smoothwall®

The Web You Want

Carisbrooke

End User Guide

Contents

Introduction

The Carisbrooke release introduces 2 main new features:

- Negotiate Kerberos / NLTM
- Multi-Tenant Categories

and a number of general enhancements, details of which can all be found below.

Negotiate Kerberos/NTLM

Scope

The Negotiate Kerberos/NTLM project created a new, non-transparent, authentication method which allows the system to negotiate with the client about whether it would rather authenticate using Kerberos or NTLM. This saves the administrator having to decide in advance. It also means the different software on a client machine that require authentication, can use either of the two protocols and still successfully authenticate. This overcomes issues that many customers experience where browsers would authenticate but many applications would fail.

Note: As this only works with non-transparent clients, this is only suitable in environments where proxy settings have been deployed to clients, redirecting their web traffic via the Smoothwall.

What's changed

New authentication method for non-transparent authentication — "Negotiate Kerberos/NTLM"

When set as the non-transparent authentication method, the system negotiates with the client to identify whether it wants to use NTLM or Kerberos. This saves the administrator from choosing to use one or the other. Browser and software application authentication is handled better.

Setup

The **Negotiate Kerberos/NTLM** authentication method can be used to authenticate requests coming from multiple user agents, typically web browsers, that have different levels of support for authentication methods. The Web Proxy will offer both Kerberos and NTLM methods to the user agent, and allow it to pick the most secure method that it supports.

As with the Kerberos and NTLM authentication methods, in order to use **Negotiate Kerberos/NTLM**, the appliance must already be configured with an entry for an Active Directory domain via the **Services > Authentication > Directories** page. Optionally, **Negotiate Kerberos/NTLM (Terminal Services Compatibility Mode)** can be used to support multiple users accessing a single system via Remote Desktop/Terminal Services.

Additionally, browsing machines must be joined to the same Active Directory domain for seamless single sign-on to work correctly. However, machines not joined to the domain can still use the **Negotiate Kerberos/NTLM** method, typically via a popup dialog displayed to the user requesting valid domain credentials.

This new method of authentication has two modes — **Negotiate Kerberos/NTLM** and **Negotiate Kerberos/NTLM (Terminal Services Compatibility Mode)**. Either of these can be selected as the **Method** of authentication for **Non-transparent** authentication policies on the **Web Proxy > Authentication > Policy wizard** page. Note: Negotiate Kerberos/NTLM is NOT currently available for transparent deployments and so only shows when creating non-transparent authentication policies.

Troubleshooting

The diagnostics available via **Services > Authentication > Directories** can test the the appliance's connection to Active Directory. Limited information is also presented to the user in the event of an authentication failure that can help to diagnose problems with the authentication system.

Addendum to Current Administration Guide for "Creating Non-Transparent Authentication Policies"

Web Proxy > Authentication > Policy Wizard

New **Method** drop-down items:

Negotiate Kerberos/NTLM	If the client is not logged in, offer the option to authenticate using either Kerberos or NTLM authentication. This method is identical to both the Kerberos and NTLM authentication methods, but allows either to be used rather than being limited to exactly one method.
Negotiate Kerberos/NTLM (Terminal Services Compatibility Mode)	As **Negotiate Kerberos/NLTM**, but this method is designed to work with network clients using Microsoft Terminal Services, including Microsoft Windows NT 4.0 Terminal Services Edition, Microsoft Windows 2000 Server, and Microsoft Windows Server 2003. **Not available for transparent policies.**

What hasn't changed

N/A

All other authentication methods are still available and will remain selected when the migration occurs. **Negotiate Kerberos/NTLM** presents a new method to choose (not default) when configuring authentication in a non-transparent proxy deployment.

Multi-Tenant Categories

Scope

The scope of this work was to provide tenant-specific category groups and policies in Guardian, and provide tenants with the ability to edit category groups and view their policies on the User Portal.

This does not offer the ability for tenants to change the policies themselves; they can only edit the groups and categories used within the policies.

Terminology: In the Portal, Categories are known as “Lists”, and Category Groups are known as “List Groups”. This was done because Portal users are unlikely to have any familiarity with Smoothwall concepts such as categories, and user feedback indicated these terms were more easily understood.

