smoothwall®

The Web You Want

Smoothwall Multi-Tenant Managed Services

Multi-Tenant Administration Guide

Smoothwall® Multi-Tenant, Administration Guide, September 2014

Smoothwall publishes this guide in its present form without any guarantees. This guide replaces any other guides delivered with earlier versions of Multi-Tenant.

For more information, contact: docs@smoothwall.net

Trademark notice

Acknowledgements

Smoothwall acknowledges the work, effort and talent of the Smoothwall GPL development team: Lawrence Manning and Gordon Allan, William Anderson, Jan Erik Askildt, Daniel Barron, Emma Bickley, Imran Chaudhry, Alex Collins, Dan Cuthbert, Bob Dunlop, Moira Dunne, Nigel Fenton, Mathew Frank, Dan Goscomb, Pete Guyan, Nick Haddock, Alan Hourihane, Martin Houston, Steve Hughes, Eric S. Johansson, Stephen L. Jones, Toni Kuokkanen, Luc Larochelle, Osmar Lioi, Richard Morrell, Piere-Yves Paulus, John Payne, Martin Pot, Stanford T. Prescott, Ralf Quint, Guy Reynolds, Kieran Reynolds, Paul Richards, Chris Ross, Scott Sanders, Emil Schweickerdt, Paul Tansom, Darren Taylor, Hilton Travis, Jez Tucker, Bill Ward, Rebecca Ward, Lucien Wells, Adam Wilkinson, Simon Wood, Nick Woodruffe, Marc Wormgoor.

Multi-Tenant contains graphics taken from the Open Icon Library project http://openiconlibrary.sourceforge.net/

Address	Smoothwall Limited 1 John Charles Way Leeds. LS12 6QA United Kingdom	
Email	info@smoothwall.net	
Web	www.smoothwall.net	
Telephone	USA and Canada: United Kingdom: All other countries:	1 800 959 3760 0870 1 999 500 +44 870 1 999 500
Fax	USA and Canada: United Kingdom: All other countries:	1 888 899 9164 0870 1 991 399 +44 870 1 991 399

Contents

About This Guide

Smoothwall Multi-Tenant Managed Services Managed Services is a licenced feature of your Smoothwall System.

This supplement provides guidance for installing and managing Multi-Tenant Managed Services. For a detailed description of all other features of your Smoothwall System, refer to your *Smoothwall System's Administration Guide*.

Audience and Scope

This guide is aimed at system administrators maintaining and deploying Multi-Tenant Managed Services.

This guide assumes the following prerequisite knowledge:

- An overall understanding of the functionality of the Smoothwall System
- An overall understanding of networking concepts

Organization and Use

This guide is made up of the following chapters and appendices:

Conventions

The following typographical conventions are used in this guide:

Item	Convention	Example
Key product terms	Initial Capitals	Multi-Tenant Managed Services
Cross-references and references to other guides	Italics	See *Chapter 1, Introducing Multi-Tenant Managed Services* on page 3
Filenames and paths	`Courier`	The `portal.xml` file
Variables that users replace	*`Courier Italics`*	`http://<my_ip>/portal`
Smoothwall System	This may be one of: • Advanced Firewall • Network Guardian • Secure Web Gateway • Unified Threat Management • WAM-Edge depending on the license purchased	

This guide is written in such a way as to be printed on both sides of the paper.

Related Documentation

The following guides provide additional information relating to the Multi-Tenant feature:

- *Smoothwall System's Administration Guide*, which describes how to configure your Smoothwall System
- *Smoothwall System's Operations Guide*, which describes how to use your Smoothwall System
- *Smoothwall System's User Portal Guide*, which describes how to use the user portal feature
- http://www.smoothwall.net/support contains the Smoothwall support portal, knowledge base and the latest product manuals.

1 Introducing Multi-Tenant Managed Services

This chapter introduces the Multi-Tenant Managed Services feature, referred to in this guide as Multi-Tenant.

About Multi-Tenant Managed Services

Smoothwall Multi-Tenant Managed Services is designed to allow you to deploy your Smoothwall filter as a managed service for discrete individual clients, referred to as tenants. It provides a means of logically partitioning a Smoothwall System into multiple virtual instances. Each instance, or tenant, applies a core set of policies for all customers, as well as policies designed for individual tenants.

A Multi-Tenant system can only provide filtering services to clients configured as tenants. It is not possible to configure your Smoothwall System to support tenant, and non-tenant modes.

Multi-Tenant Managed Services provides the following features:

- Central administration control over all tenants
- Maintains data integrity between individual tenants, ensuring no data or policy overlap
- Tenant-level control of report generation
- Tenant specific category filtering, and content modification rules

Deploying a Multi-Tenant System

When deploying a Multi-Tenant system, the following core elements should be considered:

- Tenant configuration — see *About Tenants* on page 4
- Authentication services — see *About Authenticating Tenant Users* on page 4

- Filtering content categories, and, or, content modifications — see *About Tenant-Specific Filtering Policies* on page 4
- Reporting system — *About User Portals* on page 21
- User portal access — *About User Portals* on page 5

About Tenants

Tenants are assumed to be in different physical locations, such as office branches. Each tenant is configured with a unique identity, and has an associated IP address range. IP address ranges cannot overlap between tenants, but you can use several non-contiguous ranges.

Note: Users that are not assigned to a tenancy cannot browse the Internet, therefore you must ensure all known IP addresses are associated to a tenant. You cannot configure a "catch-all", default tenant.

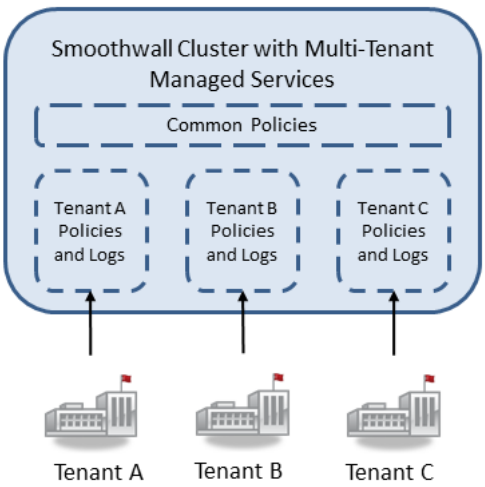
For a detailed description of how to configure tenants, see *Chapter 2, Configuring Tenants* on page 9.

