APPTIX
Connecting Your Business. Anywhere.

ClientNet

Portal Admin Guide

Document Revision Date: June 5, 2013

Contents

Introduction to the Portal

About the Portal

Use the portal as a center for the resources, support, and configuration of your security services. The easy-to-use screens provide you with a dashboard view of your service statistics, with extensive reporting features and functionality for managing your users, all in one place.

The features that you see in the portal depend on your access permissions and on your organization's service configuration.

NOTE: Using Microsoft Internet Explorer 6 for viewing the portal is not recommended.

Section	Description
Dashboard	The Dashboard provides a visual snapshot of all your key service statistics in one place. You can configure the Dashboard to show the key statistics that are most important to you.
Users and Groups	The **Users and Groups** tab is a central point of access for the management of users and groups across your services.
Services	You can configure the settings for your cloud Email Security, Web Security, and Instant Messaging Security services.
Reports	You can download PDF summary reports of your email, web, and IM services, containing graphs, tables, and key statistics relating to traffic volumes and service performance. You can download CSV files containing detailed statistics on your services. You can also schedule reports to be emailed to you at regular intervals.
Tools	The **Tools** tab provides access to resources such as Track and Trace, and to software that you can download to help you manage your services.
Support	The **Support** tab provides links to the Support Ticketing Center and the online Help system. You can set up alerts to inform you of issues with your services.
Administration	Use the **Administration** tab to manage your users and submit change requests.

Logging On and Off the Portal

To log on to the portal, you need a user name and password.

To log on to the portal:

1. Enter your user name.
2. Enter your password.
3. Click **[Log in]**.

To log out of the portal:

- From any screen in the portal, click the **Log Out** link in the top right of the screen.

Language Support in the Portal

You can view the portal in 11 languages.

To change the language you see on screen, do one of the following:

- Select the required language from the drop-down menu at the top of any screen.
- Select the **My Profile** link at the top of any page of the portal, then choose the required language from the **Preferred language** drop-down and click **[Save and Exit]**.

In most places where you enter characters in the portal, you can use all Unicode characters. You are limited to single-byte alphanumeric characters (ASCII characters) in Email Content Control and IM Content Control for the following:

- Names of lists
- Names of rules
- Names of groups

Names of files can be entered using double-byte characters but these must be UTF-8 encoded. Most character sets and encoding types are supported for use in Email Content Control and IM Content Control lists to detect text content in emails and instant messages.

How Long Do Settings Take to Apply?

Typically, changes that you make to settings in the portal take effect within an hour. Some configuration changes are visible in the portal within minutes.

Setting SMS Alerts

You can receive SMS alerts to inform you of critical announcements on your security services. For example, we can send you an alert to notify you of a delay to our services. The alerts are delivered to a mobile device as text messages.

The SMS alerts are specific to your services. You can define the domains that you want to receive alerts for. You can have SMS alerts sent to up to five telephone numbers.

NOTE: Depending on how the portal is set up, you may not be able to set up SMS alerts.

To receive SMS alerts:

1. Select **Support > SMS Alerts**.
2. From the **Global settings** drop-down list, either:
   - To receive SMS alerts for all domains on the same telephone numbers, select **Global settings**.
     OR
   - To receive SMS alerts for a specific domain, select the required domain name.
3. Enter up to five telephone numbers on which to receive SMS alerts. Include the country and the area codes.
4. Click **[Save and Exit]**.

General Security Best Practice

The following guidelines will help the users in your organization follow computer security best practices:

- You should understand your company's requirements around electronic messaging policy and any regulatory obligations applicable to your industry and jurisdiction. It is recommended that you have such a policy in place to govern your employees' use of email. The online resources are provided to help enable you to enforce and effectively implement an acceptable computer use policy.
- Logon details to the portal should be kept secure and only used on a secure computer and a trusted computer. Because the portal is accessed over the Internet, ensure that procedures exist to revoke access when a member of staff leaves or no longer needs access. Service Desk authorized contacts should also be kept current.
- Choose long, non-obvious, and complex passwords that cannot be guessed by using a combination of uppercase, lowercase, numerals, and special characters, e.g. !#&'()+. Do not write down passwords. If you have difficulty remembering them, use Password Safe™ (if approved by your company's IT/Information Security department). Password Safe™ enables you to store multiple passwords securely, and means that you only have to remember one password to access them.
- Do not share passwords.
- Change your password on a regular basis.
- When logging into the portal, ensure that your web browser goes to the correct URL for the portal. Further verification of the correct site can be made by viewing the site SSL certificate which is issued by the Entrust certificate authority. Your web browser should verify that the certificate is genuine with the Entrust root certificate.
- When you download documents from the portal, the spreadsheet, word processing, or document software may cache a copy to a temporary area on your hard drive. Caching definitely occurs if an automatic save function is active. The cached copy may not be removed automatically - even after you close the document. The cached copy may be accessible to other users of your computer.
- Web browsers cannot cache the portal contents. Increase your security by not enabling web browsers or proxy servers to override this feature.
- Be careful when adding or changing the settings in the portal. Check and check again that the correct settings are entered. Although we have safeguards in place, inadvisable changes to the portal settings may result in disrupted service or email that is directed to the wrong location.
- Regularly check the list of users who have access to the portal. Do users have more access than required for their role? Should they still have an account or be removed?
- Ensure that the computer that you use to access the portal is protected from malicious attacks. Use firewalls, proxy services, anti-malware detection, and other methods, as appropriate. Have security policies, standards, processes, and procedures in place at your company to ensure that you protect your information assets appropriately for your business. Ask your local IT/Information Security department for the policies that govern how information security is carried out in your company.
- Occasionally we may send you an email that requests that you log into the portal, for example

to access a report. To reduce the risk of being exposed to a phishing email that contains branding or links that mimic the genuine portal, use the Anti-Virus service.

- It is recommended that you set up a separate account for the portal for each of your users. It is not advisable to share accounts.
- Ensure that your DNS is secure to prevent alteration of the MX records, which can potentially allow malicious redirection and unauthorized interception of email. To prevent domain hi-jacking, also ensure that contact details and security procedures are in place and up to date with the domain registrar.

About Logging into the Portal Using the Authentication Server

The authentication server handles your login to the portal. You may notice that the system redirects you to this authentication server when you log in to the portal. Once you have authenticated successfully, the system redirects you back to the portal.

The authentication server lets you change your own password. If you forget your password, you can reset it by answering the security questions that you have already set up.

Setting Up Your Authentication Security Information

The first time that you log into the portal using the authentication server, you need to set up your security information.

To set up your security information:

1. The login page for the portal redirects you to the authentication server.
   Enter your user name and password.
2. The first time that you log in using the authentication server, it identifies you as having an incomplete authentication profile.
   It prompts you to set up your security information.
   - Enter your email address (optional).
   - For all three security questions, select the new question from the list.
     Enter your answers. You must choose three unique questions. Your answers to the questions must be 3-50 characters long.

Updating Your Authentication Profile

Your authentication profile contains your password and security questions. Your security questions are used to confirm your identity if you forget your password.

To update your profile:

1. To view your profile, click **My Profile**.
   The **My Profile** page displays.
2. To change your password:
   - Click **Create new password**.
   - Enter your old password.
   - Enter and confirm your new password.

3. To change your security questions and answers:
   - Click **Create new security questions**.
   - For all three security questions, select the new question from the list.
     Enter your answers. You must choose three unique questions. Your answers to the questions must be 3-50 characters long.
4. To complete updating your profile, click **[Save and Exit]**.
   To abandon your changes click **[Cancel]**.

Managing Portal Users and Domains

About Managing Portal Users and Domains

You can manage your portal users and your domains within the Administration tab of the portal.

The main administrative areas are as follows:

User Management	View, add, edit, or delete administrator users and their permissions.
Domain Changes	Add a new domain to use the services.

Defining a Portal User

Users can be delegated one of several roles that give them various levels of permission to carry out administrative tasks in the portal.