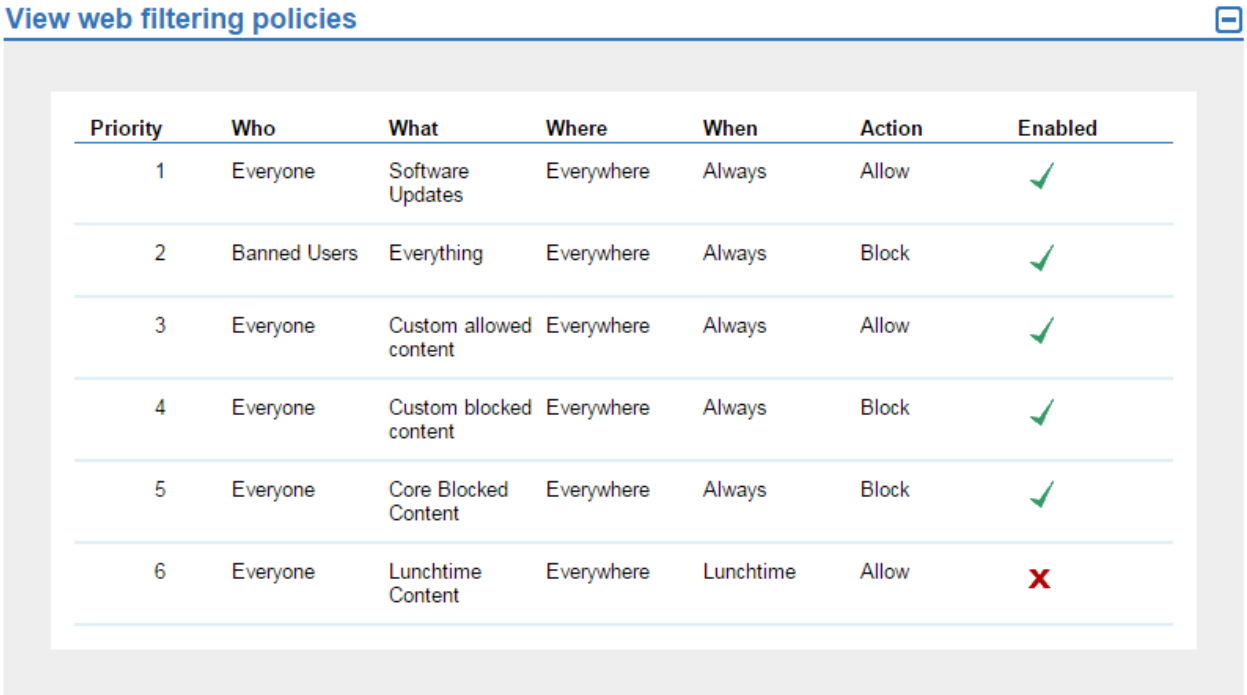
Note: The changes made to support multi-tenant categories only affect customers with a multi-tenant system.

What’s changed

New Filter policies page in the User Portal

The User Portal has gained a new read-only page to view Guardian policies: **Filter Policies**. On a single-tenant (non-multi-tenant) system, you see all policies. On a multi-tenant system, it only shows the policies specific to the logged-in tenant and does not show the global policies surrounding them, or those owned by the central administrator (see below).