About Authenticating Tenant Users

Each tenant must be linked to a directory service for user authentication. These can be centrally provided, or local to the tenant itself. The full range of Smoothwall directory service configurations are available for individual tenants. For more information, see *Assigning Directory Services to Tenants* on page 10.

About Tenant-Specific Filtering Policies

Each tenant makes use of a core set of system-wide policies, as well as policies tailored for individual tenants. Note that you can have the same, or similar, policies for both specific tenants and all tenants. Both policies will apply to the tenant, and in no particular order.



For more information, see *Creating Custom Categories* on page 11, and *Creating Content Modifications Policies* on page 13.

About Multi-Tenant Administrators

There are two management roles within a Multi-Tenant installation:

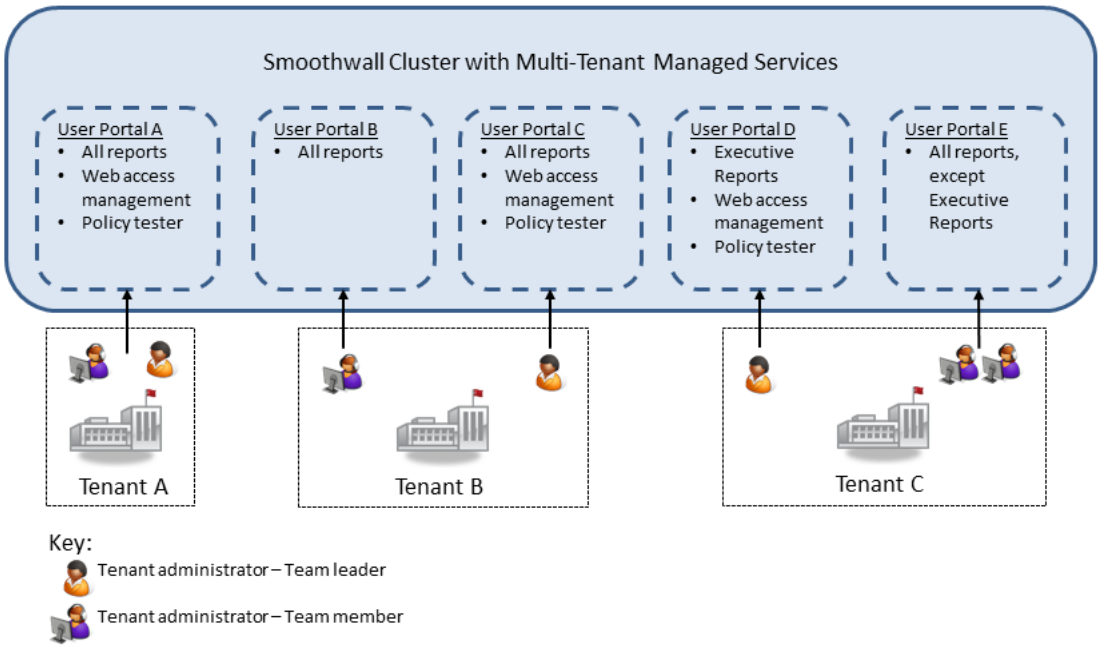
- Central Administrator — Typically, the central administrator is the system administrator for the complete Multi-Tenant installation. They have the ability to change policies, manage tenant configurations such as access to the policy tester, and manage reporting functions for any and all tenants, including those reports set up by the tenant administrator themselves. They also assign tenant administrators for tenancy management.
- Tenant Administrator — The tenant administrator is a user within a specific tenant, who is able to manage their tenant via a simplified web interface (see *About User Portals* on page 5).

  Note that a tenant administrator cannot manage operations for a tenant that they do not belong to. However, the central administrator may grant access to some, or all, of the reports allocated to another tenant.

About User Portals

Each tenant administrator can be assigned to a specific user portal, which allows them to manage and report upon their own tenancy. Each user portal can be tailored to show only the reporting and management operations relevant to that tenant, and can only be accessed by authorised tenant administrators.

It is also possible to assign multiple user portals to a tenant, allowing different groups of tenant administrators access to a different suite of reports and management functions for the same tenancy.



In the above example, the following assignments are displayed:

- User Portal A is accessible from everyone in Tenant A
- Team members from Tenant B can only access User Portal B
  - Team members can only run reports

- User Portal C is only accessible from team leaders in Tenant B
  - No distinction has been made between the reports run from User Portal B and User Portal C
  - Team leaders have access to additional operations from User Portal C
- The team leader from Tenant C can only access User Portal D
  - User Portal D is only accessible from Tenant C's team leaders
  - Only Executive Reports are available from User Portal D
- Team members from Tenant D can only access User Portal E
  - Team member can only run reports from User Portal E. However, Executive Reports are not available and cannot be run by team members.

For a detailed description of how to setup a user portal for a tenant, see *Chapter 4, Using Portals* on page 21.

For more information about using the user portal, refer to the *Smoothwall System's User Portal Guide*.

Use Case Examples

A Multi-Tenant system can be deployed in the following scenarios:

- A local education authority, with multiple schools and colleges to administer:

Core Element	Example Deployment
Tenant configuration	Each separate school, or college is a single tenant, with: • 1 x IP address range for teachers within that tenant • 1 x IP address range for students within that tenant
Authentication services	Each tenant uses two directory services: • Centrally provided authentication for teachers • Local authentication for students
Filtering content categories, and, or content modifications	Each tenant uses the following policies: • Each school and college has its own list of custom allowed sites, and custom blocked sites • System-wide policies that apply to teachers • System-wide policies that apply to school administration staff • System-wide policies that apply to student year groups
Reporting system	Reports are grouped into: • Needed by the Principal • Needed by the Heads of Year • Needed by the teachers

Core Element	Example Deployment
User portal access	Tenant administrators have access to the following user portals: • A user portal with full access — Typically, the Principal and ICT team would have access. • A user portal with access to a limited set of reports, web access management, and filter policy management — Typically used by Heads of Year, and Heads of Subject. Note that an additional user portal with the same operations available but a different report set, can be used to separate Heads of Year from Heads of Subject access. • A user portal with access to web access management, and filter list management — Typically used by all teachers.

