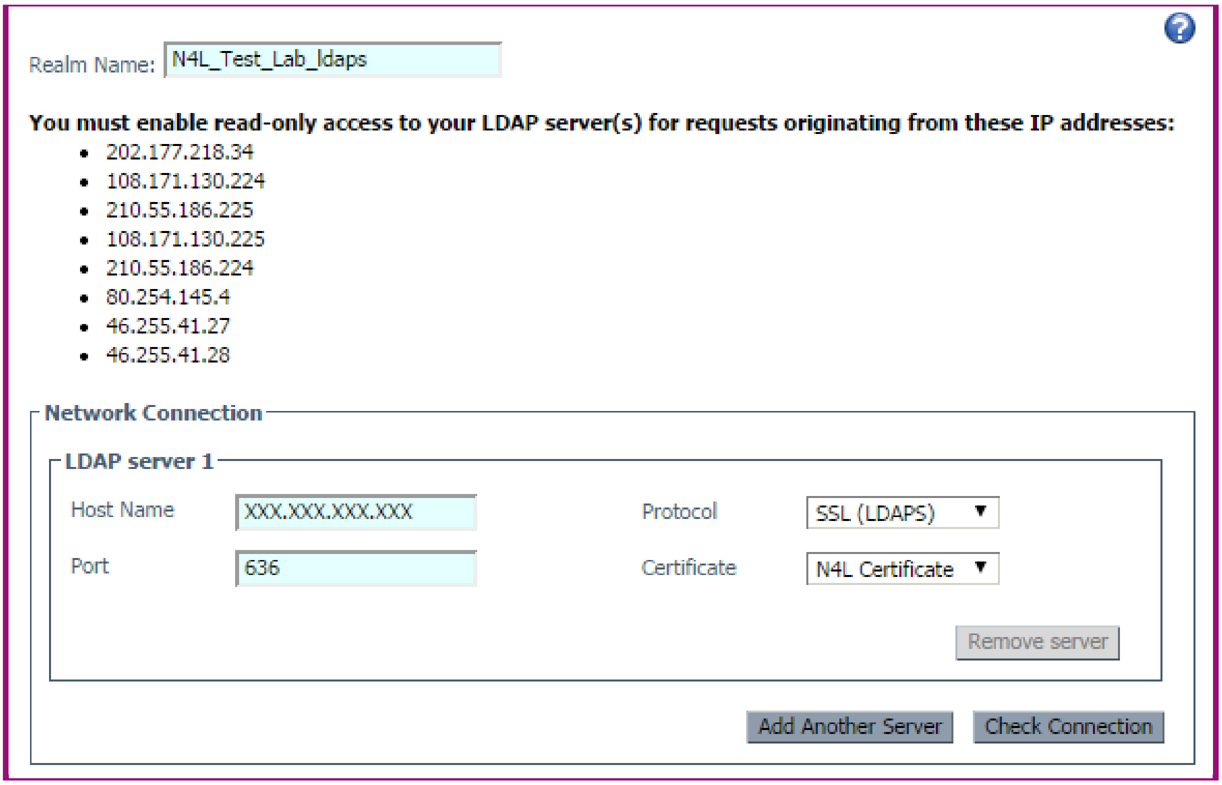
Add at least one authentication realm to authenticate users.

You may only have one active SAML realm or many active LDAP realms.

Realm Name	Type	Active	Edit	Remove
N4L_Test_Lab	LDAP	☑	✎	🗑

Add LDAP Realm ✚ Add SAML Realm ✚

   - 8.2. Select **Add LDAP Realm** or choose to edit an existing realm
     - 8.2.1. Provide a name for your realm
     - 8.2.2. Enter the IP address of your read-only LDAP server as supplied earlier
     - 8.2.3. Select the protocol LDAP or LDAPS, this will auto populate which port to use
     - 8.2.4. If using LDAPS, select the certificate uploaded earlier from the list
     - 8.2.5. Click on **Check Connection** to save your settings



Realm Name: N4L_Test_Lab_ldaps

You must enable read-only access to your LDAP server(s) for requests originating from these IP addresses:

- 202.177.218.34
- 108.171.130.224
- 210.55.186.225
- 108.171.130.225
- 210.55.186.224
- 80.254.145.4
- 46.255.41.27
- 46.255.41.28

Network Connection

LDAP server 1

Host Name: XXX.XXX.XXX.XXX

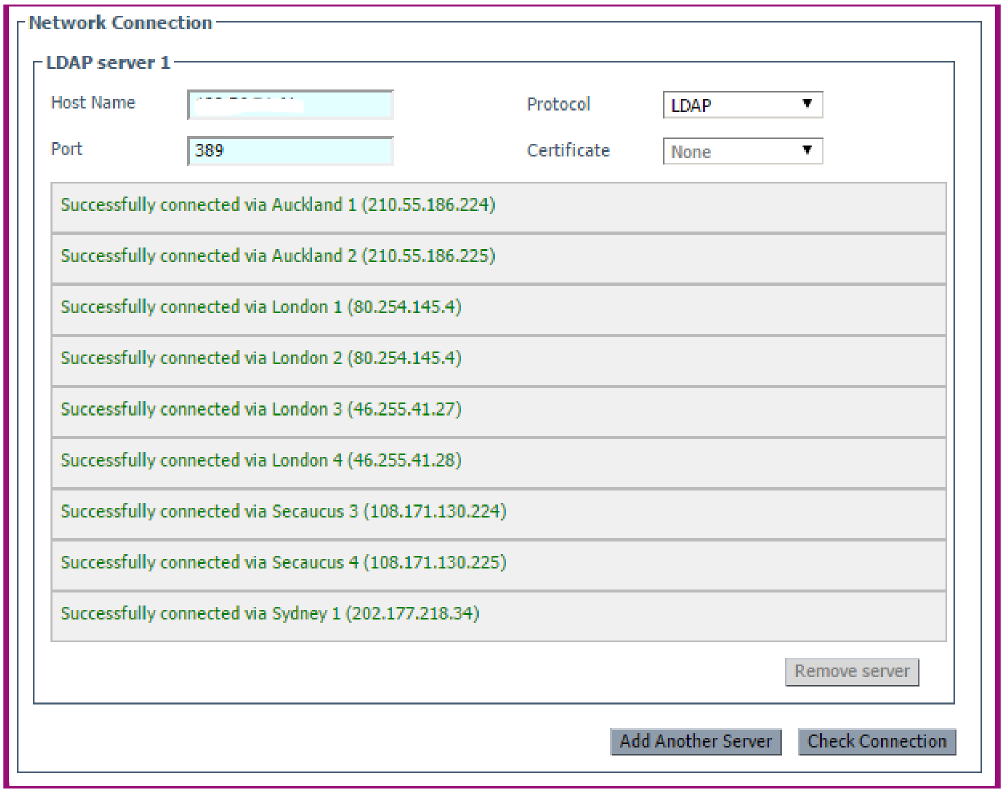
Port: 636

Protocol: SSL (LDAPS)

Certificate: N4L Certificate

8.3. The N4L Web Filtering Dashboard will then attempt to make a connection to your LDAP server/s, and if all the firewall rules are correct then *"**Successfully connected via …**"* results will be displayed.

Note: A successful connection is not required to all the servers.



Network Connection

LDAP server 1

Host Name: [redacted]

Port: 389

Protocol: LDAP

Certificate: None

Successfully connected via Auckland 1 (210.55.186.224)

Successfully connected via Auckland 2 (210.55.186.225)

Successfully connected via London 1 (80.254.145.4)

Successfully connected via London 2 (80.254.145.4)

Successfully connected via London 3 (46.255.41.27)

Successfully connected via London 4 (46.255.41.28)

Successfully connected via Secaucus 3 (108.171.130.224)

Successfully connected via Secaucus 4 (108.171.130.225)

Successfully connected via Sydney 1 (202.177.218.34)

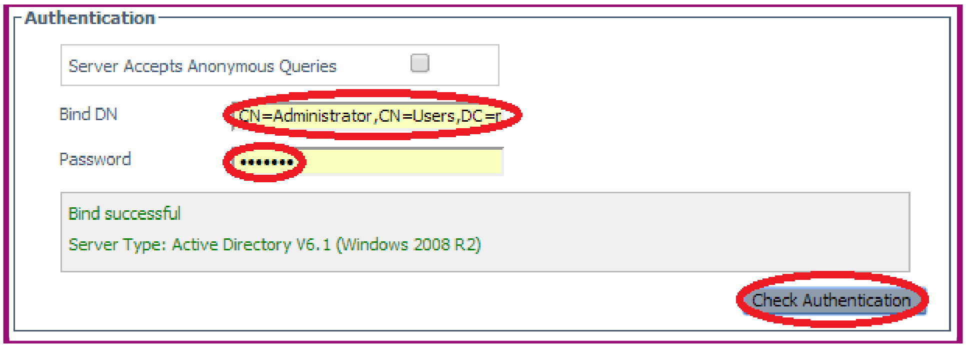
8.4. Once the connection is established **Bind DN** credentials can be entered. Your school’s IT administrator will be able to supply you with these details to:

8.4.1. Enter the **Bind DN** user details and password

8.4.2. Click **Check Authentication**

8.4.3. If the bind is successful the **Server Type** will be returned

Note: Any valid user with at least read access to the directory can be used. The format of the **Bind DN** user must match the syntax used by the particular directory that is being used.



Authentication

Server Accepts Anonymous Queries □

Bind DN CN=Administrator,CN=Users,DC=r

Password •••••••

Bind successful

Server Type: Active Directory V6.1 (Windows 2008 R2)

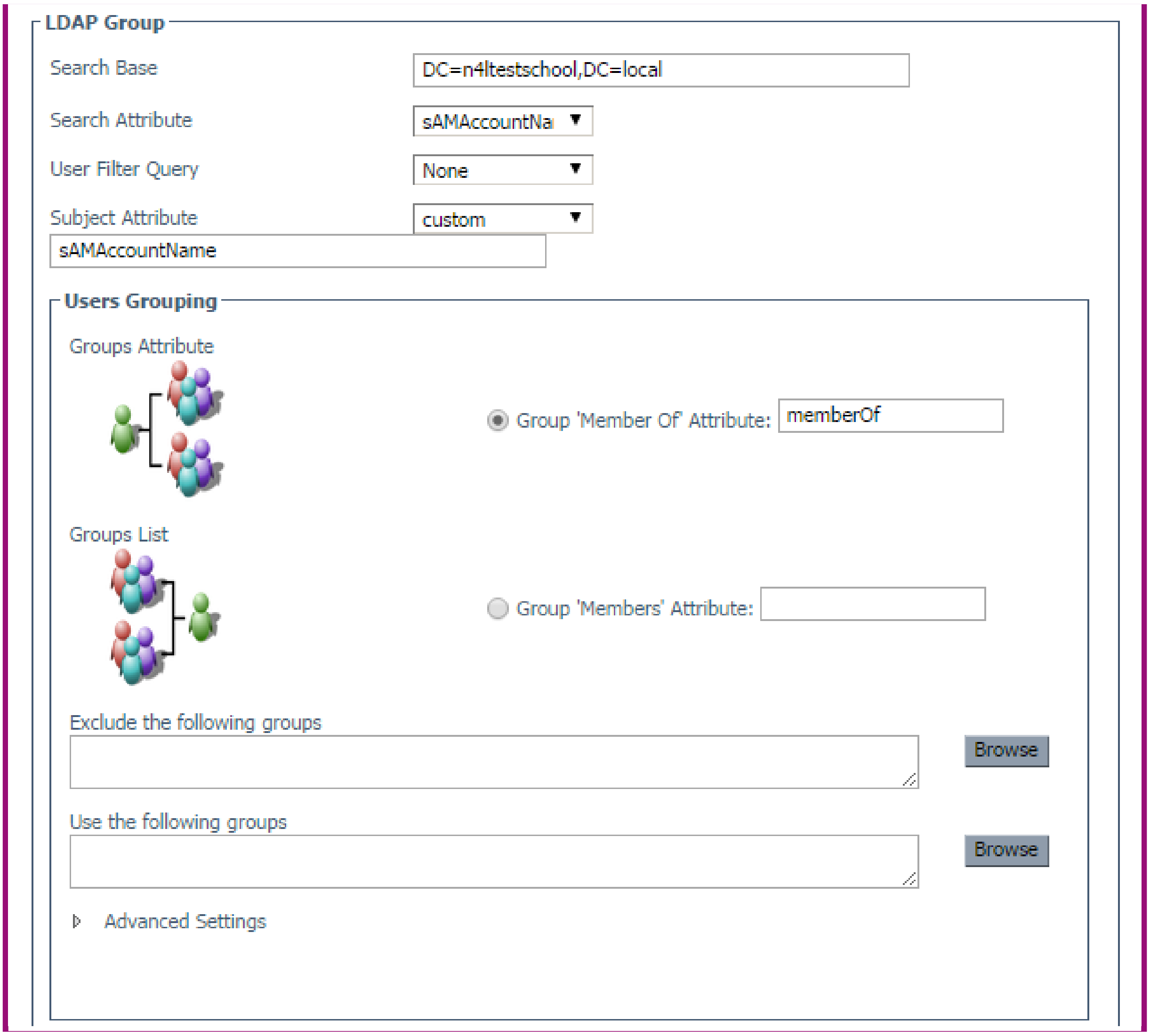
If the password of the **Bind DN** user is ever changed then this **<u>must</u>** be reflected here too.

8.5. Scroll down to LDAP Group and add the following details:

8.5.1. For Search Base, enter the details for the specific LDAP server. This could refer to just a specific CN if required eg “CN=Users,DC=domain,DC=local”

8.5.2. Complete details as shown for:

- Search Attribute
- User Filter Query
- Subject Attribute – this should be set to “Custom” and “sAMAccountName”



LDAP Group

Search Base: DC=n4ltestschool,DC=local

Search Attribute: sAMAccountNa

User Filter Query: None

Subject Attribute: custom

sAMAccountName

Users Grouping

Groups Attribute

● Group 'Member Of' Attribute: memberOf

Groups List

○ Group 'Members' Attribute:

Exclude the following groups

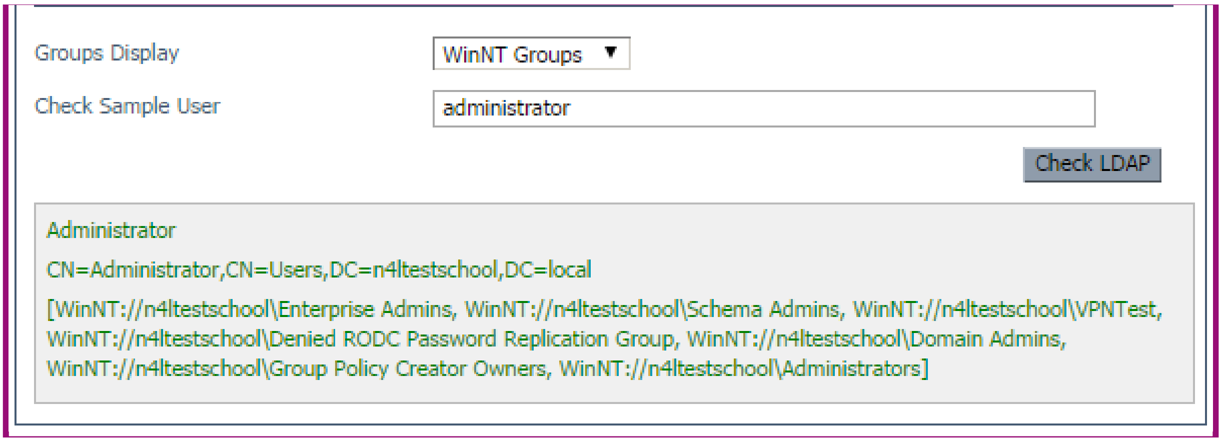
Use the following groups

8.5.3. Groups can be excluded, which doubles to improve authentication speed

8.5.4. Next we will test to make sure we have supplied the correct group details. If the LDAP server is a Windows domain controller, select “WinNT Groups” from “Groups Display”. Otherwise select “LDAP Standard” from the pull-down menu

8.5.5. To check a user enter the username into the “Check Sample User” box and click “Check LDAP”

- In the example below the “WinNT://” groups are displayed



Groups Display: WinNT Groups

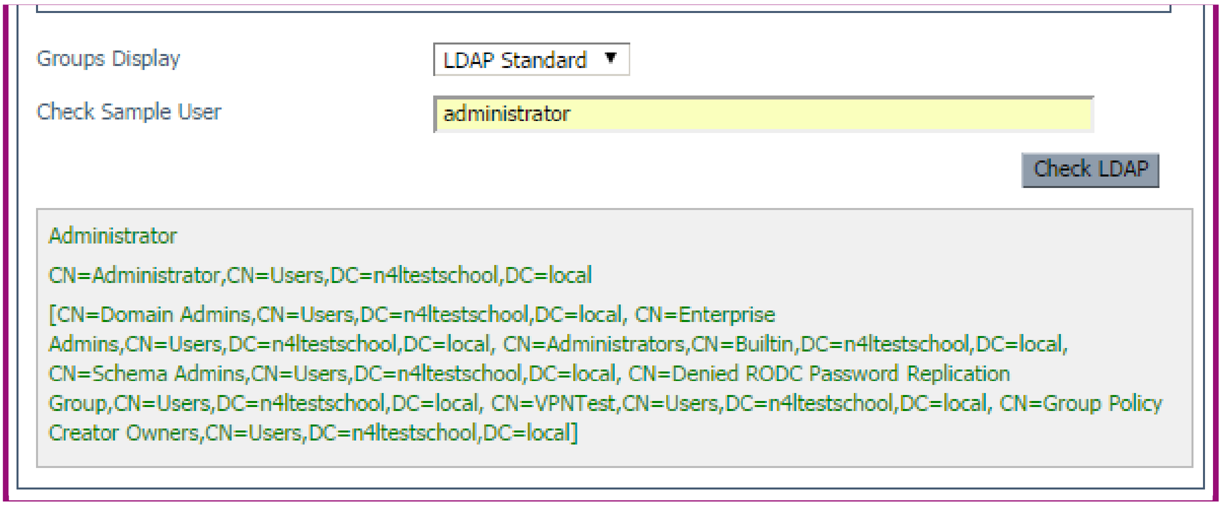
Check Sample User: administrator

Administrator

CN=Administrator,CN=Users,DC=n4ltestschool,DC=local

[WinNT://n4ltestschool\Enterprise Admins, WinNT://n4ltestschool\Schema Admins, WinNT://n4ltestschool\VPNTest, WinNT://n4ltestschool\Denied RODC Password Replication Group, WinNT://n4ltestschool\Domain Admins, WinNT://n4ltestschool\Group Policy Creator Owners, WinNT://n4ltestschool\Administrators]

- If "LDAP Standard" is selected then the full LDAP paths for the groups are displayed.



Groups Display: LDAP Standard

Check Sample User: administrator

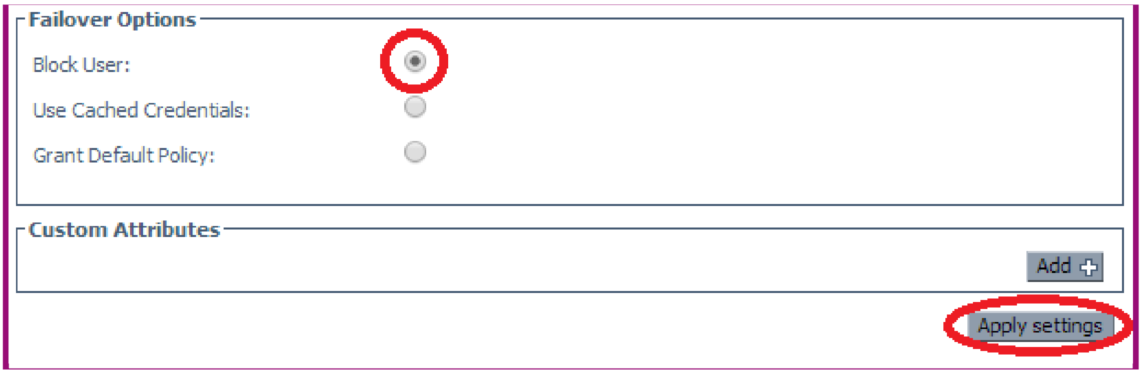
Administrator

CN=Administrator,CN=Users,DC=n4ltestschool,DC=local

[CN=Domain Admins,CN=Users,DC=n4ltestschool,DC=local, CN=Enterprise Admins,CN=Users,DC=n4ltestschool,DC=local, CN=Administrators,CN=Builtin,DC=n4ltestschool,DC=local, CN=Schema Admins,CN=Users,DC=n4ltestschool,DC=local, CN=Denied RODC Password Replication Group,CN=Users,DC=n4ltestschool,DC=local, CN=VPNTest,CN=Users,DC=n4ltestschool,DC=local, CN=Group Policy Creator Owners,CN=Users,DC=n4ltestschool,DC=local]

Note: Later "Groups" will need to be defined to N4L Web Filtering dashboard in order to allow user based filtering, and these user checks help ensure you provide the correct information to match the groups back to your directory structure.