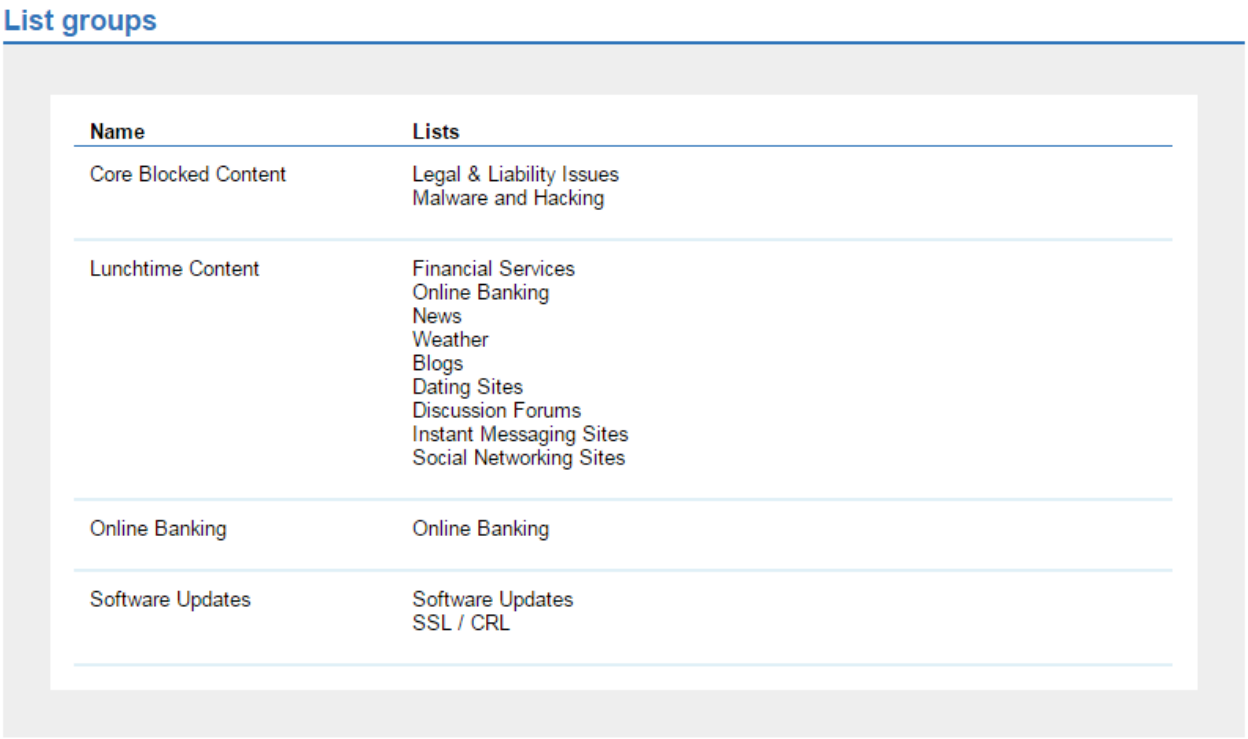
On a single-tenant system:



Priority	Who	What	Where	When	Action	Enabled
1	Everyone	Software Updates	Everywhere	Always	Allow	✓
2	Banned Users	Everything	Everywhere	Always	Block	✓
3	Everyone	Custom allowed content	Everywhere	Always	Allow	✓
4	Everyone	Custom blocked content	Everywhere	Always	Block	✓
5	Everyone	Core Blocked Content	Everywhere	Always	Block	✓
6	Everyone	Lunchtime Content	Everywhere	Lunchtime	Allow	✗

New Filter Lists page in the User Portal

The User Portal has gained a new page to edit category groups: **Filter List Groups**. This allows portal users to edit which categories are in category groups (click on the category group contents). They can not create or delete category groups, just change their contents. On multi-tenant systems they can only see and edit category groups they own and can therefore edit.



New menu look and feel in the User Portal

The appearance of the User Portal menu has changed. Entries are grouped into drop-down menus which appear when hovered over.

Removal of advanced view from the Category Groups page

Within the administration user interface, the option to manually switch to the **Advanced** view of category groups is no longer available. It can only be accessed from existing category groups that currently make use of the advanced settings.

If a category group with advanced settings in edited in the User Portal, then a warning appears and any advanced settings are converted to non-advanced settings in the editor. It is these that are saved when the edit is saved.

Category changes for multi-tenant

You can no longer change the tenant of a category after creation. This avoids a category being reassigned to a different tenant when it is part of a category group or policy which is tenant-specific. This is a safety mechanism to prevent data leakage between tenants.

Category groups are now multi-tenant

When creating a new category group in **Guardian > Policy objects > Category groups**, a tenant may be selected at the top of the form.