- A healthcare authority, with separate hospitals to administer:

Core Element	Example Deployment
Tenant configuration	Each separate hospital is a single tenant, with: • 1 x IP address range for nursing staff • 1 x IP address range for administration staff • 1 x IP address range for patients
Authentication services	Each tenant uses two directory services: • Centrally provided authentication for nursing and administration staff • Local authentication for patients
Filtering content categories, and, or content modifications	Each tenant uses the following policies: • A separate filtering policy for patients • System-wide policies that apply to both staff and patients
Reporting system	The full range of reports are available to use,
User portal access	Tenant administrators have access to the following user portals: • A user portal with full access — Typically used by hospital management and IT teams • A user portal with access to all except web access management — Typically used by administration staff

2 Configuring Tenants

This chapter describes how to configure your Smoothwall System support tenants, including:

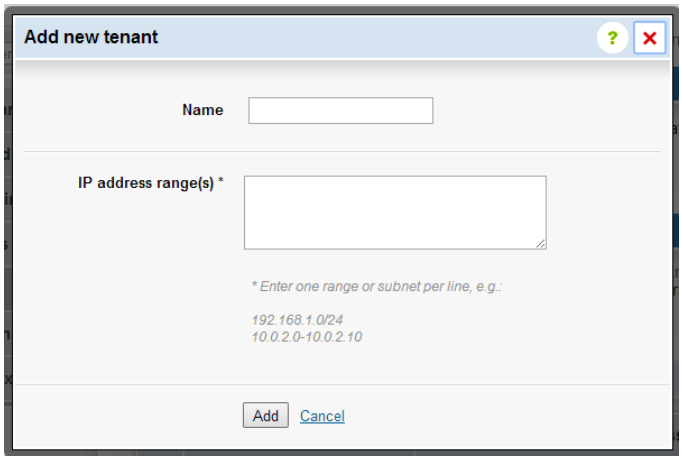
Creating Tenants

You must assign a unique name to each tenant supported, including the IP ranges used by that tenant.

Note: Requests from IP addresses not assigned to a tenancy will be blocked.

To create tenants, do the following:

1. From your Smoothwall System, browse to **System > Administration > Tenants**.
2. Click **Add new tenant**.



3. Configure the following parameters:
   - **Name** — The name of the tenant.
   - **IP address range(s)** — The IP address ranges that are assigned to the tenant.

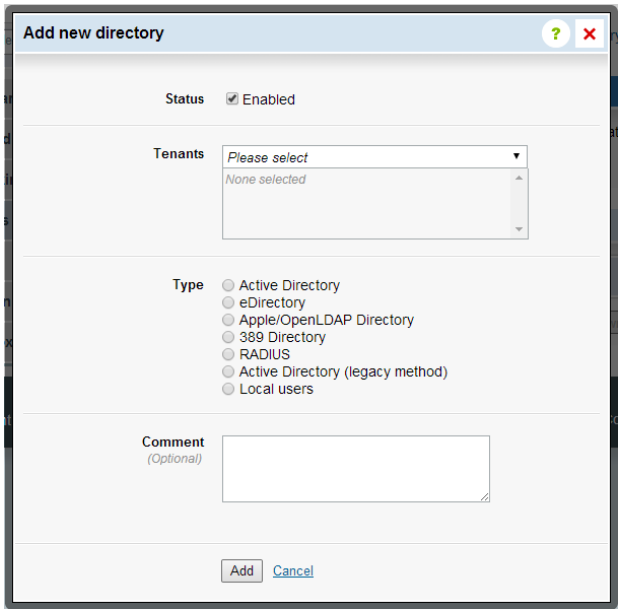
     If multiple ranges are assigned to the tenant, add each range on a new line.
4. Click **Save changes**.

Assigning Directory Services to Tenants

You must also add the user authentication directories to the tenants in order to verify the user and apply any filtering configured. The directory services can be centrally provided, or local to the tenant.

To assign the directory services to the tenants, do the following:

1. From your Smoothwall System, browse to **Services > Authentication > Directories**.
2. Click **Add new directory**.



3. Configure the following parameters:
   - **Status** — Select this option to enable or disable the connection to the directory service.
   - **Tenants** — From the drop-down menu, select the appropriate tenants.
   - **Type** — Depending on the directory type selected here, extra parameters must be configured. For a detailed description of these parameters, refer to your *Smoothwall System's Administration Guide*.
   - **Comment** — Enter an optional comment for this directory.
4. Click **Add**.

If you have selected **Local users** as the directory service type, you must configure local user details for authentication purposes. For more information, see *Managing Local Users* on page 11.

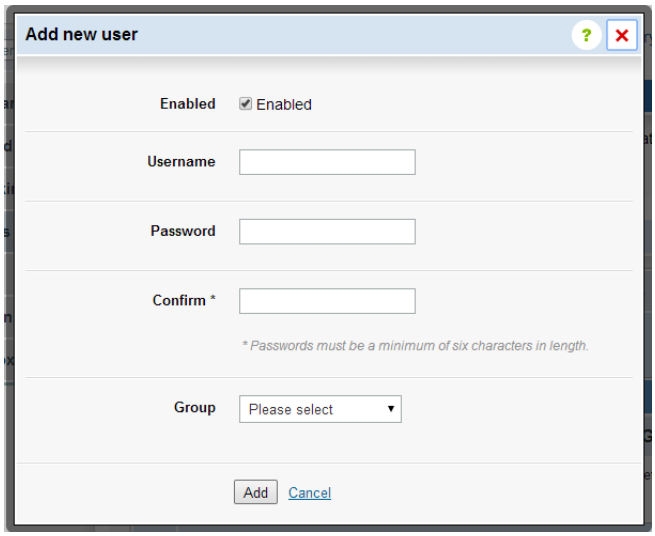
For more information about directory services, refer to your *Smoothwall System's Administration Guide*.