8.5.6. Next we have the ability to define how users who do not successfully authenticate against your directory are handled.



Failover Options

Block User: ●

Use Cached Credentials: ○

Grant Default Policy: ○

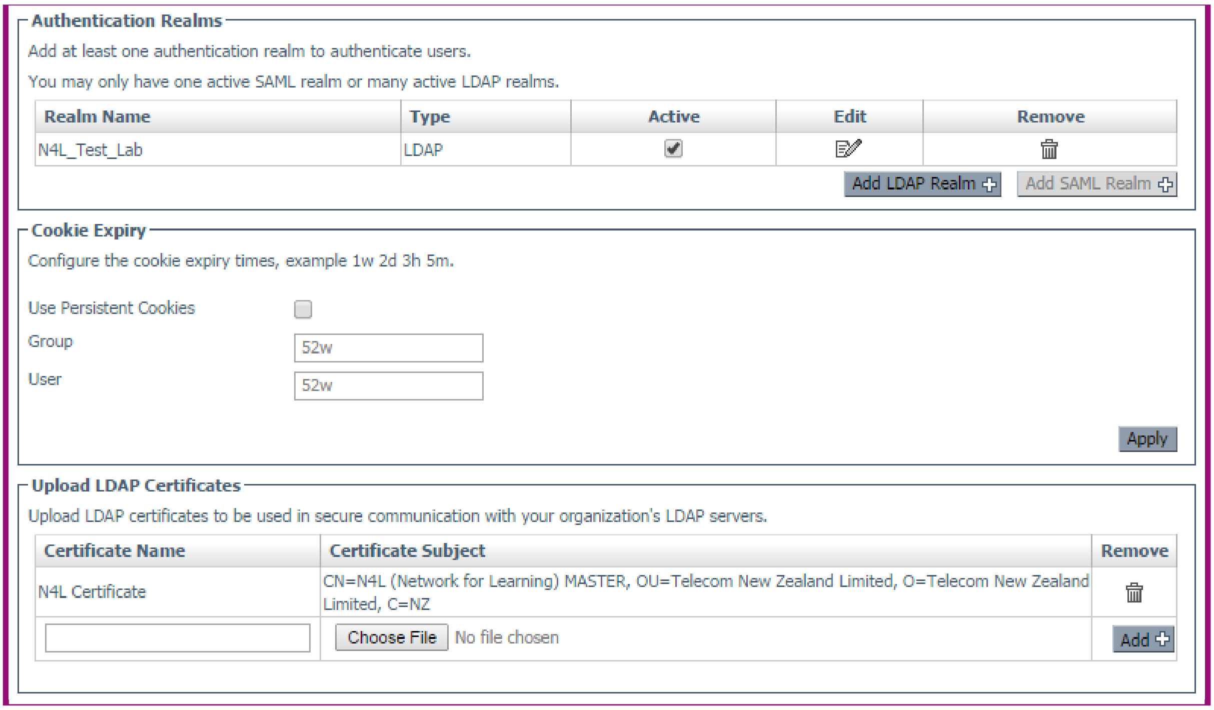
Custom Attributes

8.6. Finally click **Apply Settings**

9. In the **Surrogate Mechanism** section you have the option to define the **Cookie Expiry** times.

Options:

- By default a cookie is non persistent meaning that it will expire when the browser is closed down.
- You may choose to force users to authenticate daily, meaning a one day Cookie Expiry may be considered.
- If you prefer you can set a cookie to be persistent. This means that all users on the device sharing the same profile will effectively be logged in for the lifetime of the cookie.
- Long session times could be used, however if a user ever needed to be logged out or suspended, cookies would need to be manually deleted using ‘behind the scenes’ features of each browser.



Authentication Realms

Add at least one authentication realm to authenticate users.

You may only have one active SAML realm or many active LDAP realms.

Realm Name	Type	Active	Edit	Remove
N4L_Test_Lab	LDAP	☑	✎	🗑

Cookie Expiry

Configure the cookie expiry times, example 1w 2d 3h 5m.

Use Persistent Cookies	□
Group	52w
User	52w

Upload LDAP Certificates

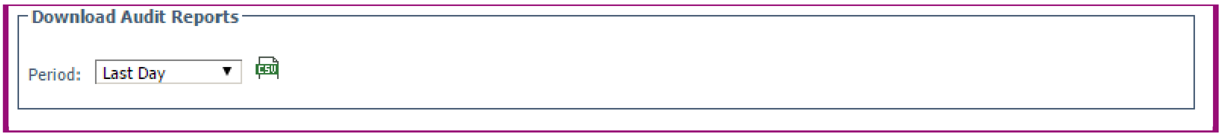
Upload LDAP certificates to be used in secure communication with your organization's LDAP servers.

Certificate Name	Certificate Subject	Remove
N4L Certificate	CN=N4L (Network for Learning) MASTER, OU=Telecom New Zealand Limited, O=Telecom New Zealand Limited, C=NZ	🗑
	Choose File No file chosen	Add

Note: In order to implement Individualised Filtering the user agent must support cookies. There are many applications (non-browser based) which will not support user authentication. The web filtering rules are flexible enough to allow a mixture of authenticated browser access and non-authenticated “other” application access.
As an example, this would allow a school to permit access from an iPad to the TVNZ OnDemand app but block access to the Facebook or YouTube apps.

If you have not yet completed the training material, a full set of resourcesare available on the N4L website (http://www.n4l.co.nz/managednetwork/webfiltering/) . The material covers web filtering, filters, schedules, rules and policy creation.

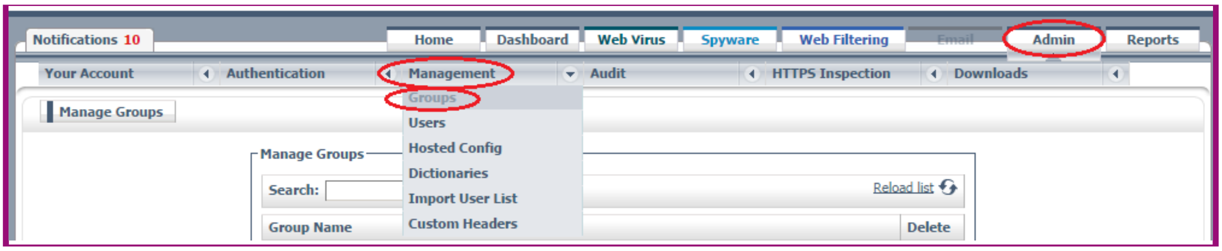
10. In order to troubleshoot any LDAP connectivity issues between the N4L Web Filtering dashboard and your LDAP servers, an audit log can be obtained by selecting the time period (last 5 minutes, last hour or last day) and clicking on the .csv export icon.

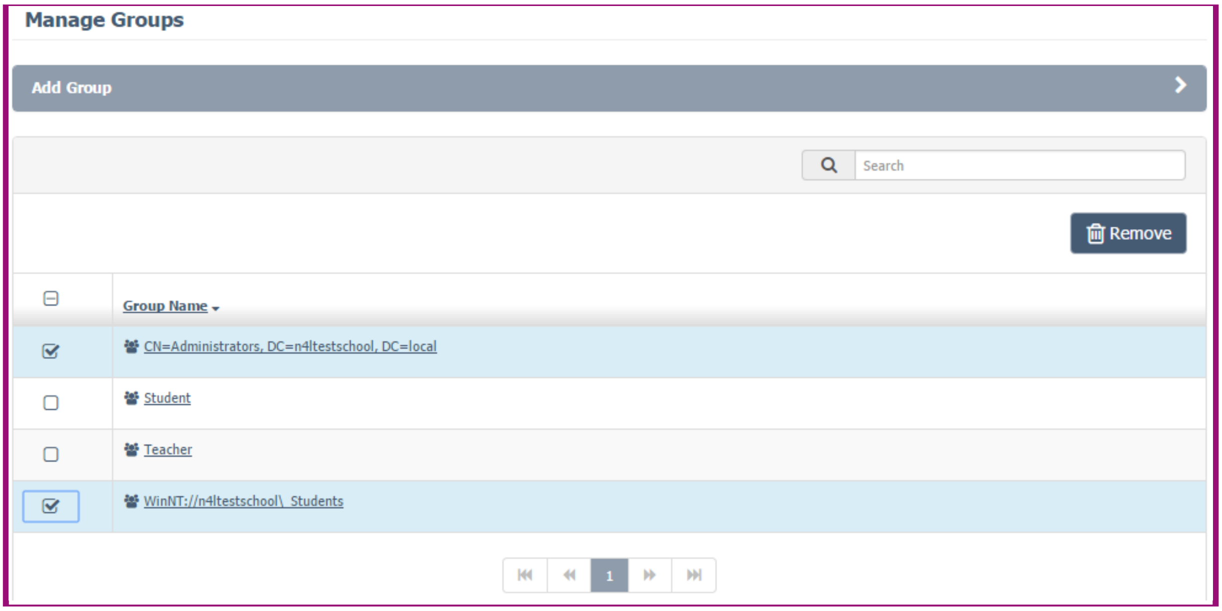

Download Audit Reports

Period: Last Day

6.3.2. Creating LDAP Groups

1. Log in to your N4L Web Filtering dashboard
2. Click on the **Admin** tab
3. Choose **Groups** from the **Management** dropdown menu



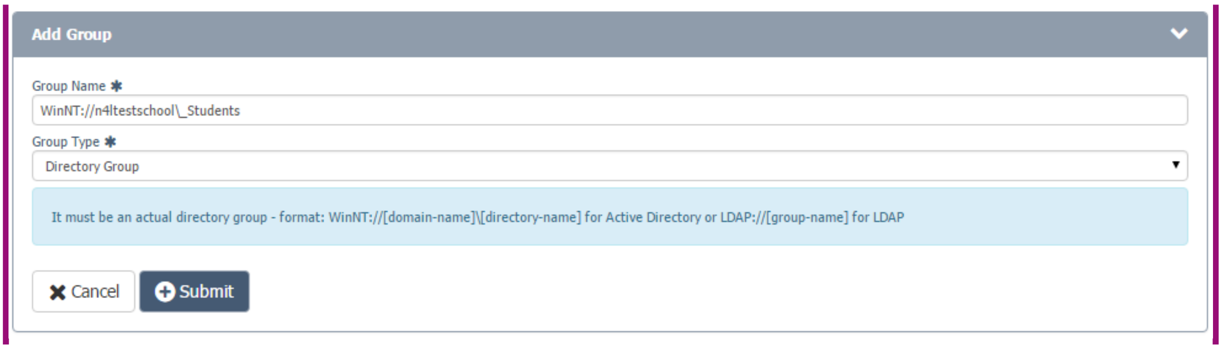

Manage Groups

	Group Name
☑	CN=Administrators, DC=n4ltestschool, DC=local
□	Student
□	Teacher
☑	WinNT://n4ltestschool_Students

4. To add a group you can either:
   4.1. Add a “WinNT://” group click **Add Directory Group**; or
   4.2. Add a “LDAP Standard” group click **Add Custom Group**

Note:
WinNT:// is used for Windows Active Directory groups. All other LDAP groups should be set us as "LDAP Standard" groups. WinNT is a shorter form of the group name. LDAP can still be used but the syntax of the group name is far more complex**.**

A **Directory Group** must be defined with "WinNT://" as the prefix for AD, or "LDAP://" as the prefix for LDAP directory services.



Add Group

Group Name ✱

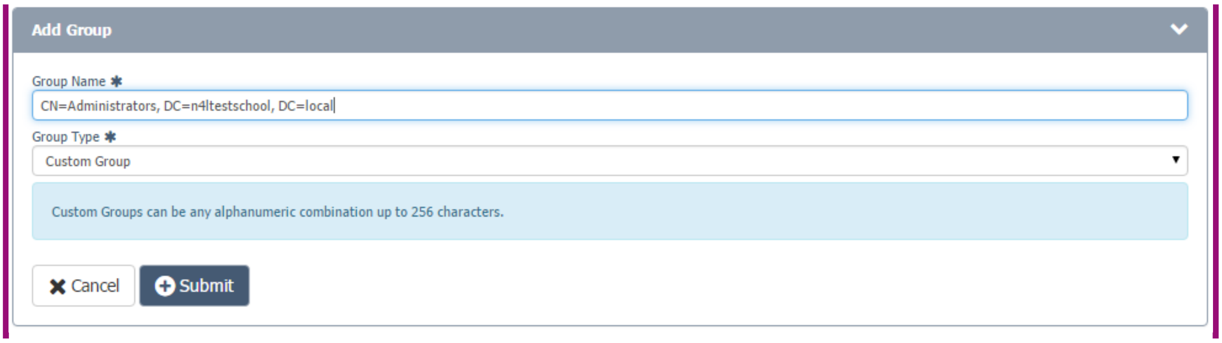
WinNT://n4ltestschool_Students

Group Type ✱

Directory Group

It must be an actual directory group - format: WinNT://[domain-name]\[directory-name] for Active Directory or LDAP://[group-name] for LDAP

A **Custom Group** is used for all other "LDAP Standard" groups:



Add Group

Group Name ✱

CN=Administrators, DC=n4ltestschool, DC=local

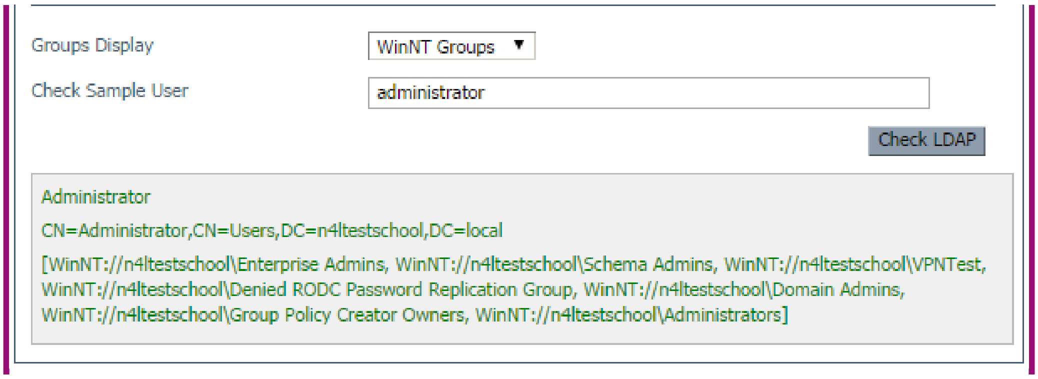
Group Type ✱

Custom Group

Custom Groups can be any alphanumeric combination up to 256 characters.

Note: The critical part of using a group name is to use the **same format** as defined by the output when checking a sample LDAP user, as shown earlier.

"WinNT Group":

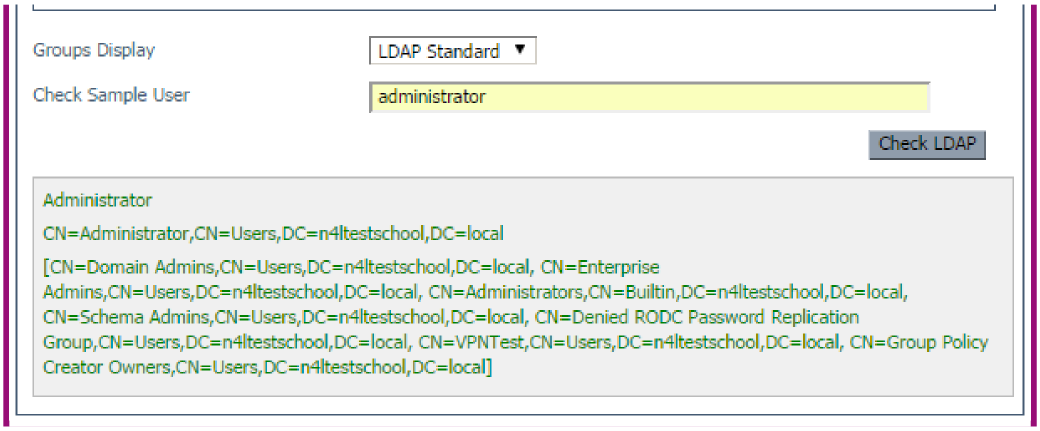


Groups Display: WinNT Groups

Check Sample User: administrator

```
Administrator
CN=Administrator,CN=Users,DC=n4ltestschool,DC=local
[WinNT://n4ltestschool\Enterprise Admins, WinNT://n4ltestschool\Schema Admins, WinNT://n4ltestschool\VPNTest,
WinNT://n4ltestschool\Denied RODC Password Replication Group, WinNT://n4ltestschool\Domain Admins,
WinNT://n4ltestschool\Group Policy Creator Owners, WinNT://n4ltestschool\Administrators]
```

"LDAP Standard":



Administrator

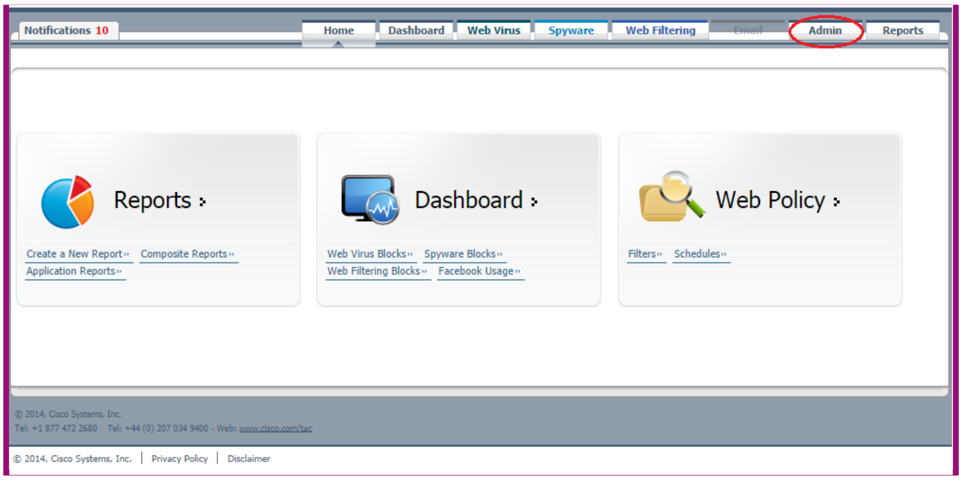
CN=Administrator,CN=Users,DC=n4ltestschool,DC=local

[CN=Domain Admins,CN=Users,DC=n4ltestschool,DC=local, CN=Enterprise Admins,CN=Users,DC=n4ltestschool,DC=local, CN=Administrators,CN=Builtin,DC=n4ltestschool,DC=local, CN=Schema Admins,CN=Users,DC=n4ltestschool,DC=local, CN=Denied RODC Password Replication Group,CN=Users,DC=n4ltestschool,DC=local, CN=VPNTest,CN=Users,DC=n4ltestschool,DC=local, CN=Group Policy Creator Owners,CN=Users,DC=n4ltestschool,DC=local]

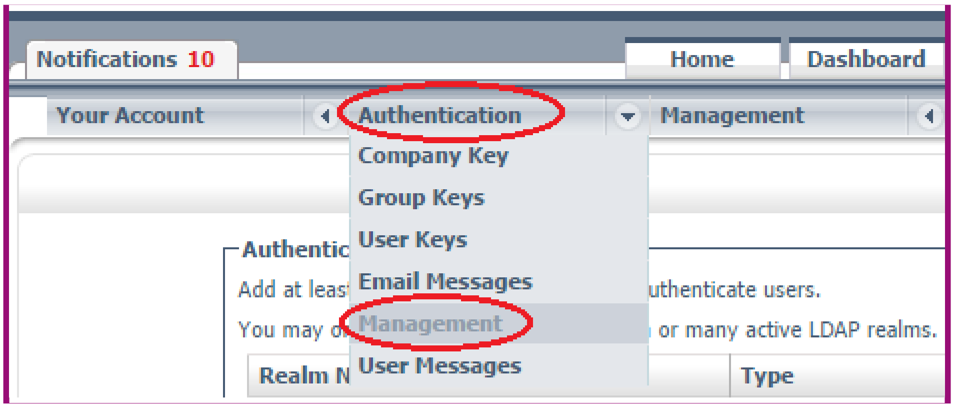
6.3.3. SAML Integration

1. Log in to your N4L Web Filtering Dashboard

2. Click on the **Admin** tab

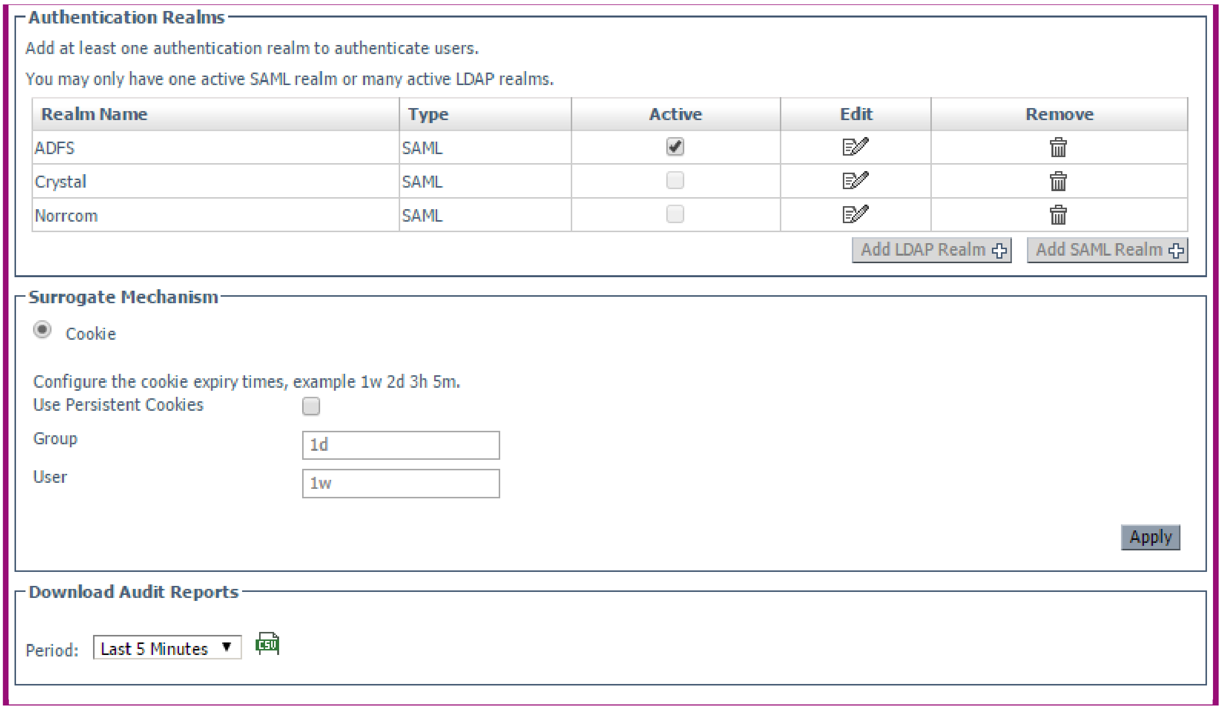


3. Choose **Management** from the **Authentication** dropdown menu



Here there are three relevant sections:

- Authentication Realms (see step 8)
- Surrogate Mechanism (see step 9)
- Download Audit report (see step 10)



Authentication Realms

Add at least one authentication realm to authenticate users.