The **All** tenant creates a category group owned, and editable, only by the central administrator. This category group is also used in a policy for any tenant.

A category group owned by a tenant may be modified through the administration user interface by the central administrator, or through the User Portal by that tenant's administrator.

A category group owned by a tenant may only be used in policies owned by that tenant.

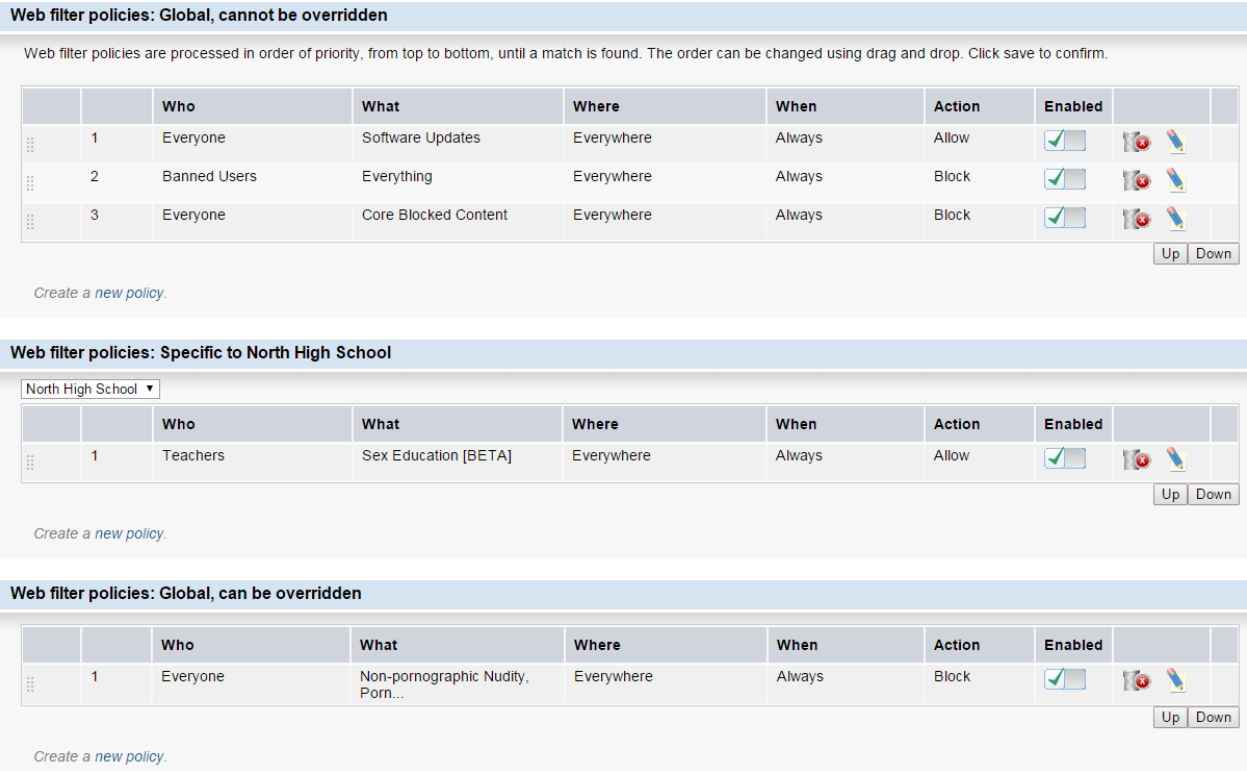
A category group owned by a tenant can only contain categories owned either by the central administrator or by the same tenant. (Categories owned by other tenants are not be displayed as an option.)

The tenant of a category group cannot be changed after it is created.

Tenant-specific categories are prefixed with the tenant name when displayed in the tree on the **Guardian > Policy objects > Category groups** page.

Policies are now multi-tenant

There are now multiple policy tables visible in **Guardian > Web filter > Manage policies**, which apply in order. Policies can be reordered within their table, but cannot be moved between tables.