Managing Local Users

If you have selected **Local users** as your directory service type, you must configure local users for authentication purposes.

To add a user to a local users directory, do the following:

1. From your Smoothwall System, browse to **Services > Authentication > Directories**.
2. Expand the **Local users** directory, and click **Add new user**.



3. Configure the following parameters:
   - **Enabled** — Select this option to enable or disable the user.
   - **Username** — Enter the username for this account.
   - **Password** — Enter the password associated with this user. Passwords must be a minimum of six characters long.
   - **Confirm** — Re-enter the password.
   - **Group** — From the drop-down menu, select the group this user belongs to.
4. Click **Add**.

Creating Custom Categories

A category is a collection of URLs, domains, phrases, and, or, list of file type rules. The Smoothwall System uses categories to determine whether a user is allowed access to the content they have requested.

Creating Custom Categories for a Tenant

You can choose to apply tenant-specific categories. You do this by creating custom categories, and assigning them to a tenant. These will only apply to the user if they are in a matching tenancy.

Each category can only apply to one tenant. All requests from that tenant will use that category as well as system-wide categories.

Note: Supplied categories from Guardian cannot be assigned to a tenant. If these categories are edited, the **Tenant** drop-down menu will not be available.

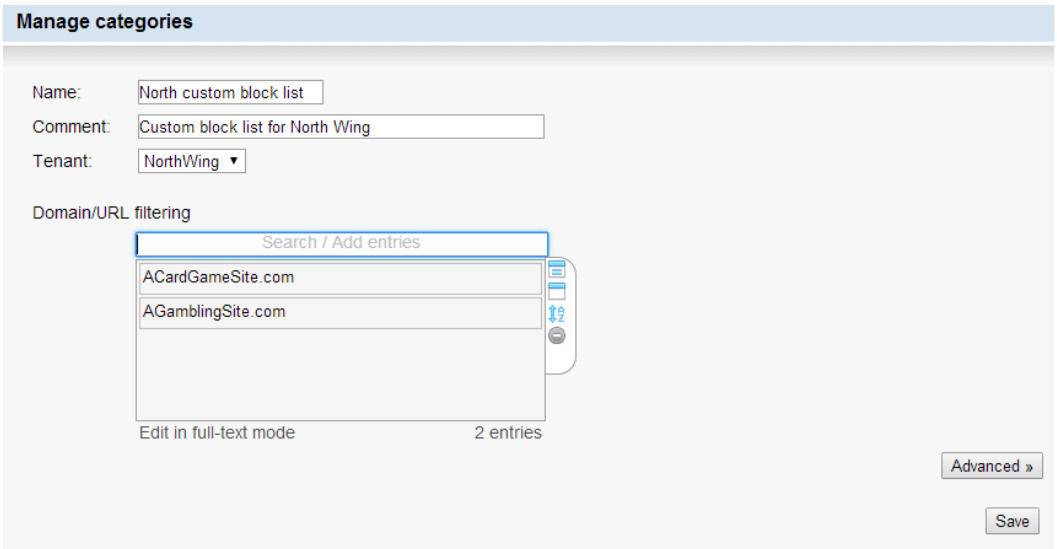
To create custom categories, do the following:

1. From your Smoothwall System, browse to **Guardian > Policy objects > Categories**.
2. From the **Manage categories** panel, configure the following parameters:
   - **Name** — The name of the category.
   - **Comment** — Enter an optional description for this category.
   - **Tenant** — From the drop-down menu, select the tenants for this category.
   - **Domain/URL filtering** — Enter the domains and or URLs for this category.

     Only one entry is allowed per line. Note that `www.` is not needed for URLs.
3. If search term filtering, URL pattern matching, or file type rules are required, click the **Advanced >>** button to display these. Configure the parameters as required.
4. Click **Save**.

   The custom category you have created will appear in the **Categories** panel at the bottom of the page.

For example:



For more information about custom categories, refer to your *Smoothwall System's Administration Guide*.

Creating Custom Categories for All Tenants

You can also create custom categories to be applied to all tenants. To do this, follow steps 1 to 4 in *Creating Custom Categories for a Tenant* on page 11, leaving the **Tenant** drop-down menu as **All**.

Creating Content Modifications Policies

A content modification policy is used to redirect users if inappropriate content is accessed. The Smoothwall System uses the requested site's capability to override the outgoing HTTP header.

Example scenarios may be:

- Schools may choose to redirect student's YouTube requests to YouTube Education.
- A restriction on available Google Apps may be required, such as, only allow access to email, calendar and documents.

For more information about content modification, refer to your *Smoothwall System's Administration Guide*.

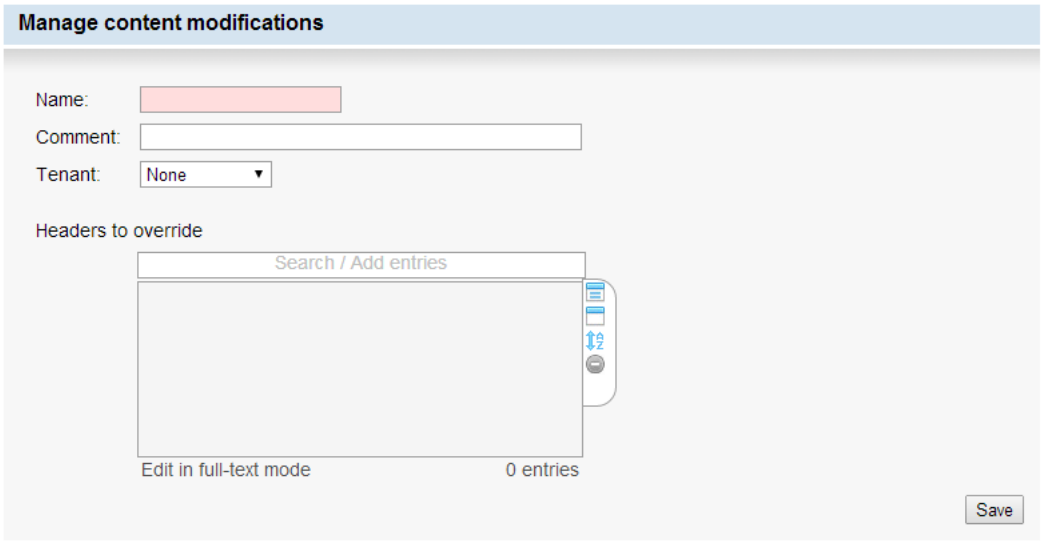
Creating Content Modification Policies for a Tenant