You may only have one active SAML realm or many active LDAP realms.

Realm Name	Type	Active	Edit	Remove
ADFS	SAML	☑	✎	🗑
Crystal	SAML	☐	✎	🗑
Norrcom	SAML	☐	✎	🗑

Surrogate Mechanism

● Cookie

Configure the cookie expiry times, example 1w 2d 3h 5m.

Use Persistent Cookies ☐

Group 1d

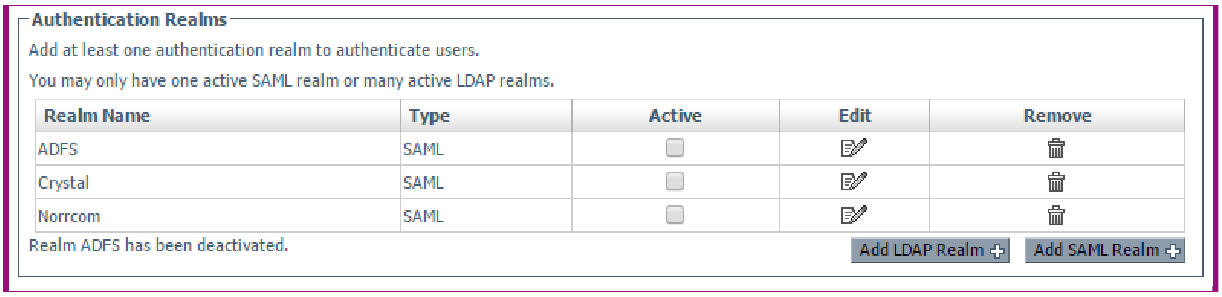
User 1w

Download Audit Reports

Period: Last 5 Minutes

4. In the **Authentication Realms** section:

4.1 Select **Add SAML Realm** or choose to **Edit** an existing realm



Authentication Realms

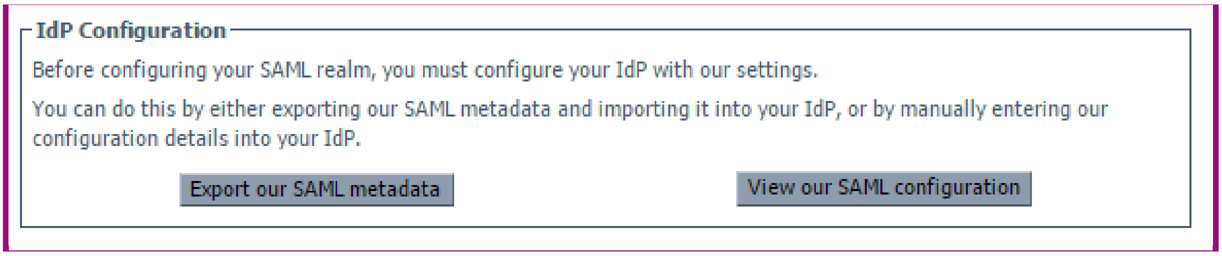
Add at least one authentication realm to authenticate users.

You may only have one active SAML realm or many active LDAP realms.

Realm Name	Type	Active	Edit	Remove
ADFS	SAML	☐	✎	🗑
Crystal	SAML	☐	✎	🗑
Norrcom	SAML	☐	✎	🗑

Realm ADFS has been deactivated.

4.2. When prompted click **Export our SAML metadata**, or click **view our SAML configuration** if your SAML Identity Provider does not support importing a .XML SAML metadata file.



IdP Configuration

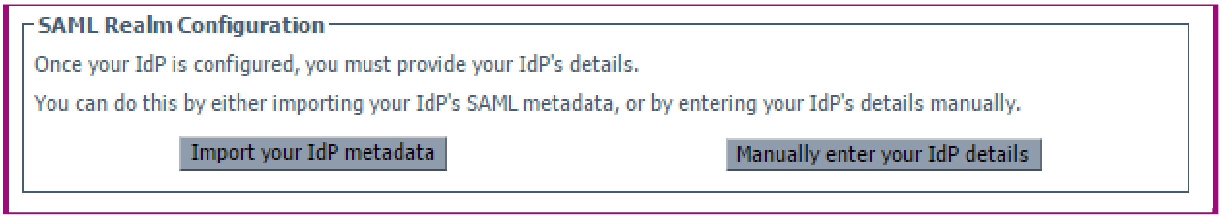
Before configuring your SAML realm, you must configure your IdP with our settings.

You can do this by either exporting our SAML metadata and importing it into your IdP, or by manually entering our configuration details into your IdP.

4.3 The next step is to import the N4L Web Filtering SAML metadata into your IdP. If you are using a hosted SAML Identity Provider and this is the first time the

Identity Provider system has integrated with N4L's Web Filtering platform, the administrators of the system may need to do this for you.

4.2.2 Next we'll configure the Web Filtering dashboard with your Identity Provider's configuration details by clicking Import your IdP metadata and selecting your SAML metadata .XML file, or by clicking Manually enter your IdP details if you do not have them in .XML format.

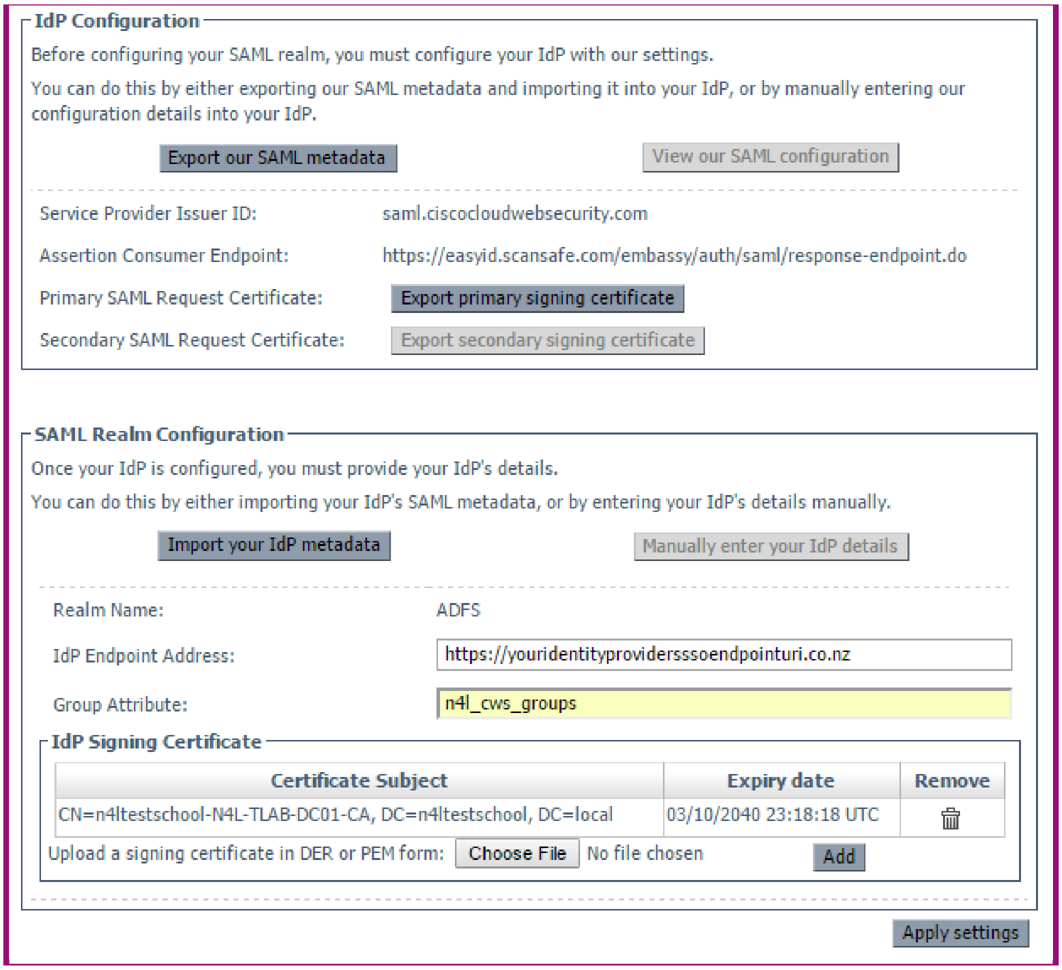


SAML Realm Configuration

Once your IdP is configured, you must provide your IdP's details.

You can do this by either importing your IdP's SAML metadata, or by entering your IdP's details manually.

4.2.3 Once you have either imported your SAML metadata or entered the details in manually, including uploading of your IdP certificate, you need to supply the Realm Name to identify the IdP. This can be anything you like. Next enter the Group Attribute which the web filtering platform will use to find user's group associations within the SAML assertion. Your Identity Provider will be able to supply this to you.



IdP Configuration

Before configuring your SAML realm, you must configure your IdP with our settings.

You can do this by either exporting our SAML metadata and importing it into your IdP, or by manually entering our configuration details into your IdP.

Service Provider Issuer ID: saml.ciscocloudwebsecurity.com

Assertion Consumer Endpoint: https://easyid.scansafe.com/embassy/auth/saml/response-endpoint.do

Primary SAML Request Certificate: Export primary signing certificate

Secondary SAML Request Certificate: Export secondary signing certificate

SAML Realm Configuration

Once your IdP is configured, you must provide your IdP's details.

You can do this by either importing your IdP's SAML metadata, or by entering your IdP's details manually.

Realm Name: ADFS

IdP Endpoint Address: https://youridentityprovidersssoendpointuri.co.nz

Group Attribute: n4l_cws_groups

IdP Signing Certificate

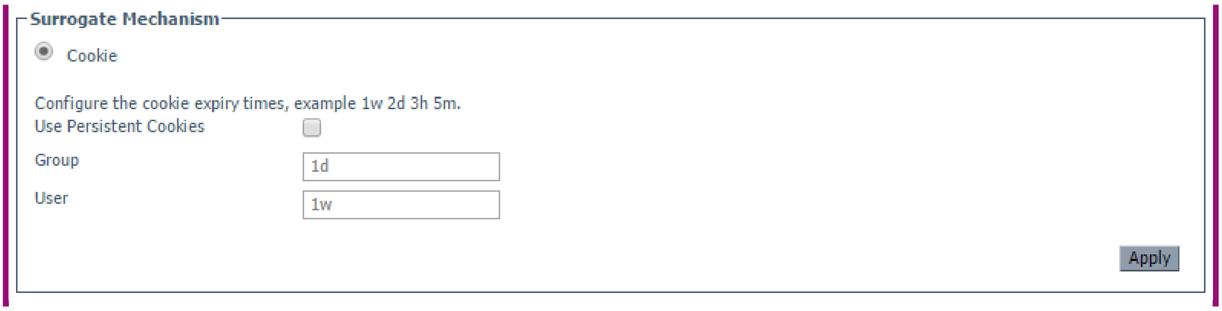
Certificate Subject	Expiry date	Remove
CN=n4ltestschool-N4L-TLAB-DC01-CA, DC=n4ltestschool, DC=local	03/10/2040 23:18:18 UTC	🗑

Upload a signing certificate in DER or PEM form: Choose File No file chosen

4.3 It is your responsibility to ensure that user data transferred over SAML contains only relevant information for the purpose of web filtering, such as web filtering groups and a human readable unique identifier supplied in the **SAML NameID** attribute field. This unique identifier could be an email address or other unique identifier.

The user's **NameID** value will be used to identify users within web filtering reports, therefore supplying the default hashed **NameID** value would make reporting on user activity extremely difficult.

5. In the **Surrogate Mechanism** section you have the option to define the **Cookie Expiry** times.



Surrogate Mechanism

● Cookie

Configure the cookie expiry times, example 1w 2d 3h 5m.

Use Persistent Cookies □

Group 1d

User 1w

Options:

- By default a cookie is non-persistent meaning that it will expire when the browser is closed down.
- You may choose to force users to authenticate daily, meaning a one-day cookie expiry may be considered.
- If you prefer you can set a cookie to be persistent. This means that all users on the device sharing the same profile will effectively be logged in for the lifetime of the cookie.
- Long session times could be used, however if a user ever needed to be logged out or suspended, cookies would need to be manually deleted using ‘behind the scenes’ features of each browser.

Note: In order to implement Individualised Filtering the user agent must support cookies. There are many applications (non-browser based) which will not support user authentication. The web filtering rules are flexible enough to allow a mixture of authenticated browser access and non-authenticated “other” application access. As an example, this would allow a school to permit access from an iPad to the TVNZ OnDemand app but block access to the Facebook or YouTube apps.

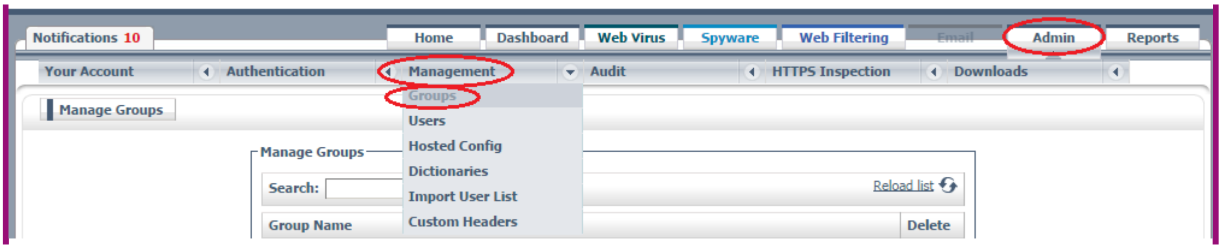
If you have not yet completed the training material, a full set of resources are available on the N4L website. The material covers web filtering, filters, schedules, rules and policy creation.

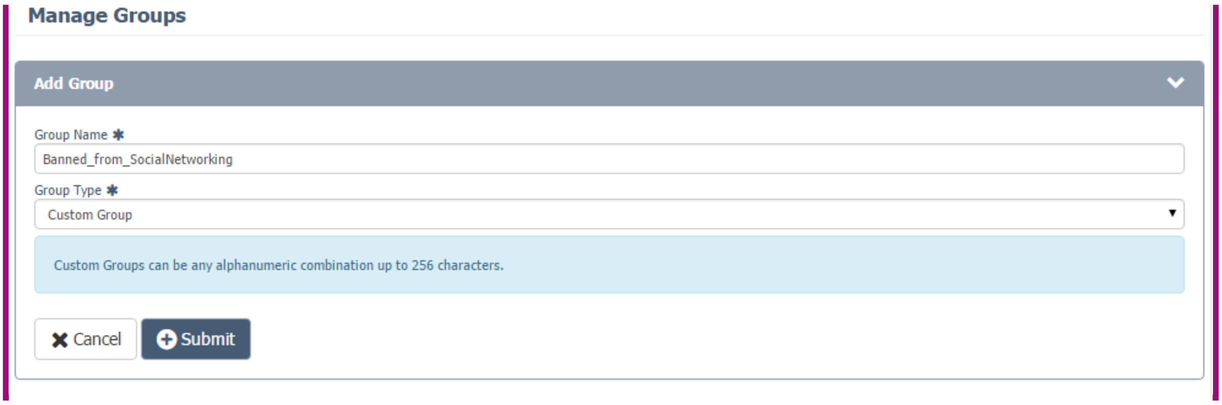
6.3.4. Creating SAML Groups

1. Log into your N4L Web Filtering Dashboard

2. Click on the **Admin** tab

3. Choose **Groups** from the **Management** dropdown menu





Group Name ✱
Banned_from_SocialNetworking

Group Type ✱
Custom Group

Custom Groups can be any alphanumeric combination up to 256 characters.

4. To add a group:

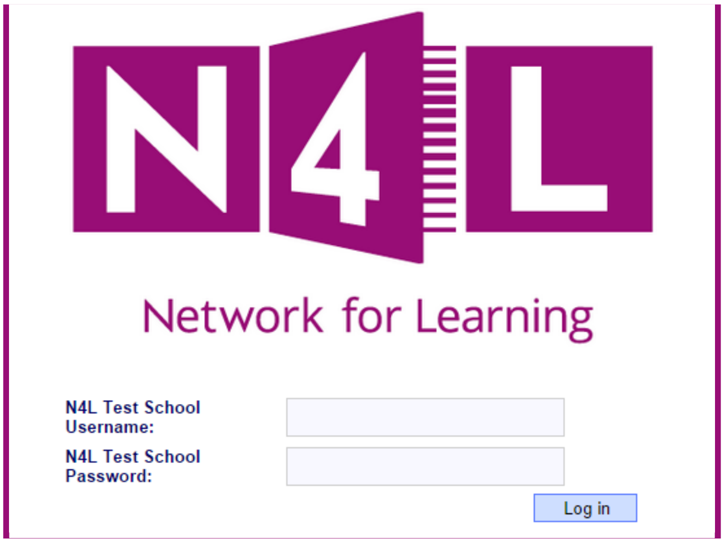
   4.3. Click **Add Group**
   4.4. Enter the **Group Name** as found in your SAML Identity Provider system
   4.5. Choose **Customer Group** for the group type.

5. Once you have created your Groups they can later be referenced when creating web filtering filters which are discussed later in this guide.

6.3.5. Creating an EasyID Login Screen (AD/LDAP only)

You may create a custom login screen

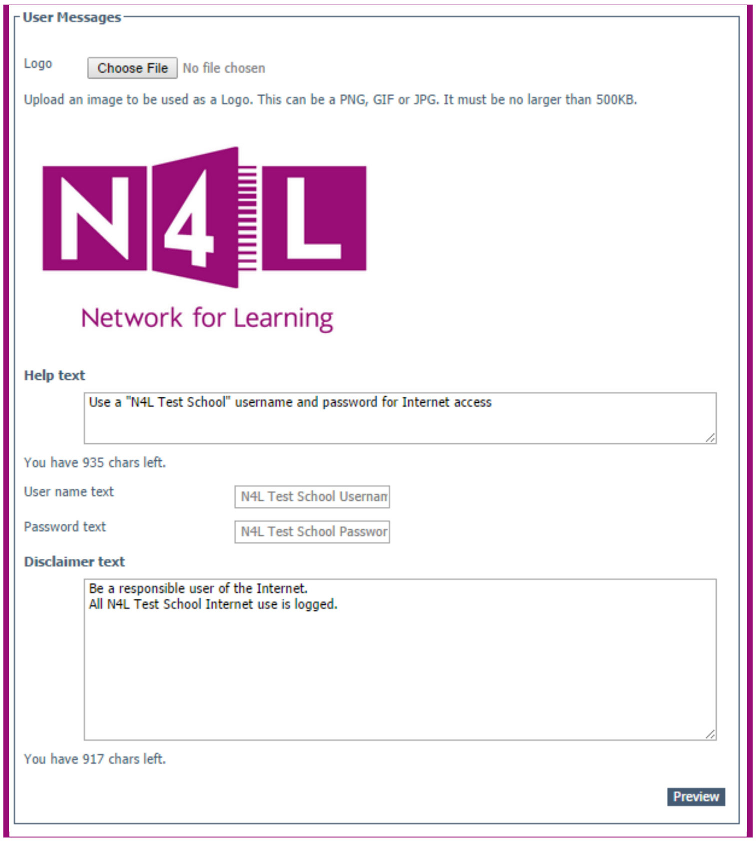
EXAMPLE:



Here you can define:

- A custom graphic to place at the top of the screen, and
- Custom text that will be displayed to all users

1. Log into your N4L Web Filtering dashboard
2. Click on the **Admin** tab
3. Choose **User Messages** from the **Authentication** dropdown menu



User Messages

Logo Choose File No file chosen

Upload an image to be used as a Logo. This can be a PNG, GIF or JPG. It must be no larger than 500KB.