To define a portal user:

1. Select **Administration > User Management**.
2. Click **Create new user**.
3. Enter the user's full name (required), login name (required), and email address (optional).
   All portal users must have a unique login name, so an email address is recommended.
4. Select the **Preferred language** that the portal displays in.
5. Select the **Preferred time zone** for the user.
   The preferred time zone is used in time-related settings such as for scheduled reports and rules for Content Control.
6. Enter a password for the user (required).
   The new password must be at least eight characters long and contain alphabetic, numeric, and symbol characters. The user is prompted to change this password when they next log in to the system. The new password is not visible to any other user.
7. Ensure that the **[User is enabled]** button is set to **Yes**.
   Setting this option to **No** disables the account. When the user has been created, this setting can be used to prevent future access to the portal for this account, without deleting the user altogether.
8. Select the appropriate option button to define whether **User can manage other users**.
   Setting this option to **Yes** enables the user to create new portal users and to manage existing portal users, including assigning new passwords to other users.
9. Click **[Save and Exit]**.
   The new user is added to the list of authorized portal users. Currently, the new user has no role allocated.

Managing Portal Users

The primary login account for the portal is the default administrator account that you are given when provisioned with the cloud security services. This account has permission to configure all provisioned services, create new users, and define user roles. To prevent accidental deletion of all portal users, this primary account cannot be deleted.

We recommend that you set up all of your users with named accounts, and only use the primary login account as a default account to ensure that there is always an account that has full permissions.

To view existing portal users:

1. Select **Administration > User Management**.
   The names of the portal users that you manage and their logins are listed.
   Use the search facility or the navigation buttons to locate the required user.
2. To view and edit more details of the user, including their roles, click the user's name.

To delete a portal user:

1. Select **Administration > User Management**.
2. Select the user to delete by ticking the checkbox to the left of their name.
3. Click **Delete selected**.

To edit a user's details:

1. Select **Administration > User Management**.
2. Use the search facility or the navigation buttons to locate the required user.
3. Click the user's name.
   The details of the user display.
4. Edit the details as appropriate.
5. Click **[Save and Exit]**.

Defining Standard Roles

Assigning a role to a user gives permissions to view and configure areas and settings in the portal.

A “standard” role enables you to grant access to all or a subset of settings in the portal. Defining a standard role for a user enables you to grant permission to view and, where applicable, edit settings in specific areas of the portal.

A user can be assigned more than one role.

The standard roles are as follows:

Full access	View and edit configurations, generate reports, and view dashboards for all of your services and domains. Access the **Administration** screens to manage users and make change requests.
Reports	View dashboards and generate reports for all of your services and domains. The user will not see the **Services** and **Administration** sections of the portal.

Support	Access all of the **Support** pages. The user will not see the **Services**, **Administration**, and **Reports** sections of the portal.
Service	View and edit configurations and generate reports for all provisioned domains for the service(s) selected from the list. The user will not see the **Administration** section of the portal. The user will only see the **Contact Support** page in the **Support** section.

NOTE: To grant permissions for a user to request changes to your provisioned domains, to use the Track and Trace feature, to raise support tickets, etc., you can assign a custom role.

To define a standard role for a user:

1. Select **Administration > User Management**.
2. Select an existing user to allocate a role for (or create a new user).
3. Click the **User roles** tab.
4. Click **Use standard role**.
5. Select the role type to apply for this user.
6. Click **Add role**.
   The role displays in the list on the **User roles** tab.

Defining Custom Roles

Assigning a role to a user gives permissions to view and configure certain areas and settings in the portal.

A "custom" role enables you to define more precisely the areas of the portal that a user can access, including the ability to make change requests to your provisioned setup. Defining a custom role for a user enables you to grant permission to view and edit configurations, statistics, and areas of the portal, and to raise change requests. Custom roles can be applied for all or specific services and domains. However, domain settings do not apply for some roles and some services.

A user can be assigned more than one role.

The uses of custom roles are explained in the following table:

Custom Role	Description
Edit Configuration	Edit the configuration settings for the selected services. To edit configuration settings, the user requires both the **View Configuration** and **Edit Configuration** roles. The user does not see the dashboards and the **Reports** and **Administration** sections of the portal. The user only sees the **Contact Support** page in the **Support** section.
View Configuration	View the current configurations settings for the selected services; no changes can be made. The user does not see the dashboards and the **Reports** and **Administration** sections of the portal. The user only sees the **Contact Support** page in the **Support** section.
View Statistics	View the dashboards and generate reports for the selected services. The user does not see the dashboards and the **Services** and **Administration** sections of the portal. The user only sees the **Contact Support** page in the **Support** section.
Track and Trace	Perform a search for an individual email on behalf of other people in the organization by the Track and Trace feature in the **Support** section. This role is only visible if your organization is provisioned to use Track and Trace. The user does not see the dashboards and the **Services**, **Administration**, and **Reports** sections of the portal. The user only sees the **Track and Trace** page and **Contact Support** page in the **Support** section.
View Service Alerts	View the **Service Alerts** page in the **Support** section. View the **Contact Support** page in the **Support** section. The user does not see the **Services**, **Administration**, and **Reports** sections of the portal.
View News Alerts	View the **News Alerts** page in the **Support** section. View the **Contact Support** page in the **Support** section. The user does not see the **Services**, **Administration**, and **Reports** sections of the portal.
View Intelligence	View the **Intelligence** page in the **Support** section. View the **Contact Support** page in the **Support** section. The user does not see the **Services**, **Administration**, and **Reports** sections of the portal.
View Support Content	View the **Online Help** page in the **Support** section. View the **Contact Support** page in the **Support** section.

Custom Role	Description
	View the **Contact Support** area in the **Support** section. The user does not see the **Services**, **Administration**, and **Reports** sections of the portal.

To define a custom role for a user:

1. Select **Administration > User Management**.
2. Select an existing user to allocate a role for (or create a new user).
3. Click the **User roles** tab.
4. Click **Create custom role**.
5. Select the role to apply for this user from the drop-down list in the **Permission** section.
6. Select the service to apply the permissions for from the drop-down list in the **Services** section.
7. To apply the permission to:
   - All domains – select **All domains**.
   - Selected domains – select **All selected domains**, select the domain(s) to which to apply the role, and click **Add to list**.
     In some circumstances it is useful to exclude domains from the selected domains list. To do so, select the domain(s) to exclude from the role and select **All except selected domains**.
8. Click **Append Role**.
   The role is applied for the user.

Selecting services and domains is not appropriate for certain roles. If any of these are selected, the **Services** and **Domains** section is inactive.

Selecting domains is not appropriate for certain services. If any of these are selected, the **Domains** section is inactive.

Making Domain Changes for Email Services

You can no longer request changes to domains, inbound routes, or outbound routes with the Domain Change Request form.

- To manage your domains, navigate in the portal to **Services > Email Services > Domains**.
- To manage your inbound routes, navigate in the portal to **Services > Email Services > Inbound Routes**.
- To manage your outbound routes, navigate in the portal to **Services > Email Services > Outbound Routes**.

You must complete a Change Request form to add your domain or domains to your Encryption or Archiving/Email Continuity configuration. You can access the necessary forms on the **Change Request form** page. Complete the necessary form or forms and email your request to Order Services.

Managing Your Details in My Profile

Viewing and Editing Your Details in My Profile

The **My Profile** page enables you to makes changes to your preferences for the portal.

In the **My Profile** page you can view your **Login name** and **Email address**.

Full name	Your full name is displayed at the top of any page in the portal. Make the required changes to your name and click **[Save and Exit]**.
Preferred time zone	The time zone that you specify here is used in several pages within the portal. For example, the time zone affects the reporting schedule and some time-related rules in Content Control.
Password	You can change the password that you use to log onto the portal.

Changing Your Time Zone in My Profile

In the **Preferred time zone** drop-down in **My Profile** you establish your default time zone. Your default time zone is used in Report Requests and for other settings such as time-based rules in Content Control.

To change your time zone:

1. Select the **My Profile** link at the top of any page of the portal.
2. In the **User Details** section, select the required time zone from the **Preferred time zone** drop-down.
3. Click **[Save and Exit]**.

Changing Your Password in My Profile.

You change your password in the **My Profile** area within the portal. Your password must be at least eight characters long and must contain at least one of each of the following character types: alphabetic, numeric, and symbol.

To change your password for the portal:

1. Select the **My Profile** link at the top of any page of the portal.
2. In the **My Details** section, select the **[Create new password option]** button.
3. Enter your current password.
4. Enter and confirm your new password.
5. Click **[Save and Exit]**.
   Confirmation that your password has been changed displays.

NOTE: Authorized portal users who have the **Can manage other users** option set to **Yes** can reset passwords for other portal users.