You can choose to apply tenant-specific content modification policies. You do this by creating custom content modification rules, and assigning them to a tenant. These will only apply to the user if they are in a matching tenancy.

Each policy can only apply to one tenant. All requests from that tenant will use that policy as well as system wide polices.

To create a content modification policy, do the following:

1. From your Smoothwall System, browse to **Guardian > Content modification > Content modifications**.



2. Configure the following parameters:
   - **Name** — The name of the content modification policy.
   - **Comment** — Enter an optional description for this policy.
   - **Tenant** — From the drop-down menu, select the tenants for this category.

- **Headers to override** — Enter the algorithm to use the requested website's capability to override HTTP headers sent to it, and redirect users to other content.

  Only one entry is allowed per line.

  For example:

  A redirect to YouTube Education would be configured as:

  ```
  X-YouTube-Edu-Filter: Abc_dEf
  ```

  where `Abc_dEf` is the search term or phrase which causes the redirect. Note that an account and key must be setup on YouTube for this to work — for more information, refer to http://www.youtube.com/schools.

  A restriction on available Google Apps to only allow access to Google Calendar and Google Drive would be configured as:

  ```
  X-GoogApps-Allowed-Domains: https://www.google.com/calendar/render,
  https://drive.google.com
  ```

  Note that for a Google Apps restriction, HTTPS interception is required as Google Apps uses HTTPS throughout. For a detailed description of how to do this, refer to your *Smoothwall System's Administration Guide*.

3. Click **Save**.

Creating Content Modification Policies for All Tenants

You can also create custom content modification policies to be applied to all tenants. To do this, follow steps 1 to 4 in *Creating Content Modification Policies for a Tenant* on page 13, leaving the **Tenant** drop-down menu as **All**.

Using a Block Page

You must create a customized block page to display to tenant members when they are blocked from accessing requested web content.

Note: The block is used for all tenants, and cannot be customized for each tenant.

For a detailed description of how to customize the block page, refer to your *Smoothwall System's Administration Guide*. However, note that the following options cannot be used for the block page:

- From **Guardian > Block page > Block pages**, under the **Advanced** button:
  - **Show unblock request**
  - **Show unblock controls**
  - **Show bypass controls**

Migrating an Existing Smoothwall System to Support Tenants

It is recommended you install a multi-tenant Smoothwall System alongside your existing centrally-managed Smoothwall System. You can then migrate configuration data from each node in your existing Smoothwall System to a tenant at a convenient time.

Note: It will not be possible to run reports for periods prior to the multi-tenant migration, as reporting data cannot be migrated over.

Changing Back to a Non-Tenant Setup

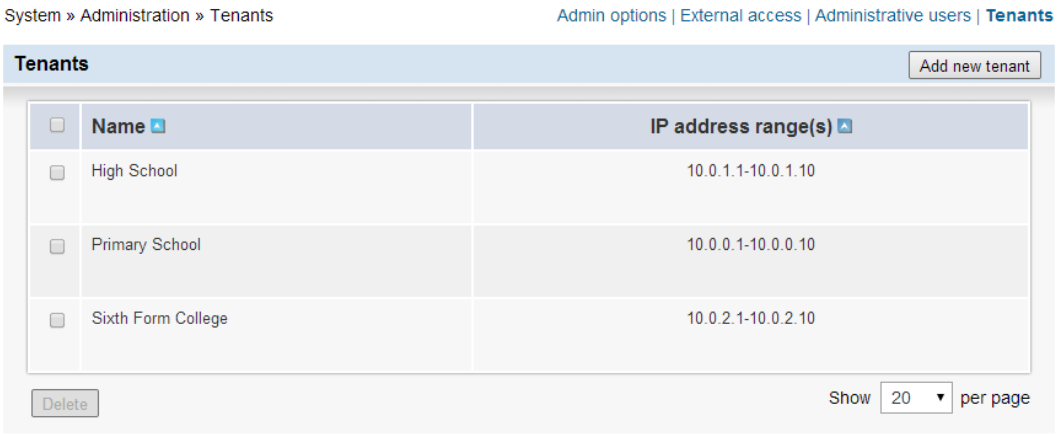
Just as you cannot migrate from a non-multi-tenant Smoothwall System to a multi-tenant installation, you cannot revert back to a non-multi-tenant mode. Backwards compatibility of tenant configurations to non-tenant configurations is also not supported.

3 Managing Tenants

This chapter describes how to manage various aspects of your Multi-Tenant system, including:

Managing Tenants

The **Tenants** panel of the **Tenants** page lists all configured tenants. You can edit, and remove tenants from this panel.



Editing a Tenant

To edit a tenant, do the following:

1. From your Smoothwall System, browse to **System > Administration > Tenants**.
2. Highlight the relevant tenant, and click **Edit**.
3. In the **Edit tenant** dialog box, change the settings as required. For a detailed description of the available settings, see *Creating Tenants* on page 9.
4. Click **Save changes**.

Deleting a Tenant

Before deleting a tenant, the following behavior should be noted:

- Any directory services assigned to that tenant, must have their association removed first before the tenant can be deleted. If this is not done, a warning message will be displayed.