The policy wizard now starts with a table/tenant selector screen to pick which table to add the policy to. If you use the **Add** links under each table, this is filled in automatically and skipped. The tenant cannot be changed when editing, so **Edit** links also skip the selection of which tenant a policy is for. Once a table/tenant has been picked, the wizard shows your selection at the top, before “Step 1”.

The top table, **Web filter policies: Global, cannot be overridden**, is owned by the central administrator and is for policies which must always be enforced. For example, a school district may wish to add a block on illegal content.

The bottom table, **Web filter policies: Global, can be overridden**, is owned by the central administrator and is for policies which should be defaults for all tenants, but could be overridden at their (the tenants’) discretion. For example, a school district may wish to add a block on social media, but, by including that block in the bottom table, a tenant administrator can override it by allowing social media in a category group used in one of their tenant specific policies.

The tables in the middle are specific to tenants: one table per tenant, but only one tenant table shown at any time. In this release, only the central administrator can modify policies, but tenant administrators can modify the tenant-owned categories and groups within. A drop-down above the tenant policy table selects which tenant’s policies are currently displayed for editing. Tenants may view their policies through the User Portal.

Policies in a tenant-specific table can use categories and category groups specific to that tenant, or global ones owned by the central administrator.

When checking a site against the policies, policies are checked top down, the top table first, then the middle tenant-specific table, followed by the bottom table (and top down within each table).

Because tenant policies are in the middle table, but policies are processed top down (in terms of which table is processed, and the rules with each table), tenants can override central administrator policies located in the bottom table. For example, a secondary school in a district may allow authenticated teachers access to a custom category of sex-education websites. This would override a global policy in the bottom table which blocks pornography . But a policy in the tenant table could not be used to override a block in the top table, as the rules located here are processed first.

Tenant-specific categories, category groups, and content modifications are prefixed with the tenant name when displayed in a policy page, a policy wizard, or confirmation page.

Migrating existing multi-tenant systems

Category groups containing categories owned by multiple tenants are split out automatically into a separate category group for each tenant involved.

Policies containing multiple tenant categories are moved or split into tenant tables. Policies which came below these in the policy table will be moved into the bottommost global table. This preserves filtering behaviour.

Web log viewer display in multi-tenant systems

Tenant-specific categories and category groups are prefixed with the tenant name when displayed in the **Policy** column of the **Web filter log** viewer (**Logs and reports > Logs > Web filter**), for example, <North High School/Grade 9 Allowed Sites>. However, tenant-specific categories are not prefixed with the tenant name in the **Category** column, as this reports the category as used by Guardian categorization, which does not include the tenant information. Note that if a tenant-specific category shares a name with a category common to all tenants, they will be treated as the same category in Guardian and both will be used for the purpose of categorisation.

What hasn’t changed

Non multi-tenant category groups and policies

There should be no visible change to behaviour of Guardian policies, category groups and categories in a non multi-tenant system, except for the additional access through the User Portal allowing portal users to edit category groups (if granted the permissions).

User Portal settings

There are no new settings to control access to new User Portal pages. They are controlled by the existing **Portal filter list management** setting on **Services » User portal » Portals** page.

Creating custom categories - revision to published documentation

The following revision is made to the current *Administration Guide* (Creating Custom Categories):

Search term filtering	Enter one search term per line, surrounded by delimiters, for example: (hardcore) (xxx) Spaces before and after a term are not removed, simplifying searching for whole words. Parentheses are required. You can use the following delimiters: [] () {} <> || Note: If the Search term you enter contains a delimiter, you must use a different delimiter to contain the whole pattern. For example: [mysearchwith(abracket)]
URL patterns	Enter a URL pattern per line, for example: adultsite|sexdream The example above looks for URLs containing either the word adultsite or the word sexdream. Avoid the use of unnecessary parentheses as these can cause issues. In particular avoid the construct (.)* as this uses a lot of memory.
File extensions	Enter one file extension per line, for example: .doc. You must include the dot (.) when entering file extensions.

Setup

Before migration of multi-tenant systems, the central administrator should review web filter policies and try to organize them into the following order:

- Common policies
- Tenant-specific policies
- Common policies

The migration makes changes to the policies, but they should have the same effect as before.