Network for Learning

Help text

Use a "N4L Test School" username and password for Internet access

You have 935 chars left.

User name text: N4L Test School Usernan

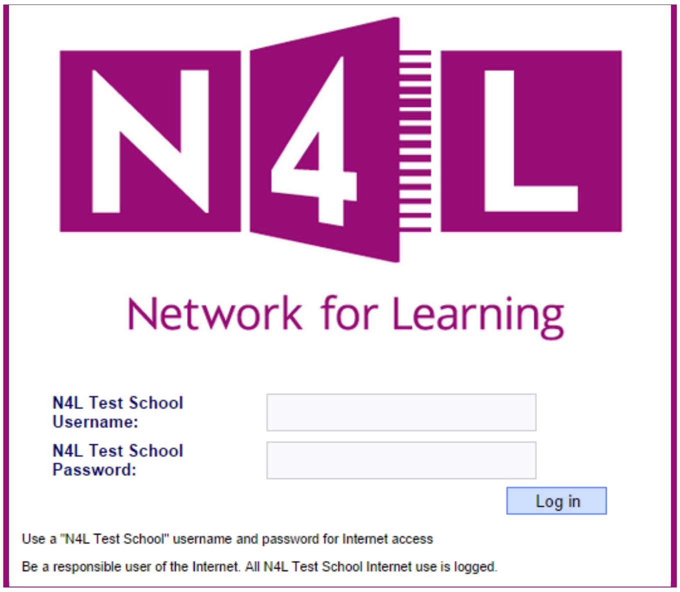
Password text: N4L Test School Passwor

Disclaimer text

Be a responsible user of the Internet.
All N4L Test School Internet use is logged.

You have 917 chars left.

4. Any .jpg, .gif or .png file smaller than 500KB may be used in place of the standard graphic
5. The “Help text”, “User name text”, “Password text” and “Disclaimer text” may all be defined
6. Once defined click “Preview”
7. Save the message by clicking “Apply Settings”



Network for Learning

N4L Test School Username:

N4L Test School Password:

Use a "N4L Test School" username and password for Internet access

Be a responsible user of the Internet. All N4L Test School Internet use is logged.

6.4. Web Filtering Rules

6.4.1 Content Filtering Overview

For detailed training on web filtering, please see the training material on the N4L website. (www.n4l.co.nz/managednetwork/webfiltering/) All schools have a profile in their filtering dashboard.

- A profile is a collection of filtering rules.
- Each profile can have up to 100 rules.
- A **Rule** consists of:
  - **WHAT**: The filter that defines the actual content to be allowed or blocked
  - **WHO**: The group(s) a rule can apply to
  - **WHEN**: The schedule that is chosen to say when the rule will apply

When creating a rule it is strongly advised to have only one “What” filter and only one “When” schedule in a rule. You may have multiple **Who** groups, including the use of exceptions.

All rules must have a **What** and a **When** component.

A **What** filter must be explicitly selected for every rule.

By default the **When** schedule is **anytime** and this may be changed as desired.

The **Who** component of a rule is optional. By default no groups are added meaning the rule will apply to everyone.

Each **Rule** has a **Rule Action** setting:

- **Allow** - Access is allowed, and data is stored for reporting purposes
- **Anonymize** - User, group, internal, and external IP details are replaced with “undisclosed” in reporting data
- **Authenticate** - The user must authenticate
- **Block** - Access is denied
- **Warn** - Access is allowed only if the user clicks through the warning page. You can define the html code that shows on the Acceptable Use Policy page.

Before a rule can be processed it must be made active. This can be done in either the rule definition screen or on the rule summary screen.

The **Rules** are processed in hierarchical order. The order can be updated on the rule summary screen. All changes to **Rules**, including filters, schedules and groups, are updated and available within a few minutes.

The **Child Abuse Content** category: This category is never displayed and the block setting cannot be disabled. All browsing is subject to the Department of Internal Affairs Digital Child Exploitation Filtering.

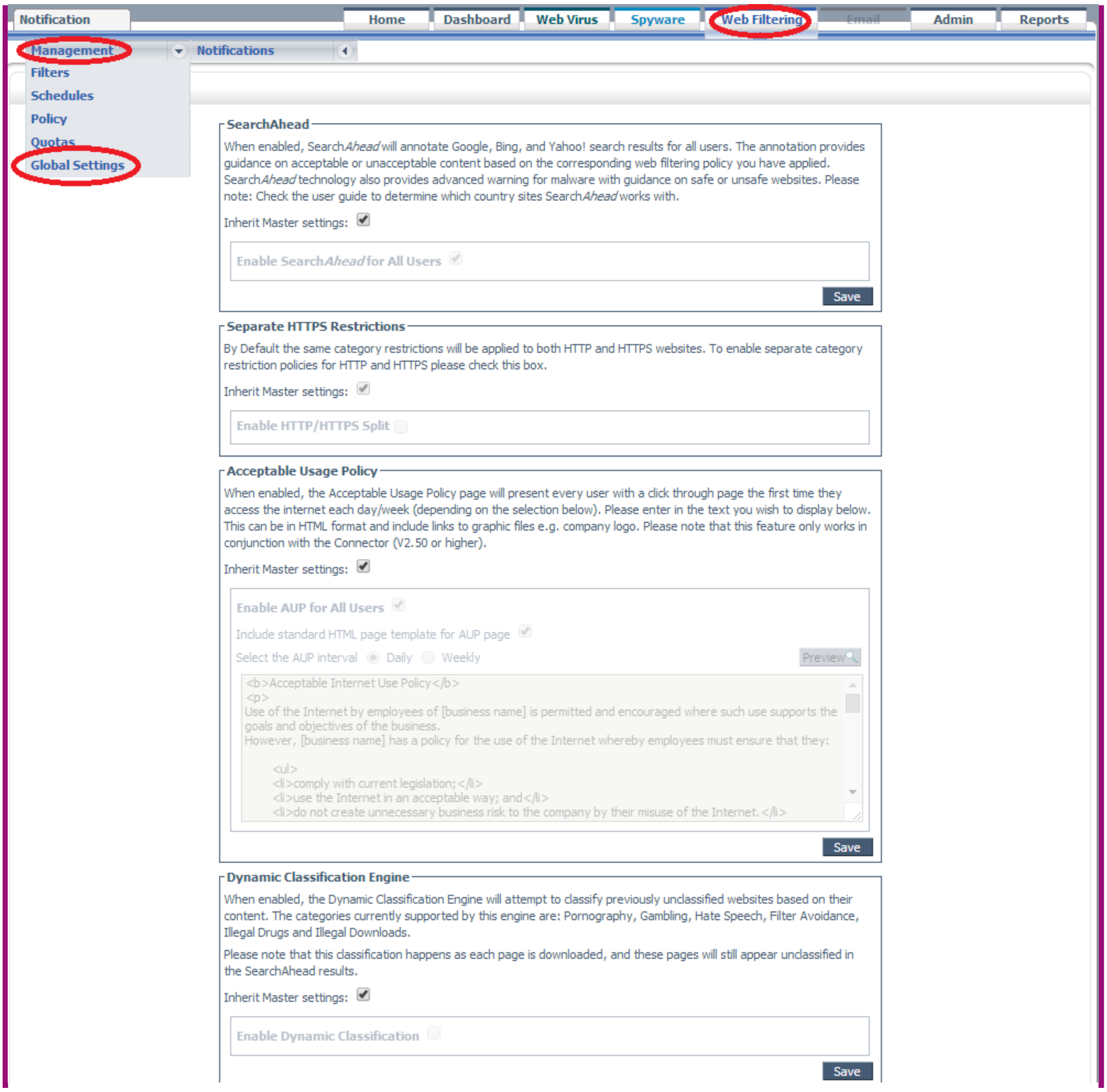
For details about this filter please see: http://www.dia.govt.nz/censorship-dcefs

The **Dynamic Classification Engine** will attempt to classify previously unclassified websites based on their content. Currently the categories that are supported by the Dynamic

Classification Engine are *Pornography, Gambling, Hate Speech, Filter Avoidance, Illegal Drugs and Illegal Downloads.*

Schools may choose to enable or disable the **Dynamic Classification Engine**, along with a range of other features:

1. Log into your N4L Web Filtering dashboard
2. Click on the **Web Filtering** tab
3. Choose **Global Settings** from the **Management** dropdown menu



SearchAhead

When enabled, Search*Ahead* will annotate Google, Bing, and Yahoo! search results for all users. The annotation provides guidance on acceptable or unacceptable content based on the corresponding web filtering policy you have applied. Search*Ahead* technology also provides advanced warning for malware with guidance on safe or unsafe websites. Please note: Check the user guide to determine which country sites Search*Ahead* works with.

Inherit Master settings: ☑

Enable Search*Ahead* for All Users ☑

Save

Separate HTTPS Restrictions

By Default the same category restrictions will be applied to both HTTP and HTTPS websites. To enable separate category restriction policies for HTTP and HTTPS please check this box.

Inherit Master settings: ☑

Enable HTTP/HTTPS Split ☐

Acceptable Usage Policy

When enabled, the Acceptable Usage Policy page will present every user with a click through page the first time they access the internet each day/week (depending on the selection below). Please enter in the text you wish to display below. This can be in HTML format and include links to graphic files e.g. company logo. Please note that this feature only works in conjunction with the Connector (V2.50 or higher).

Inherit Master settings: ☑

Enable AUP for All Users ☑

Include standard HTML page template for AUP page ☑

Select the AUP interval ● Daily ○ Weekly

Preview

```
<b>Acceptable Internet Use Policy</b>
<p>
Use of the Internet by employees of [business name] is permitted and encouraged where such use supports the
goals and objectives of the business.
However, [business name] has a policy for the use of the Internet whereby employees must ensure that they:

        <ul>
        <li>comply with current legislation;</li>
        <li>use the Internet in an acceptable way; and</li>
        <li>do not create unnecessary business risk to the company by their misuse of the Internet.</li>
```

Save

Dynamic Classification Engine

When enabled, the Dynamic Classification Engine will attempt to classify previously unclassified websites based on their content. The categories currently supported by this engine are: Pornography, Gambling, Hate Speech, Filter Avoidance, Illegal Drugs and Illegal Downloads.

Please note that this classification happens as each page is downloaded, and these pages will still appear unclassified in the SearchAhead results.

Inherit Master settings: ☑

Enable Dynamic Classification ☐

Save

6.4.1.1. “Who” Groups

All **Who** groups should be defined as described earlier:

1. Log into your N4L Web Filtering dashboard
2. Click on the **Admin** tab
3. Choose **Groups** from the **Management** dropdown menu

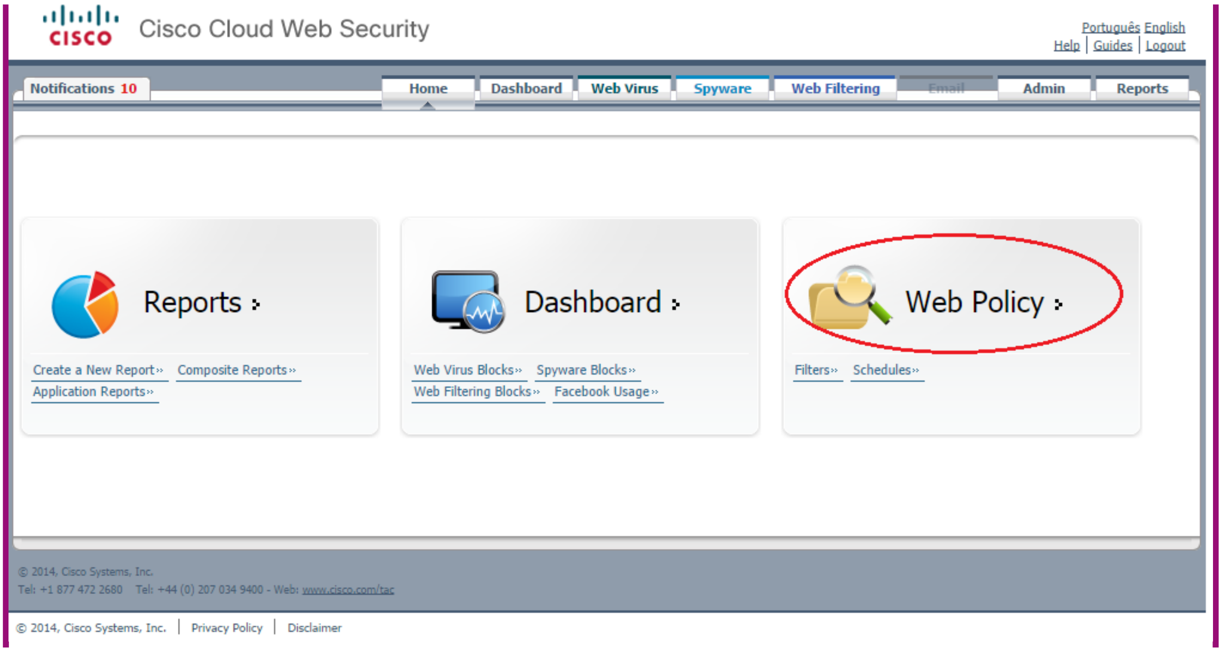
It is possible to manually add users and place these users in custom groups. This document is focussing on users and groups defined by LDAP so it will not be covered here.

6.4.1.2. “What” Filters

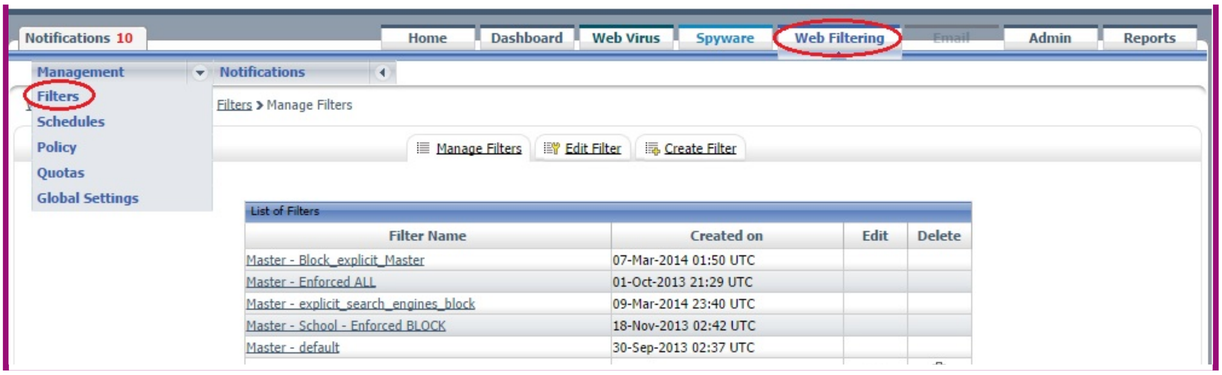
What filter rules are the core of the dashboard. Typically a school will have two predefined **What** filter rules:

- One will be a specific **Allow** filter and
- the other a specific **Block** filter.

1. Log into your N4L Web Filtering dashboard
2. Click on the **Web Policy** icon



3. Choose **Filters** from the **Management** dropdown menu



Filters > Manage Filters

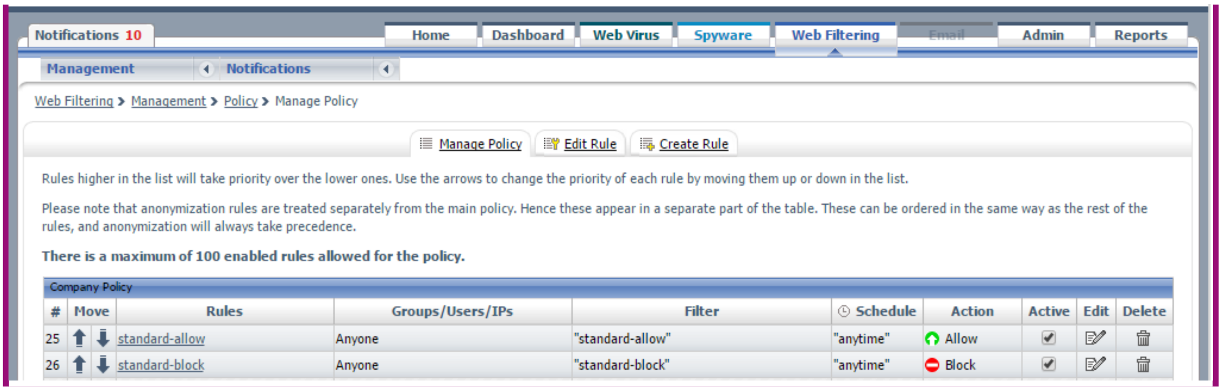
List of Filters

Filter Name	Created on	Edit	Delete
Master - Block_explicit_Master	07-Mar-2014 01:50 UTC		
Master - Enforced ALL	01-Oct-2013 21:29 UTC		
Master - explicit_search_engines_block	09-Mar-2014 23:40 UTC		
Master - School - Enforced BLOCK	18-Nov-2013 02:42 UTC		
Master - default	30-Sep-2013 02:37 UTC		

Please Note:

- A **Rule** may be given the same name as a **Filter**.
- Ensure that you are editing the **Filter** rather than the **Rule**.

The example below shows how **Rules** and **Filters** can have the same name:



Web Filtering > Management > Policy > Manage Policy

Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.

Please note that anonymization rules are treated separately from the main policy. Hence these appear in a separate part of the table. These can be ordered in the same way as the rest of the rules, and anonymization will always take precedence.

There is a maximum of 100 enabled rules allowed for the policy.

Company Policy

#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
25	↑ ↓	standard-allow	Anyone	"standard-allow"	"anytime"	Allow	☑		
26	↑ ↓	standard-block	Anyone	"standard-block"	"anytime"	Block	☑		

- The **Rules** (on the left) have the same names as the **Filters** on the right.
- **Filters** cannot be edited from this screen.
- If you see the above screen when attempting to edit a **Filter** - click on **Filters** in the **Management** dropdown menu as previously described.

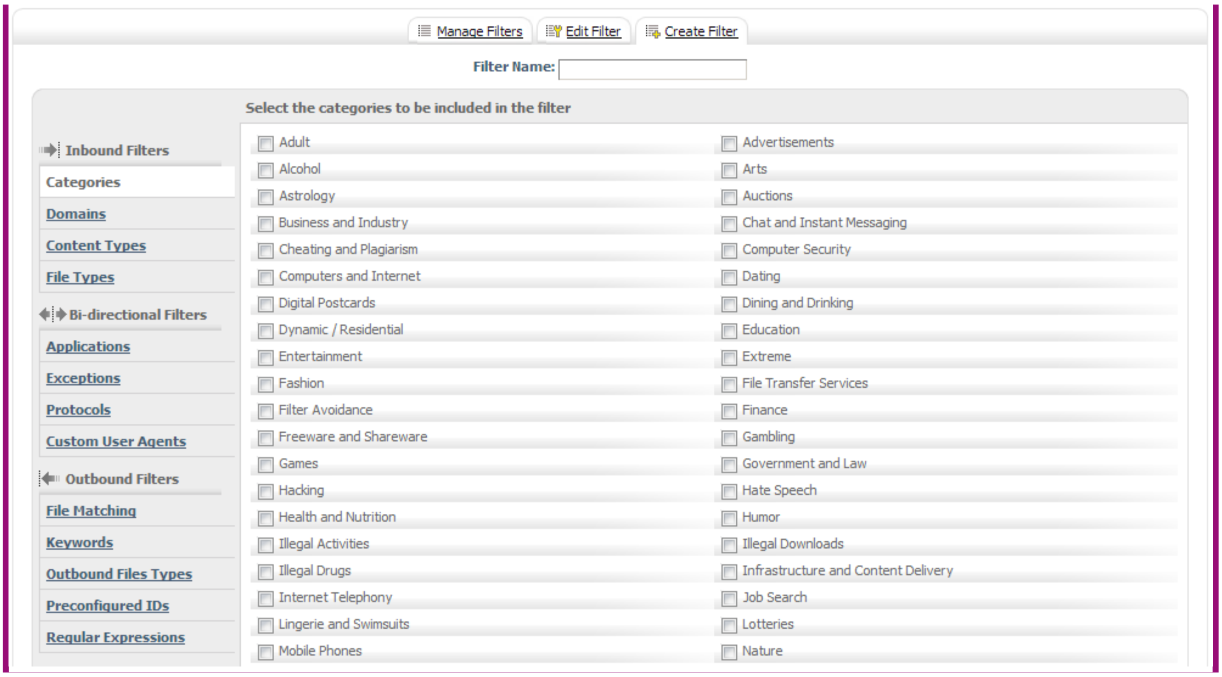
Important reminders:

- Schools may not edit the “Master” filters. The “Master” filters apply to all N4L schools.
- Schools may view the “Master” filters (just click on the filter) to see what is being blocked. If a school needs to allow a site blocked by a “Master” filter then a school will need to create a rule to explicitly allow access..

