Using web filter overrides to control website access

This example shows two methods of using web filter overrides to control access to specific websites: one for the entire network and one for specific users.

This example requires an active license for FortiGuard Web Filtering Services.

Method 1
1. Creating a rating override
2. Adding FortiGuard blocking to the default web filter profile
3. Adding the web filter profile to a security policy
4. Results

Method 2
1. Creating a user group and two users
2. Creating a web filter profile
3. Adding the web filter profile to a security policy
4. Results
Method 1
Creating a ratings override

Go to Security Profiles > Web Filter > Rating Overrides.

Create a new override and enter the URL fortinet.com. Select Lookup Rating to see its current FortiGuard Rating.

Set Category to Custom Categories (local categories) and create a new Sub-Category for blocked sites.

The sub-category has been added to the list of FortiGuard Categories, under Local Categories.
Adding FortiGuard blocking to the default web filter profile

Go to Security Profiles > Web Filter > Profiles.

Create a new profile and enable FortiGuard Categories. Right-click on Local Categories and select Block.

Adding the web filter profile to a security policy

Go to Policy > Policy > Policy.

Edit the policy that allows outbound traffic. Under Security Profiles, enable Web Filter and set it to use the new profile.
Results

In a web browser, go to www.fortinet.com.

The website will be blocked and a replacement message from FortiGuard Web Filtering will appear.

Rating overrides can also be used to allow access to specific sites within a FortiGuard category, such as General Interest - Personal, while still blocking the rest of the sites listed in that category.

Method 2
Creating a user group and two users

Go to User & Device > User > User Groups. Select Create New and create the group override_group.
Go to **User & Device > User > User Definition.**

Using the **User Creation Wizard**, create two users (in the example, *ckent* and *bwayne*). Assign *ckent* to *override_group* but not *bwayne*. 
Creating a web filter profile

Go to Security Profiles > Web Filter > Profiles.

Create a new profile and enable FortiGuard Categories. Right click on Local Categories and select Block.

Expand the Advanced Filter and enable Allow Blocked Override. Set Apply to Group(s) to override_group.

Set Assign to Profile to default to use it as the alternate web filter profile for override_group users.

Because the default web filter does not block Local Categories, using it will allow client to access fortinet.com for the duration of the override period (by default, Duration is set to 15 minutes).

Adding the web filter profile to a security policy

Go to Policy > Policy > Policy.

Edit the policy that allows outbound traffic and set the Policy Subtype to User Identity.
Create an **Authentication Rule** that includes both `override_group` and `bwayne` and has **Web Filter** set to `override_profile`.

### Results

In a web browser, go to www.fortinet.com.

After the user authentication screen, the website is blocked and a replacement message from FortiGuard Web Filtering appears.

Select **Override**. You are prompted to authenticate to view the page.

User `bwayne` is not able to override the web filter and receives an error message.
However, user *ckent* is able to override the filter and can access the site for 15 minutes.

You can monitor web filter overrides by going to Log & Report > Traffic Log > Forward Traffic.

Select an entry for more information about a session, including the user and hostname.