  For more information, see *Assigning Directory Services to Tenants* on page 10.

- Any tenant-specific custom categories, and content modifications are retained for future use by other tenants.

  The Smoothwall System will display **Deleted tenant** against categories or content modifications for deleted tenants.

- Access to historical data from the deleted tenant must be made using SQL. For more information, refer to your Smoothwall representative.

Note: An option for maintaining access to data from a tenant, whilst also removing the tenant from the managed service, is to delete the associated IP address range. This maintains all references to the tenant in the user interface, including the ability to run reports against the data, but disables ongoing services for that tenant. For more information, refer to your Smoothwall representative.

To delete a tenant, do the following:

1. From your Smoothwall System, browse to **System > Administration > Tenants**.
2. Highlight the relevant tenant, and click **Delete**.
3. Confirm that you want to delete the tenant.

You can also delete multiple tenants at the same time.

To delete multiple tenants, do the following:

1. From your Smoothwall System, browse to **System > Administration > Tenants**.
2. **Mark** the relevant tenants, and click **Delete**.
3. Confirm that you want to delete the tenants.

Using the Policy Tester

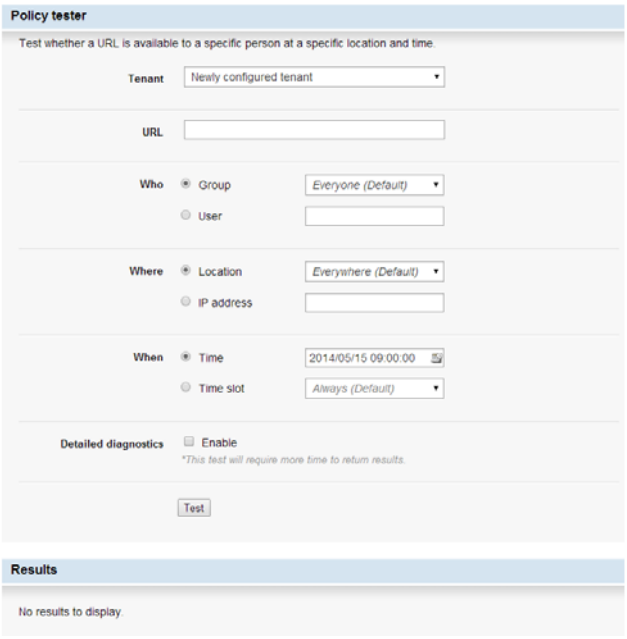
The Smoothwall System's policy tester works by sending an impersonated request for access to a URL. This enables you to determine what policy actions would apply for the URL. You can also test the URL against a specific user or group, a specific location or IP address, or a specific time.

Tip: Use the policy tester to check possible negative side effects of adding a user, group, location, or time slot to a Guardian policy.

Note: The policy tester can impersonate a user or group(s) attempting to access web content. The Smoothwall System does not log impersonated requests. However, an upstream proxy may capture and log the request as coming from the user or group(s) being impersonated.

To use the policy tester, do the following:

1. From your Smoothwall System, browse to **Guardian > Quick links > Policy tester**.



2. Configure the following settings:

   - **Tenant** — From the drop-down menu choose the tenant to policy test. You can either test the policy for:

Tenant Option	Description
Configured tenants	All tenants you have configured on your Smoothwall System will b e listed under this heading available for testing.
Other tenants	Additional options to test are: • **Temporarily create a new tenant** — The test is run from a hypothetical, newly created tenant. This should only match those categories that are applicable to all tenants. • **None** — The test is run as if a user is attempting to browse whilst not assigned to a tenant. The request is blocked.

   - **URL** — The URL to test. You can use `www.` if required.
   - **Who** — Optionally, select whether to test a group or user, and enter the appropriate details.
   - **Where** — Optionally, select whether to test a location or IP address, and enter the appropriate details.
   - **When** — Optionally, select whether to test a timestamp or time slot, and enter the appropriate details.
   - **Detailed diagnostics** — Select to enable or disable detailed diagnostics, such as, what policy actions apply to resources such as images, Javascript, CSS tags, HTML5 multimedia tags, and so on.

     Note that only the specific URL is tested. Content from other pages are not tested.

3. Click **Test**.

   For each policy enabled at that time, the Smoothwall System displays what action has been applied to the specified URL, and any requested options.

Note: When testing a URL which results in a redirect, the redirect destination and its status are displayed, enabling you to policy test the redirect URL. For more information on URL statuses, refer to http://www.w3.org/Protocols/rfc2616/rfc2616-sec6.html#sec6.1.1.

For more information about the policy tester, refer to your *Smoothwall System's Administration Guide*.

4 Using Portals

This chapter describes how to setup and maintain a portal for tenant users, including:

About User Portals

The Multi-Tenant user portal allows tenant administrators to manage operations for their tenancy, including one or more of the following tasks:

- Use the policy tester — This is a simplified version of the Smoothwall System's policy tester - see *Using the Policy Tester* on page 18.

  In addition to the policy tester, tenant administrators can request a block, or an unblock, for the URL they are testing.
- Generate reports — You can restrict the number of report templates available to tenant administrators. You can also publish reports generated on the Smoothwall System, to the user portal. Additionally, you can choose to assign multiple user portals to the same tenant, with each user portal having a different set of report templates available.
- Manage web access — You can block web access for groups of users, or from specified locations.
- Manage tenant-specific categories — You can add or remove domains, and search terms from tenant-specific categories.

For a detailed description about how to use the portal, refer to your *Smoothwall System's Administration Guide*.

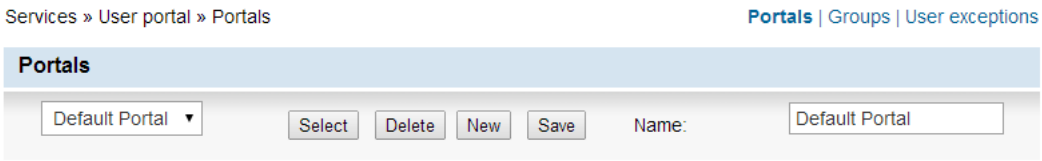
Note: You cannot access a tenant's user portal from outside the allocated IP address range for that tenant. However, you may be able to access their data for reporting purposes if you have permission — see *Running Other Tenant's Reports* on page 27.