A filter is a combination of:

- Inbound,
- Bi-directional, and
- Outbound filters

A filter is then set to “Allow”, “Block” (or other action as defined earlier) by the rule that it is a part of.



Manage Filters | Edit Filter | Create Filter

Filter Name:

Inbound Filters
- Categories
- Domains
- Content Types
- File Types

Bi-directional Filters
- Applications
- Exceptions
- Protocols
- Custom User Agents

Outbound Filters
- File Matching
- Keywords
- Outbound Files Types
- Preconfigured IDs
- Regular Expressions

Select the categories to be included in the filter

□ Adult	□ Advertisements
□ Alcohol	□ Arts
□ Astrology	□ Auctions
□ Business and Industry	□ Chat and Instant Messaging
□ Cheating and Plagiarism	□ Computer Security
□ Computers and Internet	□ Dating
□ Digital Postcards	□ Dining and Drinking
□ Dynamic / Residential	□ Education
□ Entertainment	□ Extreme
□ Fashion	□ File Transfer Services
□ Filter Avoidance	□ Finance
□ Freeware and Shareware	□ Gambling
□ Games	□ Government and Law
□ Hacking	□ Hate Speech
□ Health and Nutrition	□ Humor
□ Illegal Activities	□ Illegal Downloads
□ Illegal Drugs	□ Infrastructure and Content Delivery
□ Internet Telephony	□ Job Search
□ Lingerie and Swimsuits	□ Lotteries
□ Mobile Phones	□ Nature

Inbound Filters:

- **Categories**: Any or none of 78 different categories can be selected. A full description of each category is available on our website at: http://www.n4l.co.nz/managednetwork/contentfilteringcategories/
- **Domains**: Place each domain or URL (omit the protocol http:// or https://) on its own line. Subdomains and paths are permitted. Network addresses or ranges are permissible (e.g. 17.0.0.0/8 or 8.8.8.8 etc).
- **Content Types**: You may select common applications, audio, video or image types. You may define custom MIME types.
- **File Types**: File types from a popular range of extensions can be selected or you can add your own custom file types.

Bi-directional filters:

- **Application**s: Specific applications or parts of applications can be selected eg Facebook Video Chat, iTunes Music or Google+ Hangouts.
- **Exceptions**: Specific domains or networks can be entered here that act as exceptions to any categories or domains selected as a part of the Inbound Filter rules.
- **Protocols**: FTP over HTTP, HTTP or HTTPS protocols can be selected.
- **Custom User Agents**: a user agent is any application that can access the internet. This could be a web browser or an application like Skype, iTunes or a media player. Common browser types are listed. Be wary if using a wildcard (e.g. “*” as a custom user agent as this selects any user agent).

Outbound Filters:

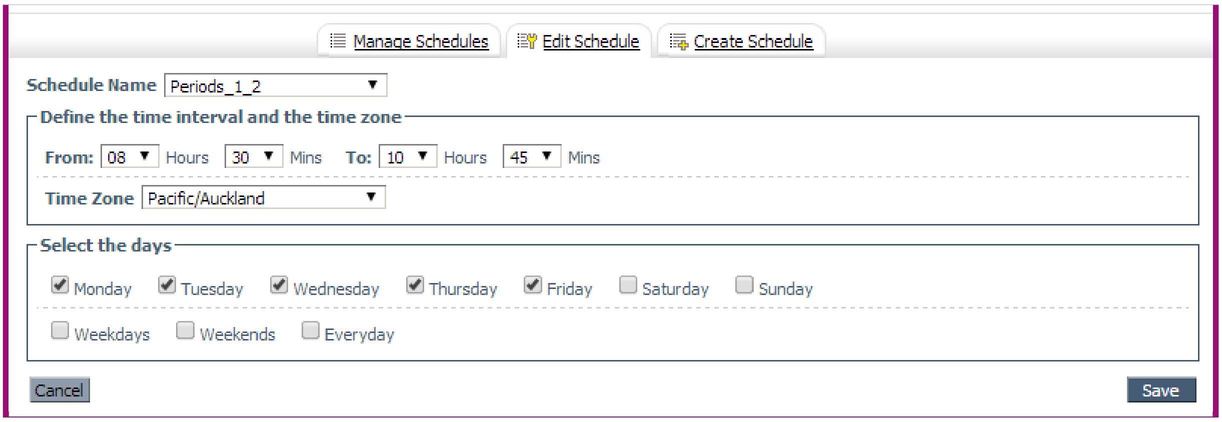
- **File Matching**: You must first have created a file information database via the “Admin”, “Management”, “File Info DBs” menu. This could be used to filter for words within files.
- **Keywords**: You must first have created a dictionary of words via the “Admin”, “Management”, “Dictionaries” menu. This could be used to filter words used on search web sites.

- **Outbound File Types**: file types from a popular range of extensions can be selected or you can add your own custom file types.
- **Preconfigured IDs**: this can be used to prevent (or permit) the use of identity information (e.g. a credit card) on a website.
- **Regular Expressions**: specific patterns of symbols, letters and numbers can be matched.

6.4.1.3. “When” Schedules

To access a **Schedule**:

1. Log into your N4L Web Filtering dashboard
2. Click on the **Web Filtering** tab
3. Choose **Schedules** from the **Management** dropdown menu



Schedule Name: Periods_1_2

Define the time interval and the time zone

From: 08 Hours 30 Mins To: 10 Hours 45 Mins

Time Zone: Pacific/Auckland

Select the days

☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday □ Sunday

□ Weekdays □ Weekends □ Everyday

Notes:

- A schedule can be any time period on any day. The time period can run overnight from (e.g. 23:00 to 06:00). Schedules use 15 minute boundaries only.
- A schedule can contain only one time period but it can be replicated over several days.
- Schedules are easiest to use if a rule only contains one schedule
- Remember time zones

7. Case Study from Mt Aspiring College supplied by Tim Harper

The best way to demonstrate Secure Website Inspection and Individualised Filtering is to show a highly customised example from a real school.

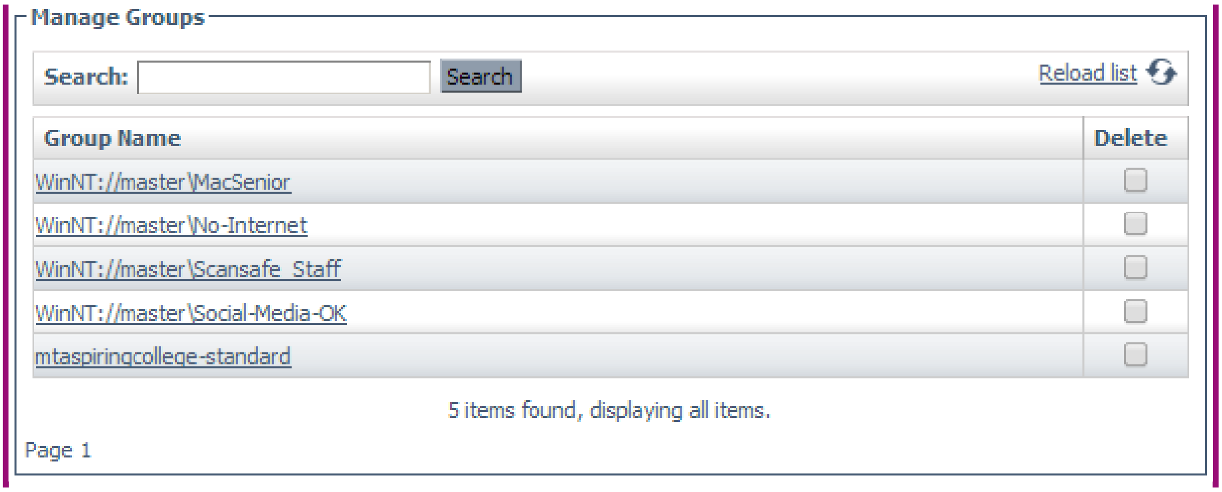
At Mt Aspiring College the web use policy was defined as:

- Staff: able to access most of the internet except for categories deemed as objectionable (e.g. Pornography) at any time.
- Banned Students: unable to access the internet at any time.
- Privileged Students: able to access most of the internet except for objectionable sites. Game sites may not be accessed during class time. Social networking (eg Facebook), streaming media (eg YouTube) and auction sites (eg TradeMe) may be accessed in class time as their course work requires it – (e.g. Young Enterprise, Music, Drama etc).
- Standard Students: able to access most of the internet except for objectionable sites. Sites classified as games, social networking, streaming media or auction sites may not be accessed during class time but are accessible before school, interval, lunch and after school.
- No students can access sites classified as games, social networking, streaming video or auction sites during hostel prep times (Tuesday and Thursday from 7pm – 9pm.)
- No students can access the internet between 11pm and 6am. Hostel students need to sleep.

A **Web Filtering** policy / rule set was designed to meet the needs of the school web use policy.

7.1. "Who" Directory Groups

The following groups were established:



Group Name	Delete
WinNT://master\MacSenior	☐
WinNT://master\No-Internet	☐
WinNT://master\Scansafe_Staff	☐
WinNT://master\Social-Media-OK	☐
mtaspiringcollege-standard	☐

5 items found, displaying all items.

Page 1

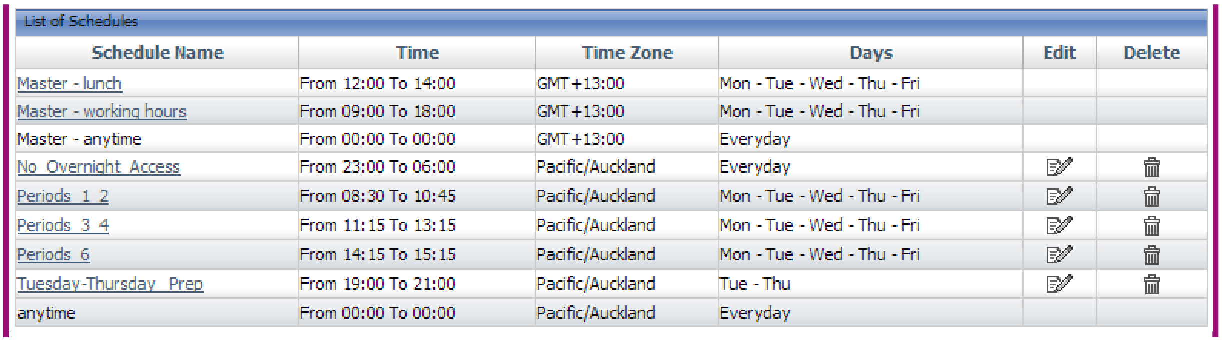
Within Active Directory all users are a member of at least one of the above groups.

- Staff are only members of the "Scansafe_Staff" group.
- All students are members of the "MacSenior" group.

- Students banned from the internet are members of the "MacSenior" and "No-Internet" groups.
- Students with privileges internet are members of the "MacSenior" and "Social-media-OK" groups.
- All users and group memberships are managed via Active Directory.

7.2. "When" Schedules

To fit the time requirements of the web use policy the following schedules were created. The three "Master" and last "Anytime" schedules exist by default.



List of Schedules

Schedule Name	Time	Time Zone	Days	Edit	Delete
Master - lunch	From 12:00 To 14:00	GMT+13:00	Mon - Tue - Wed - Thu - Fri		
Master - working hours	From 09:00 To 18:00	GMT+13:00	Mon - Tue - Wed - Thu - Fri		
Master - anytime	From 00:00 To 00:00	GMT+13:00	Everyday		
No_Overnight_Access	From 23:00 To 06:00	Pacific/Auckland	Everyday	✎	🗑
Periods_1_2	From 08:30 To 10:45	Pacific/Auckland	Mon - Tue - Wed - Thu - Fri	✎	🗑
Periods_3_4	From 11:15 To 13:15	Pacific/Auckland	Mon - Tue - Wed - Thu - Fri	✎	🗑
Periods_6	From 14:15 To 15:15	Pacific/Auckland	Mon - Tue - Wed - Thu - Fri	✎	🗑
Tuesday-Thursday_Prep	From 19:00 To 21:00	Pacific/Auckland	Tue - Thu	✎	🗑
anytime	From 00:00 To 00:00	Pacific/Auckland	Everyday		

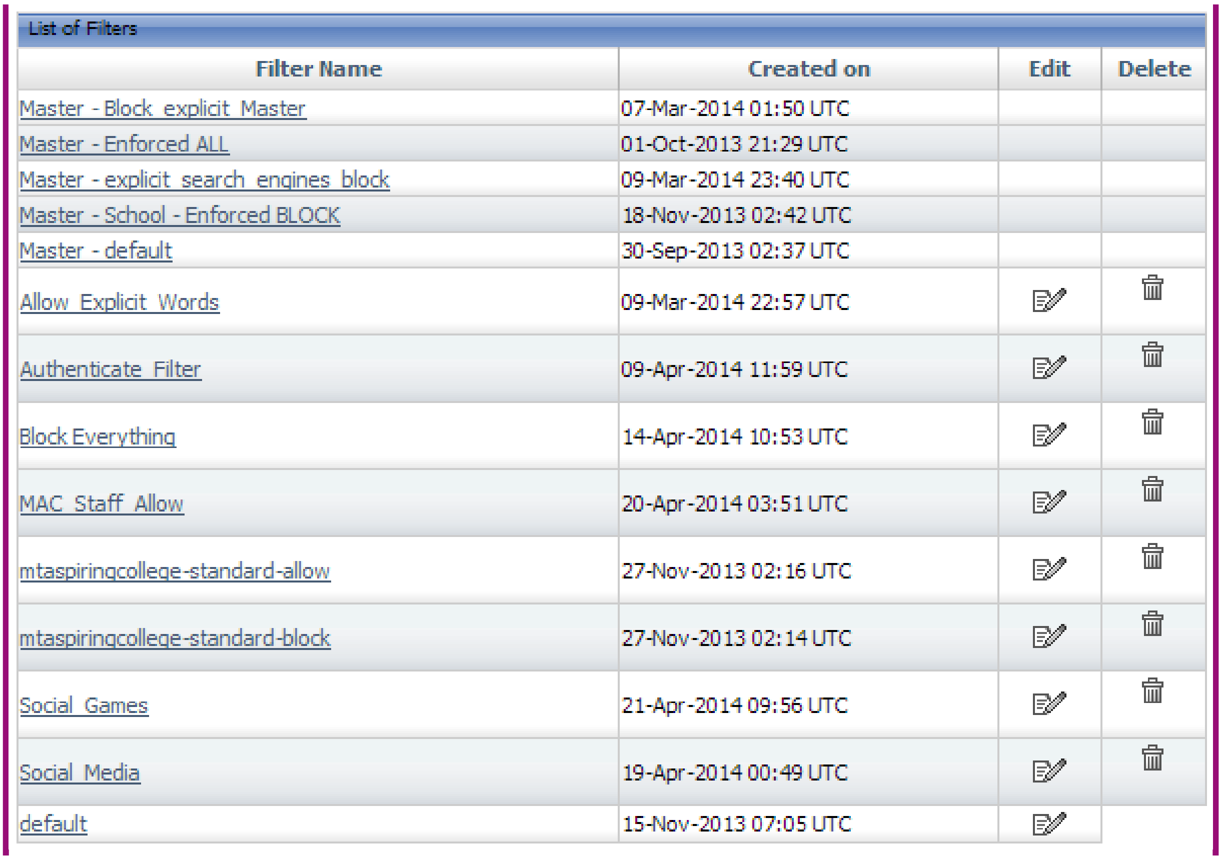
All the schedules were designed to be "best-fit" within the 15 minute boundaries defined by CCWS and the actual period start/finish times used by the school.

7.3. "What" Filters

To fit the **What** requirements of the school's web use policy the filters listed below were created. The five "Master" and last "default" filters exist by default.

The "-standard-allow" and "-standard-block" filters also exist by default and these have been modified to fit the needs of the school.

The "Allow Explicit Words" filter has been created to counter the effects of some of the master filters that prohibit searching for banned words. In particular the school found it necessary to allow search terms that included the words "kill" or "execution" as students were searching for material about "To Kill a Mockingbird" for English or "application execution" for Computer Studies.

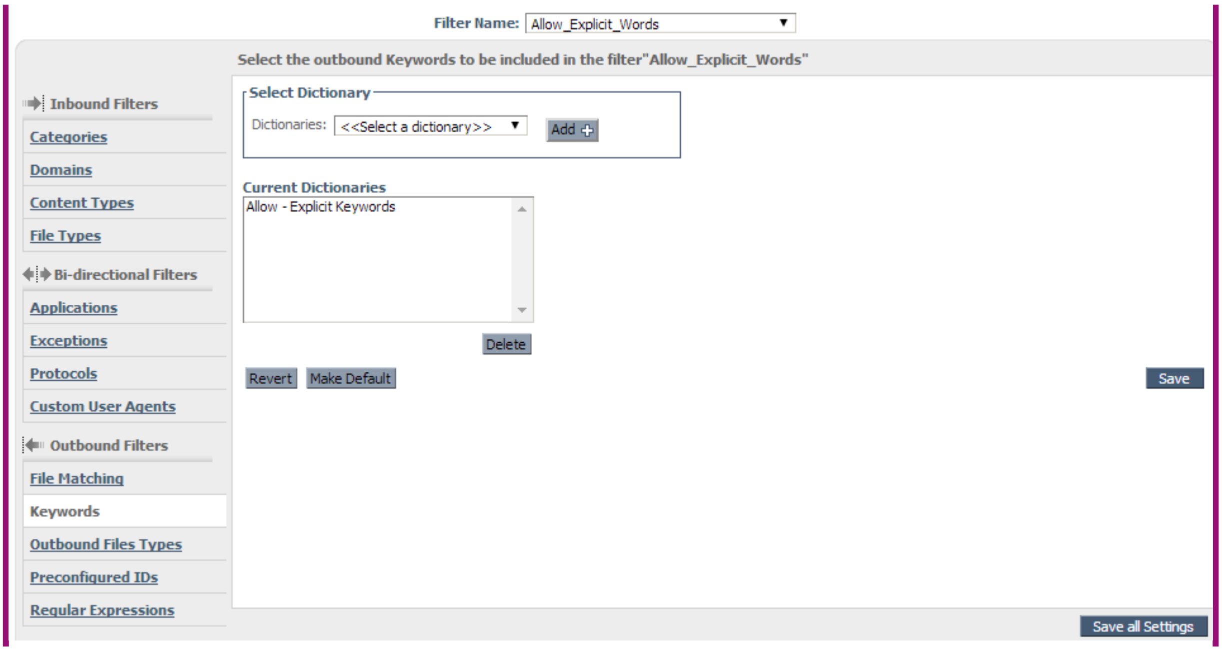


List of Filters

Filter Name	Created on	Edit	Delete
Master - Block explicit Master	07-Mar-2014 01:50 UTC		
Master - Enforced ALL	01-Oct-2013 21:29 UTC		
Master - explicit search engines block	09-Mar-2014 23:40 UTC		
Master - School - Enforced BLOCK	18-Nov-2013 02:42 UTC		
Master - default	30-Sep-2013 02:37 UTC		
Allow Explicit Words	09-Mar-2014 22:57 UTC	✎	🗑
Authenticate Filter	09-Apr-2014 11:59 UTC	✎	🗑
Block Everything	14-Apr-2014 10:53 UTC	✎	🗑
MAC Staff Allow	20-Apr-2014 03:51 UTC	✎	🗑
mtaspiringcollege-standard-allow	27-Nov-2013 02:16 UTC	✎	🗑
mtaspiringcollege-standard-block	27-Nov-2013 02:14 UTC	✎	🗑
Social Games	21-Apr-2014 09:56 UTC	✎	🗑
Social Media	19-Apr-2014 00:49 UTC	✎	🗑
default	15-Nov-2013 07:05 UTC	✎	