After migration, remove any redundant tenant-specific policies for locations that are not applicable to that tenant that the migration has generated. You should revise all policies to use tenant-specific category groups. For further information, refer to your Smoothwall representative.

General Carisbrooke Enhancements

New Web Proxy Authentication Method: Non-SSL Login Page

The Non-SSL login page functions like the SSL login page method, but uses HTTP rather than HTTPS. Because of this, it does not require the administrator to roll out certificates to all users using the login page.

NOTE: *It is considerably less secure because passwords are passed between the client and the system in plain text, and can therefore be intercepted. It is only recommended on networks where the connection between the clients and the system is secure and all the clients themselves are trusted.*

Addendum to Current Administration Guide for "Creating Non-Transparent Authentication Policies" and "Creating Transparent Authentication Policies"

Web Proxy > Authentication > Policy Wizard

New **Method** drop-down items:

Redirect users to non SSL login page (with background tab)	Select this method if a user's browser cannot accept cookies. This method is also suitable if a user's browser plugins or applications require the authenticated session to remain active. If the client is not logged in, redirect web requests to the non-SSL login page, which checks their username and password. The page is not secure because it uses HTTP to submit the username and password, but avoids the certificate needed for SSL login. The authentication service supports only one user per client IP address. Using this method, the non SSL login page automatically refreshes itself so that the authentication time-out period does not elapse. Because of this, the user must leave the non-SSL login page open at all times. To securely logout, the user must click **Logout** on the non-SSL login page. For more information, refer to the *Administration Guide*.

Redirect users to non SSL login page (with session cookie)	If the client is not logged in, redirect web requests to the non-SSL login page, which checks their username and password. The page is not secure because it uses HTTP to submit the username and password, but avoids the certificate needed for SSL login. The authentication service supports only one user per client IP address. Using this method, the Smoothwall System stores a session cookie in the user's browser. The cookie removes the need for the user to reauthenticate. This method is useful for users of tablets and other mobile devices which have problems keeping tabs in browsers open in the background. To securely logout, the user must click **Logout** from the non-SSL login page. For more information, refer to the *Administration Guide*.

New Web Proxy Logging Option — Local accesses

In some cases badly configured clients can flood Guardian's logs with accesses to local host addresses, causing various performance and disk usage issues. Typically, such access attempts should be logged, but you can choose turn off the logging of local host address accesses.

Addendum to Current Administration Guide for "Advanced Web Proxy Settings"

Web Proxy > Web proxy> Settings

Local accesses	Local accesses are those made through the web proxy to localhost or IP addresses 127.0.0.*. Typically, these should be logged. However, in some cases badly configured clients can swamp the log files, and it may then be desirable to turn this off. Select one of the following options: **Log** – Select this option to log information on local accesses. **Do not log** – Select to disable the logging of local accesses.

Guardian Using Asynchronous DNS

Guardian now uses asynchronous DNS meaning that multiple DNS queries can be made to the DNS servers at the same time. There should be no change to functionality, but better performance when used with a slow DNS server since Guardian is not waiting for responses in a serial (synchronous) fashion.

Guardian Reduced Memory Use

Guardian now uses less memory when reloading its configuration.

Turning Off the Squid Disk Cache

If the Squid disk cache size is set to zero, the disk cache is turned off rather than causing Squid to fail to start. This means that only system memory is used for the cache. This can have either positive or negative performance impacts, depending on the environment.

Decommissioning of Web Proxy Module

As of the Carisbrooke release, the Web Proxy module has been deprecated in favour of Guardian. Guardian includes the same functionality (namely a proxy and caching of web content), as well as extra features, such as filtering functionality and content modification.

The Carisbrooke release cannot be seen, or be available to, customers with the Web Proxy module installed on their system.

Customers can take one of 2 courses of action in order to upgrade to Carisbrooke (and any future updates):

- If a proxy and subsequent caching are not required features, simply uninstall the module on the **System > Maintenance > Modules** page.

OR

- If a proxy and subsequent caching are required, install Guardian from the **System > Maintenance > Modules** page — the installation of Guardian automatically removes the old Web Proxy module.