Creating User Portals

You can create unique portal instances for tenant administrator from specific tenants. This enables each portal to be customized for each tenant, or even each tenant administrator, ensuring only relevant functions and reports are available.

To create a user portal for a tenant administrator, do the following:

1. From your Smoothwall System, browse to **Services > User portal > Portals**.



2. From the **Portals** panel, click **New**.
3. Configure a name for the portal in the **Name** text box.
4. Click **Save**.

Tenant administrators access the portal from a web browser, using the URL:

`http://<SmoothwallSystem_IPAddress>/portal`

where *SmoothwallSystem_IPAddress* is the internal IP address assigned to your Smoothwall System.

Configuring User Portals

Configuring a user portal involves the following:

- *Enabling the Policy Tester* on page 22
- *Making Report Templates Available* on page 23
- *Enabling Group and Location Blocking* on page 24
- *Managing Filter Lists* on page 24
- *Configuring a Welcome Message* on page 25

The following sections describe how to add configuration to a tenant's user portal.

Enabling the Policy Tester

The policy tester enables tenant administrators to test if a URL is accessible to a user at a specific location and time. Tenant administrators can also request that blocked content be allowed through, or to block previously allowed content.

To grant access to the policy tester, do the following:

1. Browse to **Services > User portal > Portals**.
2. Select the relevant portal from the drop down list, and click **Select**.

3. Scroll down to the **Policy tester** panel, and configure the following:

   - **Enabled** — Select to enable or disable access to the policy tester from this portal.
   - **Allow block/unblock requests** — Select this to allow portal users to send an unblock request to the system administrator.
   - **Administrator's email address** — Enter the email address to send the unblock request to.

4. Scroll down to the bottom of the page, and click **Save**.

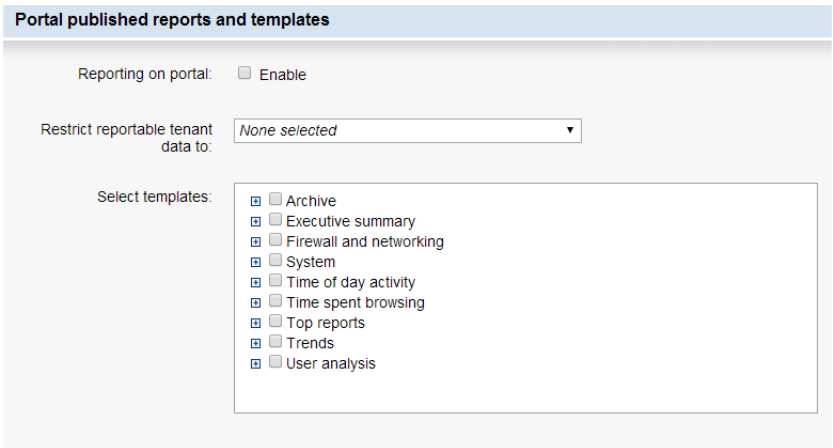
Making Report Templates Available

There are two methods available to make report templates available to a user portal; you can either add a number of templates at the same time, or add them individually.

The following procedure describes how to add a number of templates to a portal. For a detailed description of how to add individual reports to a portal, refer to your *Smoothwall System's Operations Guide*.

To make a number of report templates available to the portal, do the following:

1. Browse to **Services > User portal > Portals**.
2. Select the relevant portal from the drop down list, and click **Select**.
3. Scroll down to the **Portal published reports and templates** panel, and configure the following:



   - **Reporting on portal** — Select to enable or disable access to reports from this portal
   - **Restrict reportable tenant data to** — From the drop-down menu, select the tenant data set that is applicable to this portal. Note that you can also allocate multiple data sets to a user portal, for more information see *Running Other Tenant's Reports* on page 27.
   - **Select templates** — Select those reports that can be run from this tenant's user portal. Note that by selecting a top-level folder, access is granted to all reports contained in that folder.

4. Scroll down to the bottom of the page, and click **Save**.

Note: Smoothwall groups are not tenant-specific. Those reports where you can select a Smoothwall group to include results from, such as the Top domains by hits and bandwidth for a chosen group report, will display all groups configured in your Smoothwall System, even if they are not used by that user portal's tenant.

Enabling Group and Location Blocking

You can allow tenant administrators to block web access for users in a specific group, or location.

Note: Groups and locations are not tenant-specific. Users from one portal will be able to see groups and locations used by other tenant configurations.

To grant access for web access management, do the following:

1. Browse to **Services > User portal > Portals**.
2. Select the relevant portal from the drop down list, and click **Select**.
3. Scroll down to the **Portal permissions for web access management** panel, and configure the following:

   - **Enabled** — Select to enable or disable web access management from this user portal.

     Note that if this option is left unticked, control of both groups and locations is disabled, even if they are left enabled.

   - **Allow control of groups** — Select to enable or disable blocking of web access for groups from this user portal.

     From the list of groups underneath, select the group, or groups, that the tenant administrator is authorized to block. Use CTRL or SHIFT to select multiple groups.

   - **Allow control of locations** — Select to enable or disable blocking of web access for locations from this user portal.

     From the list of locations underneath, select the location, or locations, that the tenant administrator is authorized to block. Use CTRL or SHIFT to select multiple locations.

4. Scroll down to the bottom of the page, and click **Save**.

Managing Filter Lists

Portal users can add or remove domains and search terms from web filter categories.

To grant access to filter lists management, do the following:

1. Browse to **Services > User portal > Portals**.
2. Select the relevant portal from the drop down list, and click **Select**.

3. Scroll down to the **Portal filter list management** panel, and configure the following:

   - **Manage filter lists on portal** — Select to enable or disable filter lists management from this user portal.