Taking each of the above filters in turn:

7.3.1. “Allow Explicit Words” - outbound keyword



Filter Name: Allow_Explicit_Words

Select the outbound Keywords to be included in the filter"Allow_Explicit_Words"

Select Dictionary

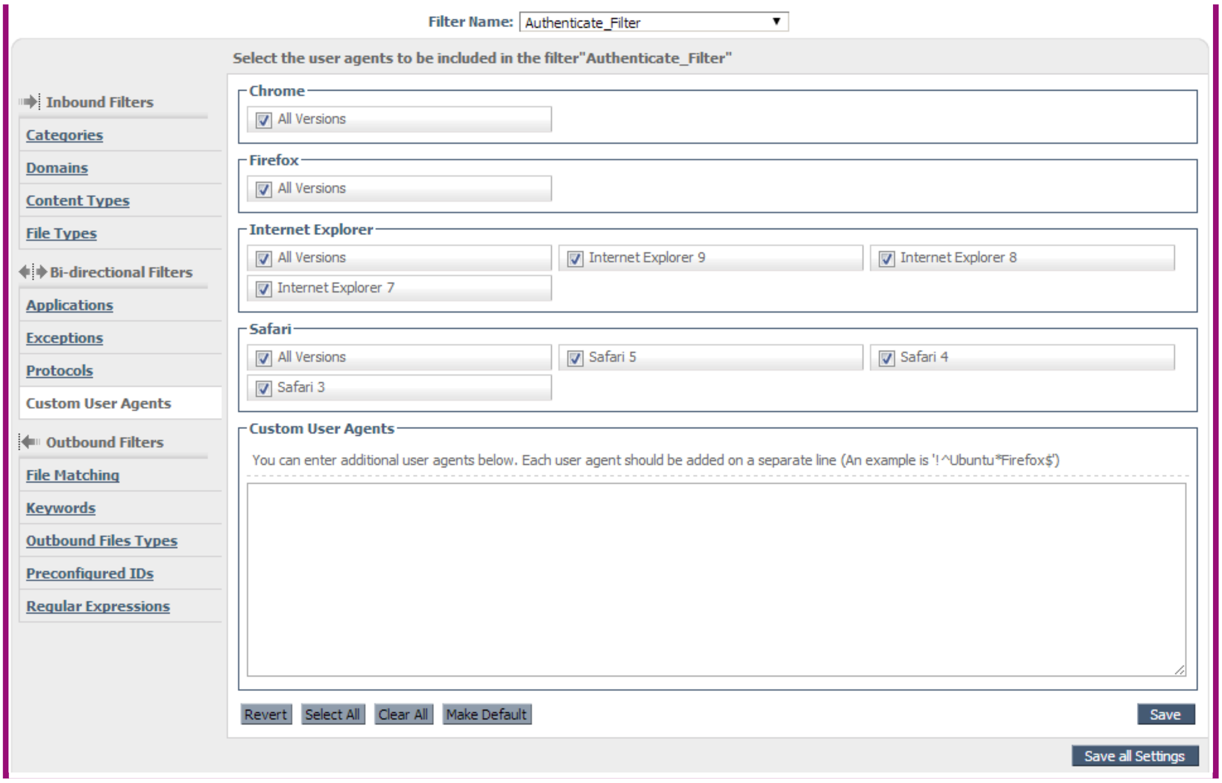
Dictionaries: <<Select a dictionary>>

Current Dictionaries

Allow - Explicit Keywords

The dictionary “Allow – Explicit Keywords” was created from the “Admin”, “Management” menu by choosing “Dictionaries”, adding a new dictionary then manually adding permitted explicit keywords to the dictionary.

7.3.2. “Authenticate Filter” – Bidirectional custom user agent



Filter Name: Authenticate_Filter

Select the user agents to be included in the filter"Authenticate_Filter"

Chrome

☑ All Versions

Firefox

☑ All Versions

Internet Explorer

☑ All Versions ☑ Internet Explorer 9 ☑ Internet Explorer 8 ☑ Internet Explorer 7

Safari

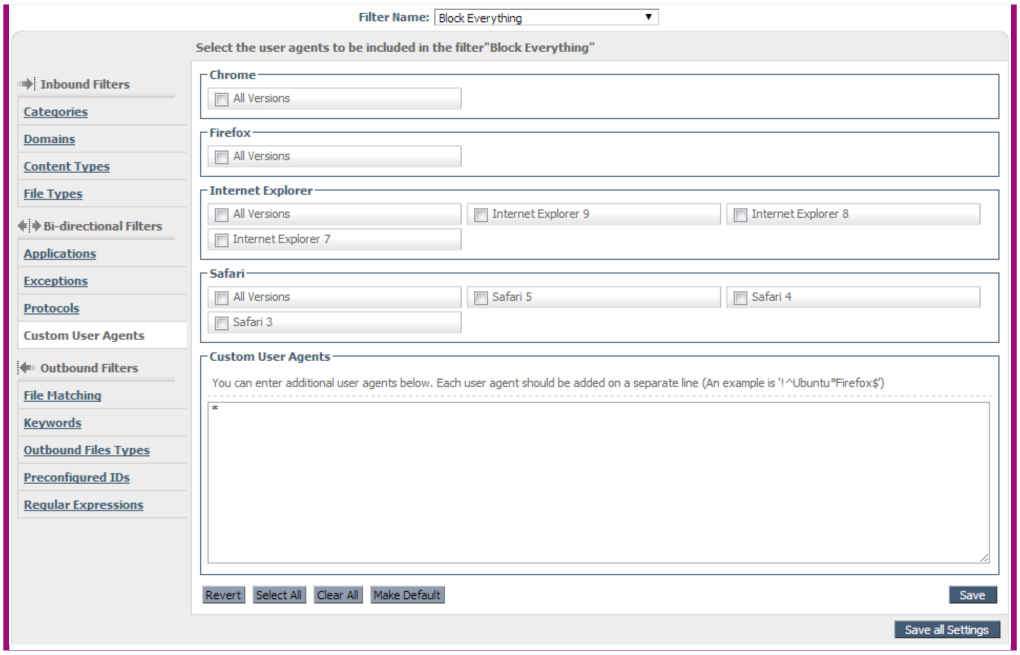
☑ All Versions ☑ Safari 5 ☑ Safari 4 ☑ Safari 3

Custom User Agents

You can enter additional user agents below. Each user agent should be added on a separate line (An example is '! ^Ubuntu*Firefox$')

Only user agents capable of supporting authentication have been referenced. The correct use of this filter in a rule will force all browsers to authenticate but still allow operating system updates, AV updates, Dropbox, Google Drive, SkyDrive, iPad applications (eg TVNZ OnDemand etc) and more to work as intended.

7.3.3. “Block Everything” – Bidirectional custom user agent



Filter Name: Block Everything

Select the user agents to be included in the filter"Block Everything"

Chrome

□ All Versions

Firefox

□ All Versions

Internet Explorer

□ All Versions □ Internet Explorer 9 □ Internet Explorer 8
□ Internet Explorer 7

Safari

□ All Versions □ Safari 5 □ Safari 4
□ Safari 3

Custom User Agents

You can enter additional user agents below. Each user agent should be added on a separate line (An example is '! ^Ubuntu*Firefox$')

```
*
```

This filter is designed to block access for any user agent. It contains just the “*” wildcard character as a custom setting. In reality this filter will only block browsers as it will be used in conjunction with a “Who” filter and any non-authenticating user agent will thus not be subjected to the rule.

If necessary further non-CCWS actions could be taken to remove the device from the school’s network if it is a BYOD device being used for access or the user’s network account could be suspended if access was happening from a school machine.

7.3.4. “MAC Staff Allow” – access to nearly everything is permitted

Inbound Categories: nearly all categories except those deemed to be objectionable are selected.

Inbound Content Types: All content types are selected.

Inbound File Types: All file types are selected.

Bi-directional Applications: All applications (including sub categories) are selected.

Bi-directional Protocols: All protocols are selected.

Bi-directional Custom User Agents: the wildcard “*” is used as a custom user agent.

7.3.5. “-standard-allow” – inbound domains

Inbound Domains: a selection of whitelisted domains and IP ranges that have been requested by teachers have been whitelisted.

7.3.6. “-standard-block” – inbound categories and domains

Inbound Categories: the categories “Alcohol”, “Dynamic / Residential”, “Lingerie and Swimsuits”, “Peer File Transfer”, “Pornography” and “Tobacco” are selected.

Inbound Domains: ask.fm is entered as a domain.

7.3.7. “-standard-block” bidirectional exceptions

Bi-directional Exceptions: a range of useful website that would otherwise be blocked by an inbound category have been entered. For example nzwine.com and feltonroad.com are on the list as these sites are needed for study but would otherwise be blocked by the “Alcohol” category.

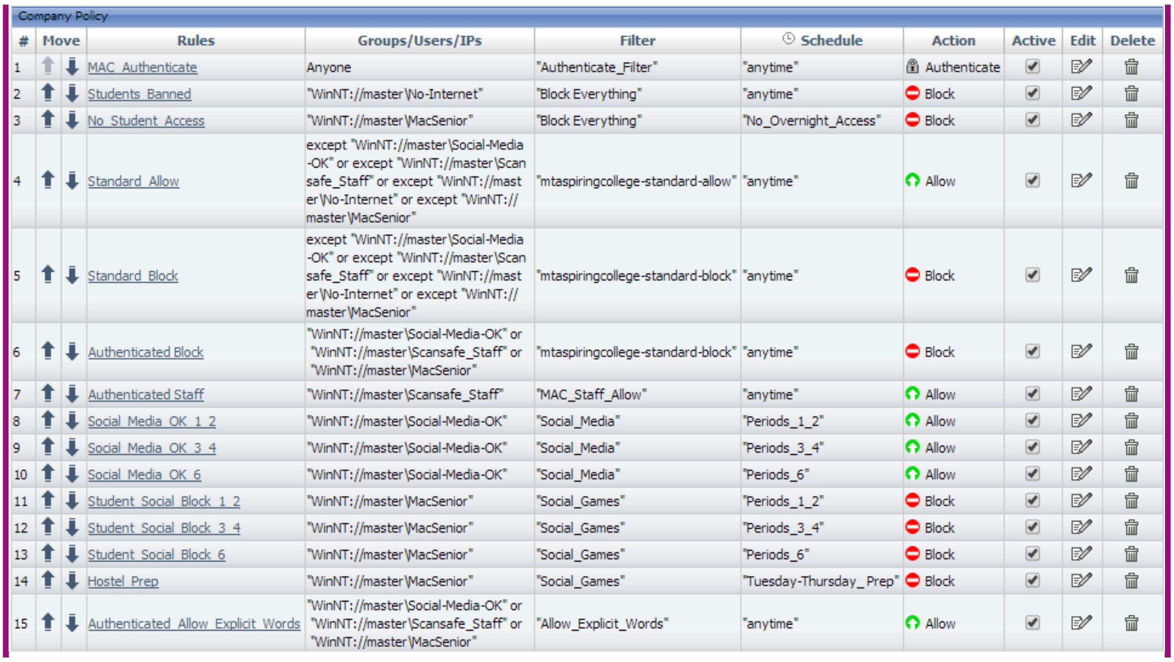
7.3.8. “Social Games” – inbound categories

Inbound Categories: the categories “Auctions”, “Games”, “Social Networking” and “Streaming Video” are selected.

7.3.9. “Social Media” – inbound categories

Inbound Categories: the categories “Auctions”, “Social Networking” and “Streaming Video” are selected.

7.3.10. Policy List: Putting all the Rules together



Company Policy

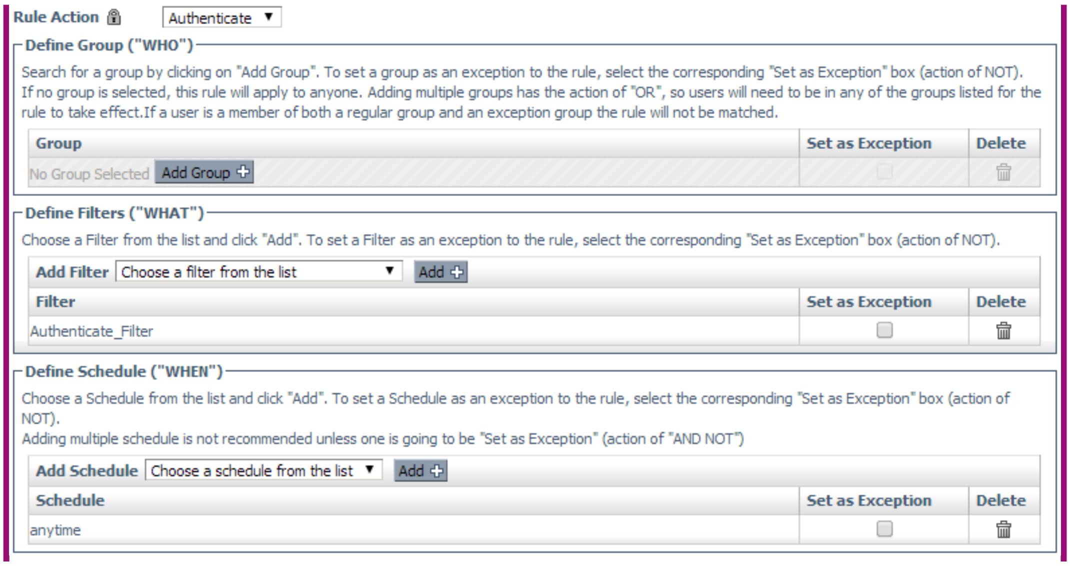
#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
1	↑ ↓	MAC_Authenticate	Anyone	"Authenticate_Filter"	"anytime"	Authenticate	☑	✎	🗑
2	↑ ↓	Students_Banned	"WinNT://master\No-Internet"	"Block Everything"	"anytime"	Block	☑	✎	🗑
3	↑ ↓	No_Student_Access	"WinNT://master\MacSenior"	"Block Everything"	"No_Overnight_Access"	Block	☑	✎	🗑
4	↑ ↓	Standard_Allow	except "WinNT://master\Social-Media-OK" or except "WinNT://master\Scansafe_Staff" or except "WinNT://master\No-Internet" or except "WinNT://master\MacSenior"	"mtaspiringcollege-standard-allow"	"anytime"	Allow	☑	✎	🗑
5	↑ ↓	Standard_Block	except "WinNT://master\Social-Media-OK" or except "WinNT://master\Scansafe_Staff" or except "WinNT://master\No-Internet" or except "WinNT://master\MacSenior"	"mtaspiringcollege-standard-block"	"anytime"	Block	☑	✎	🗑
6	↑ ↓	Authenticated Block	"WinNT://master\Social-Media-OK" or "WinNT://master\Scansafe_Staff" or "WinNT://master\MacSenior"	"mtaspiringcollege-standard-block"	"anytime"	Block	☑	✎	🗑
7	↑ ↓	Authenticated Staff	"WinNT://master\Scansafe_Staff"	"MAC_Staff_Allow"	"anytime"	Allow	☑	✎	🗑
8	↑ ↓	Social_Media_OK_1_2	"WinNT://master\Social-Media-OK"	"Social_Media"	"Periods_1_2"	Allow	☑	✎	🗑
9	↑ ↓	Social_Media_OK_3_4	"WinNT://master\Social-Media-OK"	"Social_Media"	"Periods_3_4"	Allow	☑	✎	🗑
10	↑ ↓	Social_Media_OK_6	"WinNT://master\Social-Media-OK"	"Social_Media"	"Periods_6"	Allow	☑	✎	🗑
11	↑ ↓	Student_Social_Block_1_2	"WinNT://master\MacSenior"	"Social_Games"	"Periods_1_2"	Block	☑	✎	🗑
12	↑ ↓	Student_Social_Block_3_4	"WinNT://master\MacSenior"	"Social_Games"	"Periods_3_4"	Block	☑	✎	🗑
13	↑ ↓	Student_Social_Block_6	"WinNT://master\MacSenior"	"Social_Games"	"Periods_6"	Block	☑	✎	🗑
14	↑ ↓	Hostel_Prep	"WinNT://master\MacSenior"	"Social_Games"	"Tuesday-Thursday_Prep"	Block	☑	✎	🗑
15	↑ ↓	Authenticated_Allow_Explicit_Words	"WinNT://master\Social-Media-OK" or "WinNT://master\Scansafe_Staff" or "WinNT://master\MacSenior"	"Allow_Explicit_Words"	"anytime"	Allow	☑	✎	🗑

The final Web Filtering policy is a list of 15 active rules. A policy can support a maximum of 100 active rules. The rules are processed in hierarchical order – once a rule is matched rule processing ceases and the user is permitted or blocked accordingly.

The policy rules used by Mt Aspiring College also assume that Secure Website Inspection is used to assist the filtering of secured websites eg https://www.facebook.com. The details for each rule in the policy are defined below. For the details on each group that the rule applies to, the filters used and the schedules that apply to the rule please see the details earlier in this document.

i. MAC Authenticate

The purpose of this rule is to force all users with a browser to authenticate at any time of day. No group is defined (meaning the rule will apply to everyone); the filter is “Authenticate Filter” (all browser types selected in as “User Agents”); the schedule is for any time.



Rule Action Authenticate ▼

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
No Group Selected Add Group	□	🗑

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter Choose a filter from the list ▼ Add

Filter	Set as Exception	Delete
Authenticate_Filter	□	🗑

Define Schedule ("WHEN")

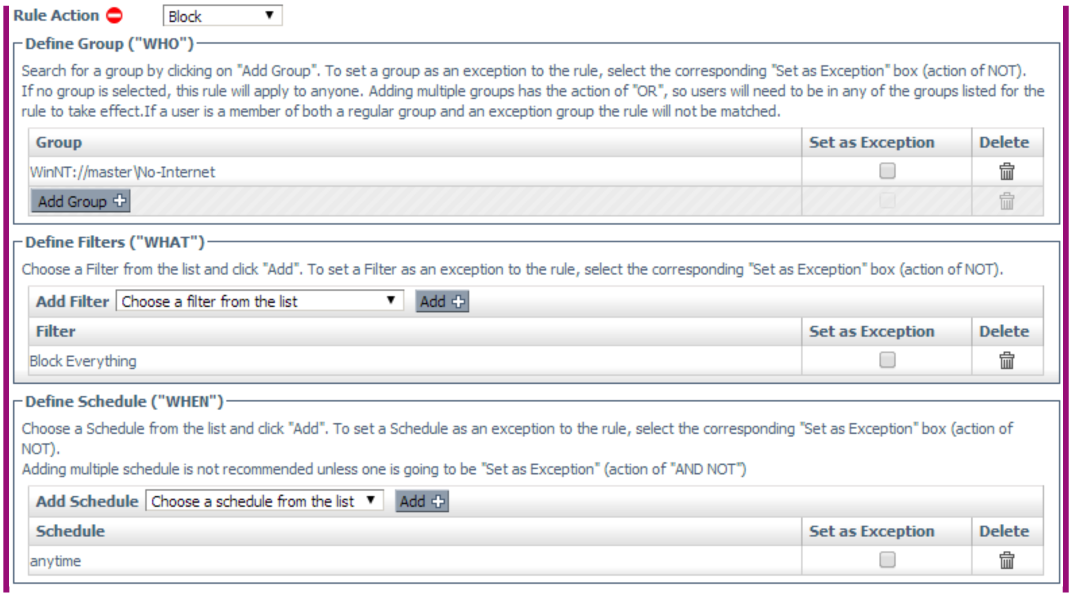
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule Choose a schedule from the list ▼ Add

Schedule	Set as Exception	Delete
anytime	□	🗑

ii. Students Banned

The purpose of this rule is to block students who have been banned from using the internet via a web browser from having access regardless of the time of day. The group defined is “WinNT://master\No-Internet”; the filter is “Block Everything” (all browser types and custom agents are selected); the schedule is for any time.