4. Scroll down to the bottom of the page, and click **Save**.

Configuring a Welcome Message

You can display a customized welcome message when a user visits a portal.

To display a welcome message on a portal, do the following:

1. Browse to **Services > User portal > Portals**.
2. Select the relevant portal from the drop down list, and click **Select**.
3. Scroll down to the **Welcome message** panel, and configure a welcome message.

   To disable the welcome message, untick the **Welcome message** box.

4. Click **Save**.

Assigning Tenant Administrators to User Portals

You can assign tenant administrators to user portals using one of two methods:

- As individual named administrators — see *Assigning Individual Tenant Administrators* on page 25
- As members of a defined, Smoothwall group — see *Assigning Groups of Tenant Administrators* on page 26

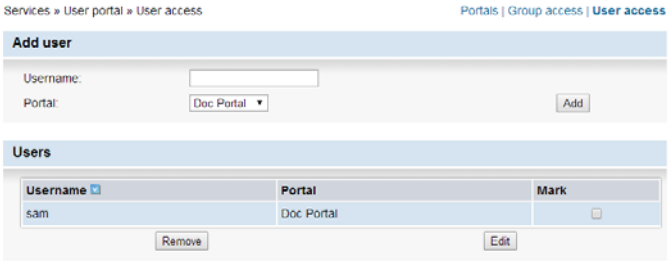
Note: It is recommended you assign individual users as tenant administrators in order to retain an individual level of control over management operations for each tenant.

Assigning Individual Tenant Administrators

A individual tenant administrator can either be a Smoothwall System local user (see *Managing Local Users* on page 11), or a directory services user (see *Assigning Directory Services to Tenants* on page 10). However, they must be mapped to the same tenancy as the user portal, see *Assigning Directory Services to Tenants* on page 10.

To assign individual users to this portal, do the following:

1. Browse to **Services > User portal > User acess**:



2. From the **Add user** panel, configure the following parameters:
   - **Username** — Enter the username for the tenant administrator for this user portal. This is case-sensitive.

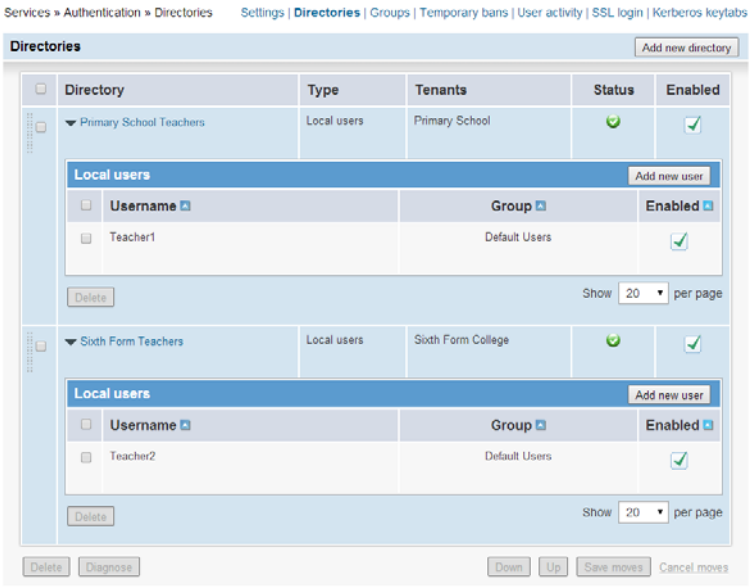
     Note that the username must already exist within the directory service for the tenant — see *Assigning Directory Services to Tenants* on page 10.
   - **Portal** — From the drop-down menu, select the portal that the tenant administrator can access.
3. Click **Add**.

Note: If a group is assigned to a user portal (see *Assigning Groups of Tenant Administrators* on page 26), all members of the group have access. Typically, you would use the above method to assign individual tenant administrators to a different user portal than those with the same group membership.

Assigning Groups of Tenant Administrators

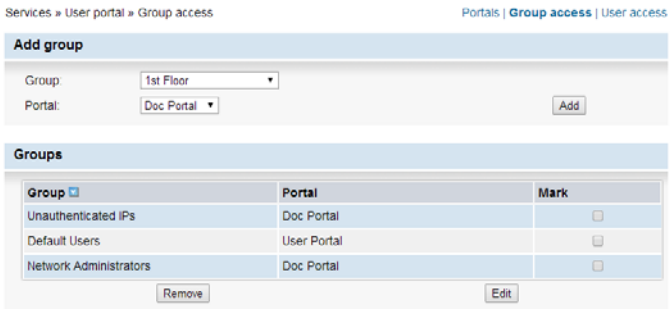
If a user portals' tenant administrators are members of the same group, either a local Smoothwall group or a directory services group, you can provide access to the group as a whole. However, it should be noted that *all* members of the group will have access to the user portal. As user portal data is restricted on a tenancy-basis, members of groups used by multiple tenants may have access to the wrong tenancy data. For example, if the configuration below were used, users from the Default

users group will have access to the user portal assigned to both the Primary School and Sixth Form College tenants:



To assign a user group to this portal, do the following:

1. Browse to **Services > User portal > Groups access**.



2. Configure the following parameters:
   - **Group** — From the drop-down menu, select the user group that will use this portal.
   - **Portal** — From the drop-down menu, select the portal that this group can access.
3. Click **Add**.

Running Other Tenant's Reports

You can allow tenant administrators to run reports using another tenant's data, but only from those report templates available in their user portal.

To allow tenant administrators to run report for other tenants, do the following:

1. Browse to **Services > User portal > Portals**.
2. Within the **Portal published reports and templates** panel, configure the following:
   - From the **Restrict reportable tenant data** to drop-down menu, select those tenants whose administrators can run these reports on behalf of other tenants.

To grant access to the report from all configured tenants, choose **None selected**.

3. Scroll down to the bottom of the screen, and click **Save**.

Note: It is not possible to allow tenant administrators to run the policy test tool, edit categories, or block web access for other tenants.

Index


smoothwall®
The Web You Want