Rule Action Block ▼

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
WinNT://master\No-Internet	□	🗑
Add Group	□	🗑

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter Choose a filter from the list ▼ Add

Filter	Set as Exception	Delete
Block Everything	□	🗑

Define Schedule ("WHEN")

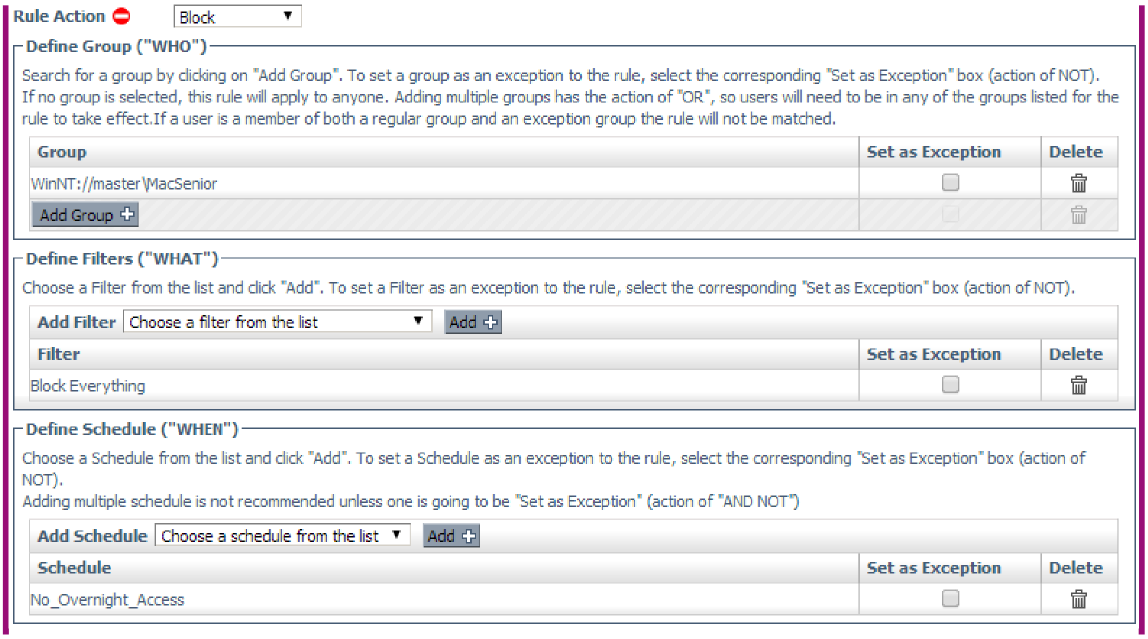
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule Choose a schedule from the list ▼ Add

Schedule	Set as Exception	Delete
anytime	□	🗑

iii. No Student Access

The purpose of this rule is to block students from using the internet via a web browser between 11pm and 6am. The group defined is “WinNT://master\MacSenior”; the filter is “Block Everything” (all browser types and custom agents are selected); the schedule is for “No_Overnight_Access” (11pm – 6am daily).



Rule Action: Block

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
WinNT://master\MacSenior	☐	🗑
Add Group		

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter: Choose a filter from the list — Add

Filter	Set as Exception	Delete
Block Everything	☐	🗑

Define Schedule ("WHEN")

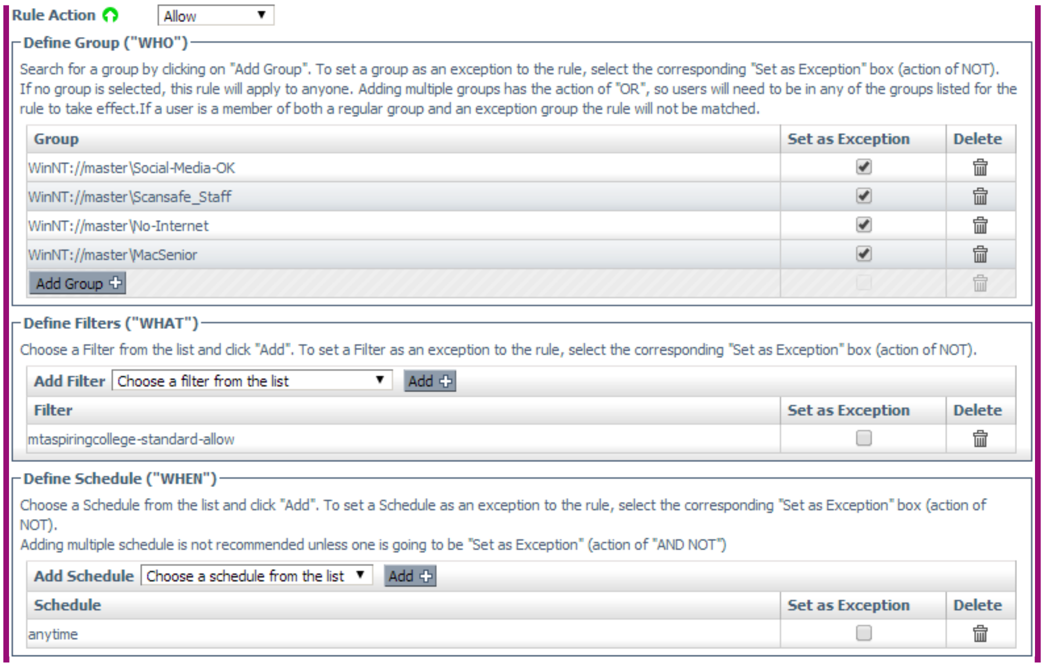
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule: Choose a schedule from the list — Add

Schedule	Set as Exception	Delete
No_Overnight_Access	☐	🗑

iv. Standard Allow

The purpose of this rule is to allow access when no authentication is possible to have a minimum level of access to resources at any time. The groups defined are all the groups as exceptions so this will apply only to unauthenticated users; the filter is “mtaspiringcollege-standard-allow” (a whitelist of domains and network ranges); the schedule is for “anytime”.



Rule Action: Allow

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
WinNT://master\Social-Media-OK	☑	🗑
WinNT://master\Scansafe_Staff	☑	🗑
WinNT://master\No-Internet	☑	🗑
WinNT://master\MacSenior	☑	🗑
Add Group		

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter: Choose a filter from the list — Add

Filter	Set as Exception	Delete
mtaspiringcollege-standard-allow	☐	🗑

Define Schedule ("WHEN")

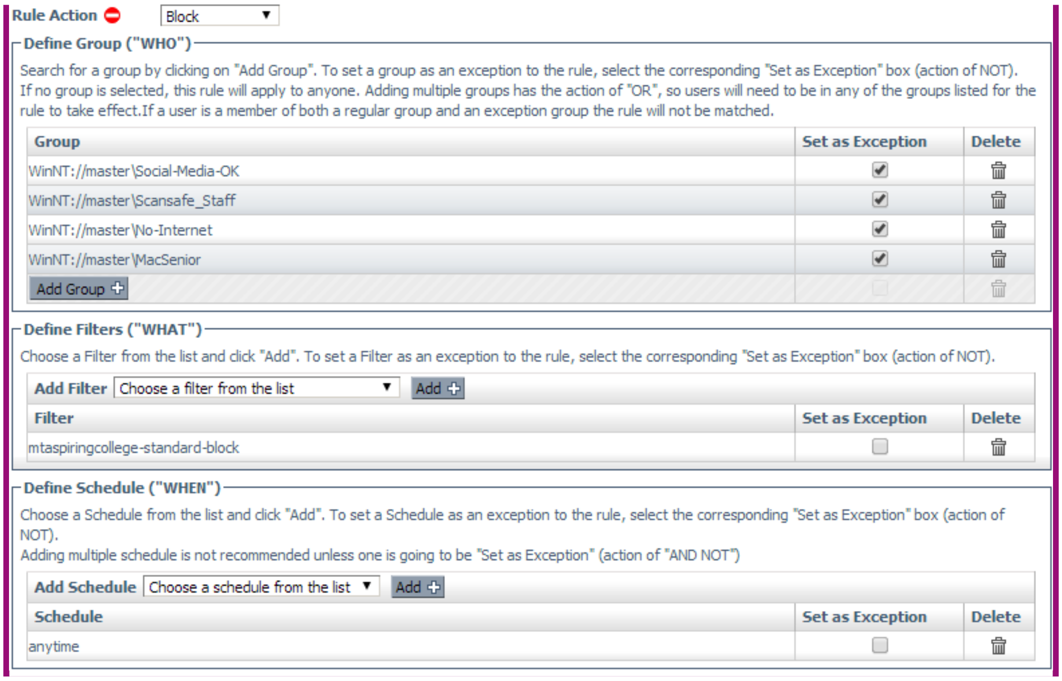
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule: Choose a schedule from the list — Add

Schedule	Set as Exception	Delete
anytime	☐	🗑

v. Standard Block

The purpose of this rule is to block access when no authentication is possible to specified resources at any time. The groups defined are all the groups as exceptions so this will apply only to unauthenticated users; the filter is “mtaspiringcollege-standard-block” (a black list of categories, domains and network ranges; and a white list of exceptions); the schedule is for “anytime”.



Rule Action ⛔ Block ▼

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
WinNT://master\Social-Media-OK	☑	🗑
WinNT://master\Scansafe_Staff	☑	🗑
WinNT://master\No-Internet	☑	🗑
WinNT://master\MacSenior	☑	🗑
Add Group ✚		

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter Choose a filter from the list ▼ Add ✚

Filter	Set as Exception	Delete
mtaspiringcollege-standard-block	□	🗑

Define Schedule ("WHEN")

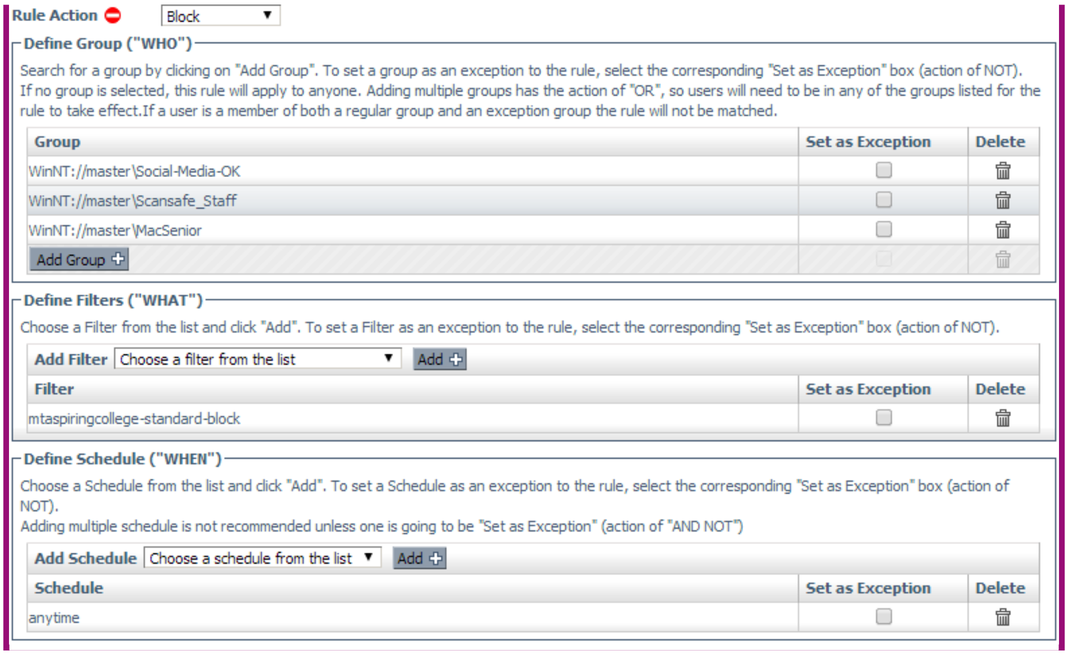
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule Choose a schedule from the list ▼ Add ✚

Schedule	Set as Exception	Delete
anytime	□	🗑

vi. Authenticated Block

The purpose of this rule is to block access when authentication is possible to specified resources at any time. The groups defined are all the groups except the “No-Internet” group; the filter is “mtaspiringcollege-standard-block” (a black list of categories, domains and network ranges; and a white list of exceptions); the schedule is for “anytime”.



Rule Action ⛔ Block ▼

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
WinNT://master\Social-Media-OK	□	🗑
WinNT://master\Scansafe_Staff	□	🗑
WinNT://master\MacSenior	□	🗑
Add Group ✚		

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter Choose a filter from the list ▼ Add ✚

Filter	Set as Exception	Delete
mtaspiringcollege-standard-block	□	🗑

Define Schedule ("WHEN")

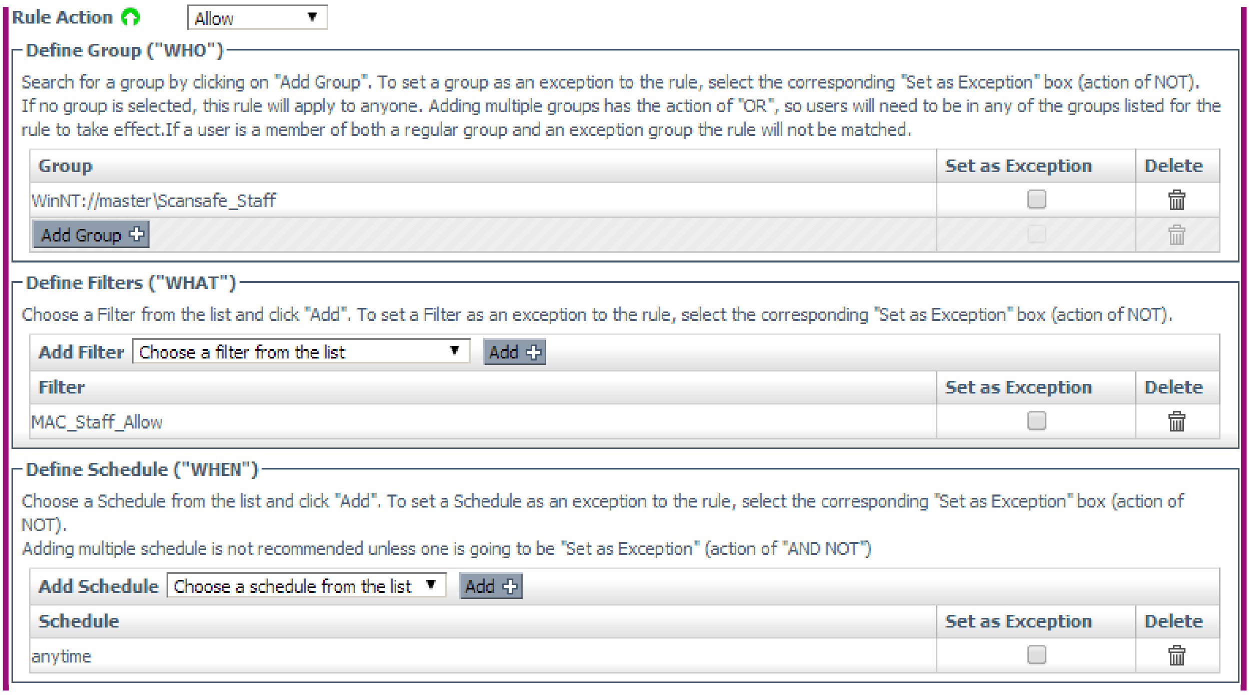
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule Choose a schedule from the list ▼ Add ✚

Schedule	Set as Exception	Delete
anytime	□	🗑

vii. Authenticated Staff

The purpose of this rule is to allow access for staff to all resources at any time. The group defined is “WinNT://master\Scansafe_Staff”; the filter is “MAC_Staff_Allow” (a white list of categories, content and file types, applications and user agents); the schedule is “anytime”.



Rule Action: Allow

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
WinNT://master\Scansafe_Staff	□	🗑
Add Group ✚	□	🗑

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter: Choose a filter from the list ▼ Add ✚

Filter	Set as Exception	Delete
MAC_Staff_Allow	□	🗑

Define Schedule ("WHEN")

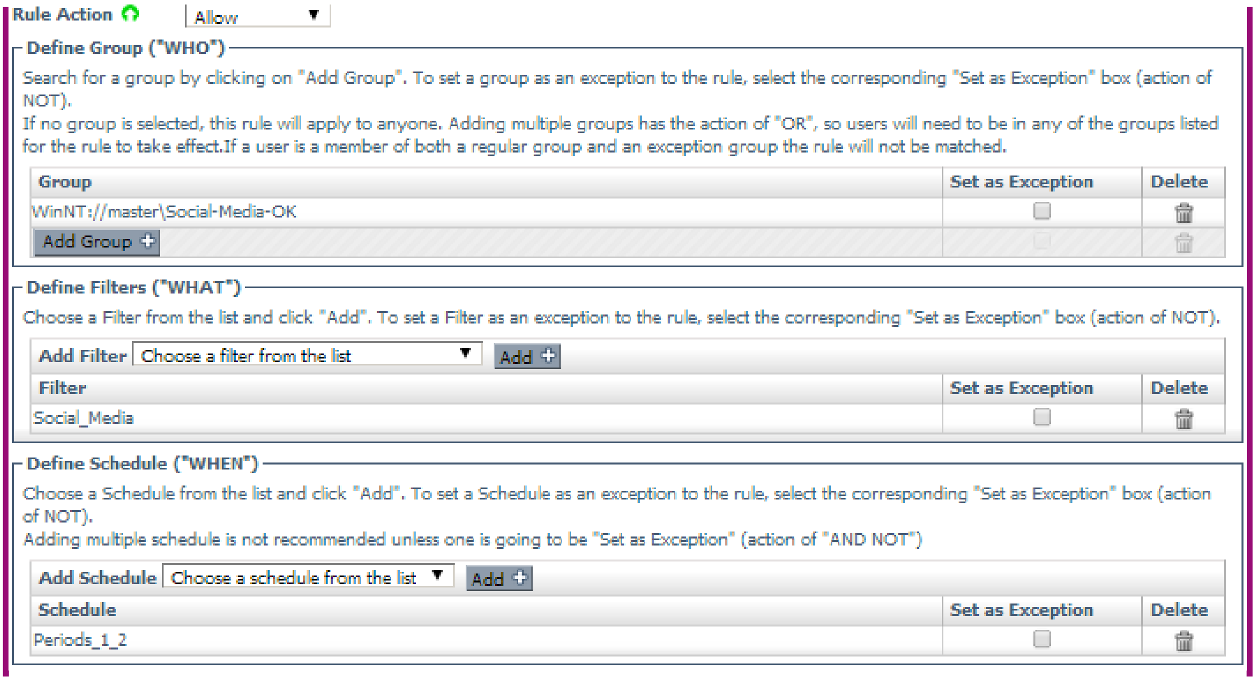
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule: Choose a schedule from the list ▼ Add ✚

Schedule	Set as Exception	Delete
anytime	□	🗑

viii. Social_Media_OK

The purpose of this rule is to allow access for privileged students to social and media sites during class time. The group defined is “WinNT://master\Social_Media_OK”; the filter is “Social_Media” (a white list of categories); the schedule is “Periods_1_2” or “Periods_2_3” or “Periods_6” as required. (There are three separate rules for each scheduled time.)



Rule Action: Allow

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
WinNT://master\Social-Media-OK	□	🗑
Add Group ✚	□	🗑

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter: Choose a filter from the list ▼ Add ✚

Filter	Set as Exception	Delete
Social_Media	□	🗑

Define Schedule ("WHEN")

Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

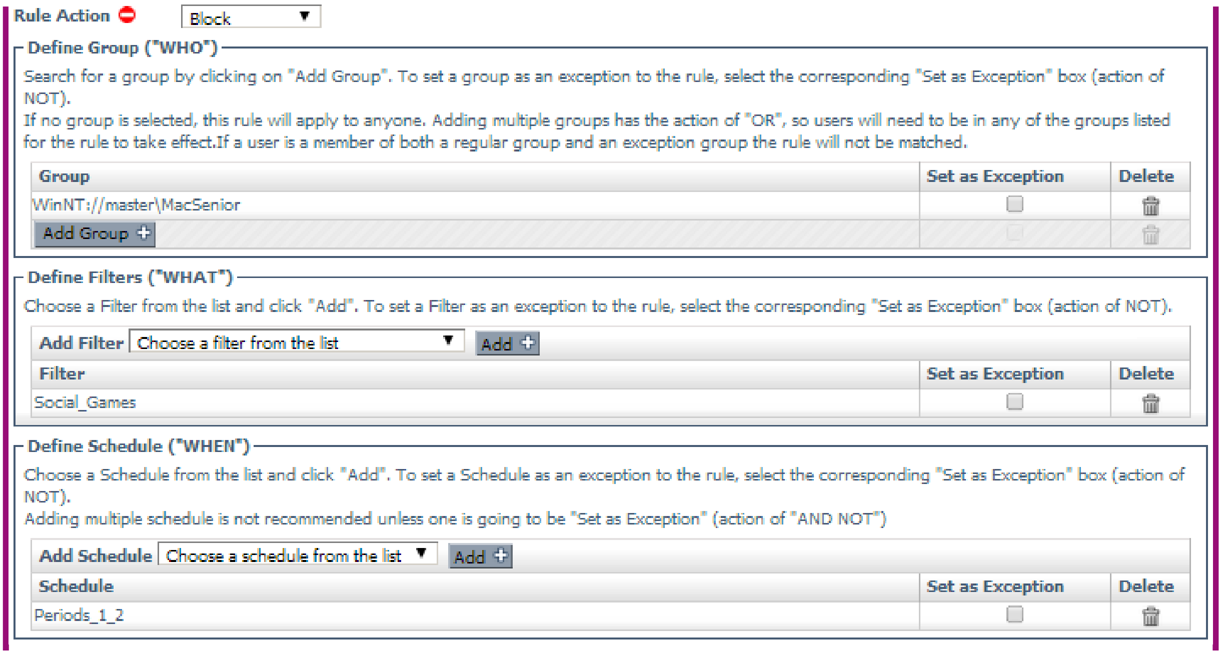
Add Schedule: Choose a schedule from the list ▼ Add ✚

Schedule	Set as Exception	Delete
Periods_1_2	□	🗑

ix. Student_Social_Block

The purpose of this rule is to block access for non-privileged students to social, games and media sites during class time. The group defined is “WinNT://master\MacSenior”; the filter is

"Social_Games" (a black list of categories); the schedule is "Periods_1_2" or "Periods_2_3" or "Periods_6" as required. (There are three separate rules for each scheduled time.)



Rule Action ⛔ Block ▼

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
WinNT://master\MacSenior	□	🗑
Add Group ✚	□	🗑

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter Choose a filter from the list ▼ Add ✚

Filter	Set as Exception	Delete
Social_Games	□	🗑

Define Schedule ("WHEN")

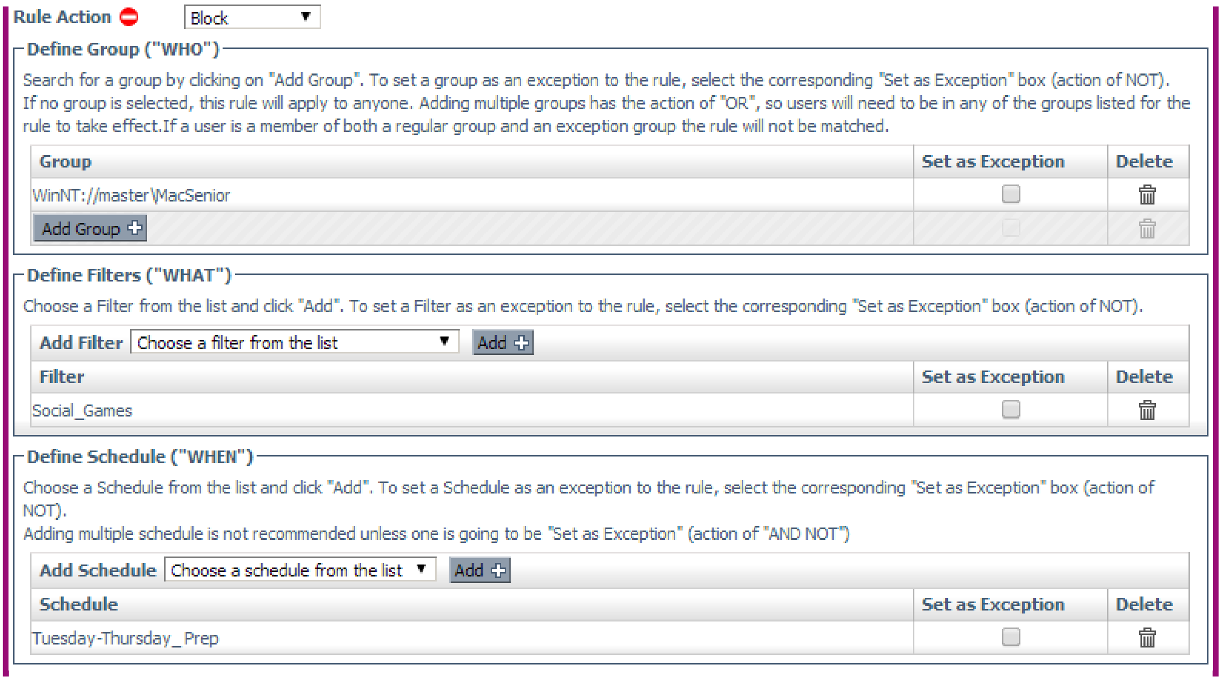
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule Choose a schedule from the list ▼ Add ✚

Schedule	Set as Exception	Delete
Periods_1_2	□	🗑

x. Hostel_Prep

The purpose of this rule is to block access for all students to social, games and media sites during Hostel prep time. The group defined is "WinNT://master\MacSenior"; the filter is "Social_Games" (a black list of categories); the schedule is "Tuesday-Thursday_Prep".



Rule Action ⛔ Block ▼

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
WinNT://master\MacSenior	□	🗑
Add Group ✚	□	🗑

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter Choose a filter from the list ▼ Add ✚

Filter	Set as Exception	Delete
Social_Games	□	🗑

Define Schedule ("WHEN")

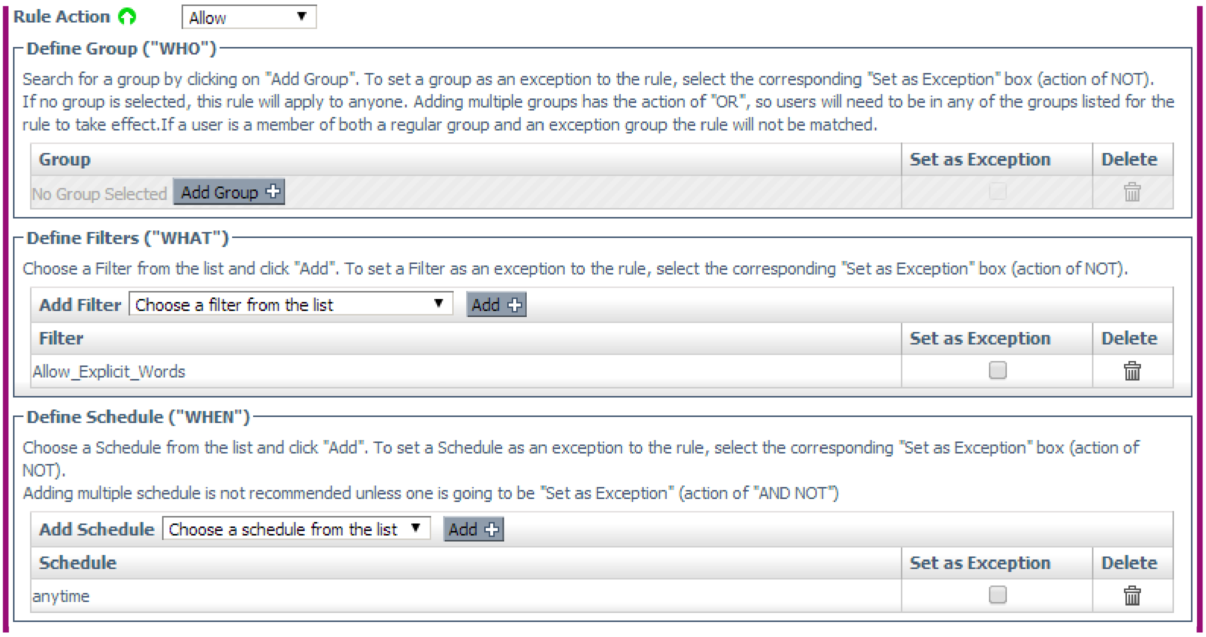
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule Choose a schedule from the list ▼ Add ✚

Schedule	Set as Exception	Delete
Tuesday-Thursday_Prep	□	🗑

xi. Authenticated_Allow_explicit_Words

The purpose of this rule is to allow access for all students to search sites using explicit words at any time. No group is defined (meaning the rule will apply to everyone); the filter is "Allow_Explicit_Words" (a white list of words that are otherwise blocked from searches for all schools eg “kill” as in “to kill a mocking bird” or “execution” as in “application execution” etc); the schedule is “anytime”.



Rule Action: Allow ▼

Define Group ("WHO")

Search for a group by clicking on "Add Group". To set a group as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT). If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as Exception	Delete
No Group Selected Add Group	□	🗑

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).

Add Filter: Choose a filter from the list ▼ Add

Filter	Set as Exception	Delete
Allow_Explicit_Words	□	🗑

Define Schedule ("WHEN")

Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as Exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as Exception" (action of "AND NOT")

Add Schedule: Choose a schedule from the list ▼ Add

Schedule	Set as Exception	Delete
anytime	□	🗑

8. Web Filtering Policy Examples

8.1. Web Filtering Example 1: Basic Filtering with Secure Website Inspection

Web Filtering Policy					
Rule Name	**Groups/IPs**	**Filter**	**Schedule**	**Action**	**Explanation**
Allow Chromebook Management Traffic	Anyone/All Networks	Specific Allowed Google Domains (see section 5.7)	anytime	Allow	Always allowing a set of Google sites needed for Chromebooks to receive security policy updates.
Specific Allowed Sites	Anyone/All Networks	Specific Allowed Sites & Categories	anytime	Allow	Bypassing the default Web Filtering rule if needed.
Default Block	Anyone/All Networks	Specific Blocked Sites & Categories	anytime	Block	Default Web Filtering block rule

HTTPS Inspection Policy					
Rule Name	**IPs**	**Filter**	**Certificate**	**Action**	**Explanation**
Do Not Inspect	Server_LAN Guest_LAN	All Categories	N/A	Do not inspect	Never inspecting secure Server or Guest WiFi traffic
Do Not Inspect Chromebook Management Traffic	Anyone/All Networks	Specific Allowed Google Domains (see section 5.7)	N/A	Do not inspect	Never inspecting a set of secure Google sites needed for Chromebooks to receive security policy updates.
Inspect Traffic	Anyone/All Networks	Specific Sites & Categories	Yes	Inspect with your school specific certificate	Choosing to inspect secure traffic for selected categories such as Search Engines and Social Media.

8.2. Web Filtering Example 2: Individualised Filtering with Secure Website Inspection

Web Filtering Policy					
Rule Name	**Groups/IPs**	**Filter**	**Schedule**	**Action**	**Explanation**
Servers	Server_LAN	All Categories	anytime	Allow	No filtering for on-site servers
Guest Wifi Allow	Guest_LAN	Allowed Guest Access	anytime	Allow	Providing fairly restricted access to guest users.
Guest Wifi Block	Guest_LAN	All Categories	anytime	Block	Blocking all other internet access to guest users which is not defined above.
Always Allow	Anyone/All Networks	Specific Allowed Sites & Categories, including specific allowed Google Domains as per section 5.7	anytime	Allow	Allowing unauthenticated access to some sites for devices which don't support cookies, and sites which all users require access to without a need for per user reporting.
Authenticate	Anyone/All Networks	All Categories	anytime	Authenticate	Force all users to now Authenticate
Authenticated Staff	Staff Directory Group	Staff Authenticated Sites & Categories	anytime	Allow	Sites which Staff are allowed to access
Authenticated Students	Student Directory Group	Student Authenticated Sites & Categories	anytime	Allow	Sites which Students are allowed to access
Default Block	Anyone/All Networks	Specific Sites & Categories	anytime	Block	Default Web Filtering block rule

HTTPS Inspection Policy

Rule Name	IPs	Filter	Certificate	Action	Explanation
Never Inspect	Server LAN Guest LAN	All Categories	N/A	Do not inspect	Never inspecting secure Guest WiFi traffic as guests are unlikely to have the Web Filtering certificate on their device.
Never Inspect Chromebook Management Traffic	Anyone/All Networks	Specific Allowed Google Domains (see section 5.7)	N/A	Do not inspect	Never inspecting a set of secure Google sites needed for Chromebooks to receive security policy updates.
Inspect Traffic	Anyone/All Networks	Staff Authenticated Sites & Categories Student Authenticated Sites & Categories	Yes	Inspect with selected certificate	Inspecting Traffic from the Authenticated Staff and Authenticated Students Web Filtering Policy

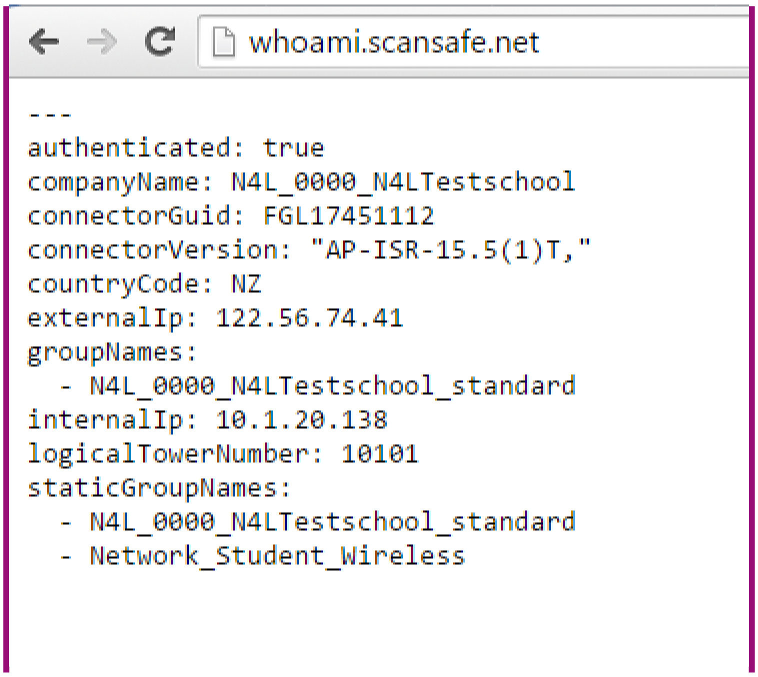
9. Troubleshooting

Checking connectivity to the Platform

There are several tools available to help troubleshooting N4L Web Filtering, the first being a check to ensure your school is actively using the system.

You can check that the Web Filtering service is enabled by browsing to http://whoami.scansafe.net

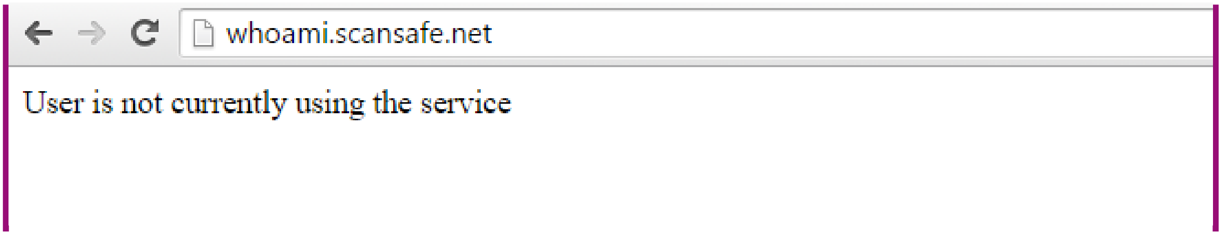
If the filtering dashboard is enabled your browser will return text similar to this:



```
---
authenticated: true
companyName: N4L_0000_N4LTestschool
connectorGuid: FGL17451112
connectorVersion: "AP-ISR-15.5(1)T,"
countryCode: NZ
externalIp: 122.56.74.41
groupNames:
  - N4L_0000_N4LTestschool_standard
internalIp: 10.1.20.138
logicalTowerNumber: 10101
staticGroupNames:
  - N4L_0000_N4LTestschool_standard
  - Network_Student_Wireless
```

Where a user has authenticated as part of Individualised Filtering, the user's username and associated directory groups will also be listed.

If the Web Filtering Dashboard is not enabled your browser will return this text:



User is not currently using the service

If the N4L Web Filtering service is not enabled you should contact N4L via email on support@n4l.co.nz to understand why this may be the case.

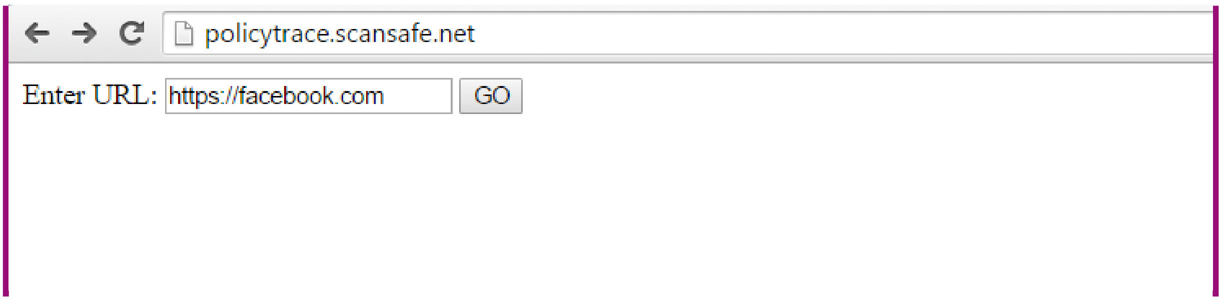
Policy Tracing

To check your settings to ensure they are being applied as you set them up through the filtering rules and policies, you can do a policy trace:

1. Open your internet browser on a computer that is configured to the filtering dashboard

2. Type in http://policytrace.scansafe.net

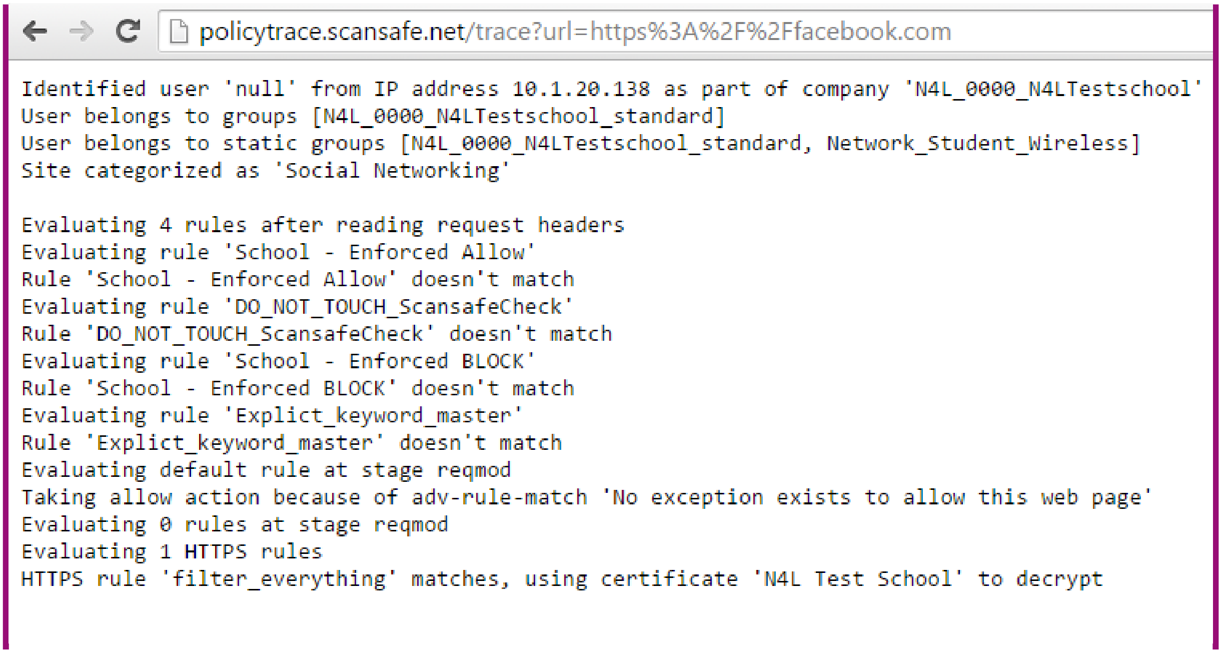
2.1 Enter the URL in the **Enter URL** box for the site you want to run a policy trace for and click **GO**



policytrace.scansafe.net

Enter URL: https://facebook.com

The result will show which rule has caused the allow/block action, or advise that no rule has been matched which results by default in an Allow action as seen in the example below.



policytrace.scansafe.net/trace?url=https%3A%2F%2Ffacebook.com

```
Identified user 'null' from IP address 10.1.20.138 as part of company 'N4L_0000_N4LTestschool'
User belongs to groups [N4L_0000_N4LTestschool_standard]
User belongs to static groups [N4L_0000_N4LTestschool_standard, Network_Student_Wireless]
Site categorized as 'Social Networking'

Evaluating 4 rules after reading request headers
Evaluating rule 'School - Enforced Allow'
Rule 'School - Enforced Allow' doesn't match
Evaluating rule 'DO_NOT_TOUCH_ScansafeCheck'
Rule 'DO_NOT_TOUCH_ScansafeCheck' doesn't match
Evaluating rule 'School - Enforced BLOCK'
Rule 'School - Enforced BLOCK' doesn't match
Evaluating rule 'Explict_keyword_master'
Rule 'Explict_keyword_master' doesn't match
Evaluating default rule at stage reqmod
Taking allow action because of adv-rule-match 'No exception exists to allow this web page'
Evaluating 0 rules at stage reqmod
Evaluating 1 HTTPS rules
HTTPS rule 'filter_everything' matches, using certificate 'N4L Test School' to decrypt
```

Where a user has authenticated as part of Individualised Filtering, the user's username and associated directory groups they are part of will also be listed. This can be used to ensure the schools filtering policy is referencing the correct directory groups.

Using these two features you can make sure everything is working the way it should be.

For any assistance or questions, please contact the N4L Helpdesk
Support@n4l.co.nz
0800 LEARNING
www.n4l.co.nz

Please see our website for links to:

- Web filtering video tutorials, manual and quick reference guides
- FAQs
-