SafeBrands Knowledge Base

Knowledge Base- Setup and how to guides

Table of Contents

Knowledge Base

1. SafeBrands Overview

SafeBrands specializes in corporate domain management and digital brand protection, ensuring the security and integrity of your online assets:

- **Domain Services**: Handles registration for all global TLDs and manages your domain name portfolio.
- **Brand Protection**: Administers your corporate domain portfolio, ensuring your brand and digital trademarks are safeguarded.
- **Monitoring**: Offers solutions that detect, address, and defend against abuses of your brand and trademarks online.

1.1 Platform Features

- **SafeBrands Dashboard**: SafeBrands's dashboard offers users a comprehensive overview of their domain portfolios and brand protection statuses, enabling them to monitor pending requests, recent acquisitions, SSL expirations, and receive crucial updates and news.
- **Brands Tab:** Offers functionalities to manage and view all the registered brands and trademarks. It allows users to associate them with divisions and input all required data for participation in the Trademark Clearinghouse. This ensures a detailed insight and streamlined oversight of brands, facilitating effective brand management and protection
- **Domains Tab:** Enables users to register, oversee, manage, transfer and configure their domain portfolios, ensuring effective domain administration.
- **SSL Certificates Tab:** Provides the ability to buy, manage and renew SSL certificates, ensuring secure and encrypted connections.
- **Brand Protection Tab:** Delivers functionalities for monitoring and safeguarding brands and trademarks against potential infringements and unauthorized uses.
- **Social Media Tab:** Facilitates the management and observation of brand interactions and presence across various social media platforms.

- **Billing Tab:** Serves as the centralized hub for managing billing details, transactions, and payment information.
- **Open Work Tab:** Displays ongoing tasks and pending assignments, allowing for efficient tracking and management of work requests.

1.2 Portal Function Glossary

- **Admonish**: Initiate a Cease-and-Desist procedure.
- **Annotate**: Add comments or notes to a specific domain.
- **Buy**: Utilize our Anonymous Purchase Service where we negotiate the procurement of a domain for you.
- **Delete**: Initiate a domain deletion request.
- **DNS**: Make changes to the Domain Name System records.
- **DNSSEC**: Toggle the Domain Name System Security Extensions.
- **Lock**: Alter a domain's status to either locked or unlocked.
- **Modify**: Update specific domain details like Nameservers or contact information.
- **Read**: View the specifics of a domain.
- **Register**: Secure a new domain.
- **Restore**: Retrieve a previously owned domain.
- **Snapback**: Order a domain that's already registered with the intent to reclaim it.
- **Takedown**: Request for us to disable a website.
- **Transfer**: Initiate a domain transfer request.
- **UDRP**: Begin a process for a Uniform Domain-Name Dispute-Resolution Policy.

2. Logging into Your SafeBrands Account

Follow the steps below to successfully log in to your SafeBrands account:

1) **Navigate to the Login Page**
- Open your web browser and visit home.safebrands.com
2) **Enter Your Credentials**
- In the provided fields, input the username and password that were shared with you when you began your association with SafeBrands.
3) **Two-Factor Authentication (2FA)**
- If mobile 2FA is activated for your account, you'll receive a verification text message on your registered phone number. Input the code from this message into the required field on the website.
- If you're using an Authenticator app, open the app, retrieve the verification code, and enter it on the website.
4) **Complete the Login Process**
- After inputting your 2FA code (if required), proceed to log in.

Note: Your administrator handles the activation of 2FA for your account. We highly recommend that all users take advantage of the 2FA feature for enhanced security.

3. Creating Contacts

Contact handles are used to fill in WHOIS information associated with domain names. Instead of filling in this information every time you register a domain name, you can create pre-populated contact handles. Contacts can be created for one, or all, of the following contact types:

● Owner Contact

● Administrator Contact

● Technical Contact

- Billing Contact

1. To create a contact handle, go to the “Domains” tab and click “Contacts”.
2. Click “Create New Contact”.
3. The mandatory info required is “First Name” & “Last Name”, “Organization”, “Street”, “Zip”, “City”, “Country”, “State” & “Telephone”.
4. We also recommend adding the Organizations ABN number in the “Commercial Register Number” section.
5. Note: for the “First Name” & “Last Name” section, we recommend adding general information such as “Domain Admin”.

6. Click “Create contact handle”.

3.1 Creating Contact Sets

Contact sets allow you to combine different Owner, Administrator, Technical & Billing Contacts. Here you can create your default contact set across all new domain name registrations.

To create a default contact set:

1. Go to the “Domains” tab and click on the “Contact Sets”.
2. Select the Owner, Administrator, Technical & Billing Contacts.
3. Check the “Make this set the default contact handle set” dialog box.
4. Press the “Create Domain contact set” button.

4. Configuring Your Dashboard

Your dashboard is designed for customization and allows you to add, remove, or rearrange various widgets to suit your workflow.

To configure your dashboard:

1. Click the “Dashboard” button to access customization options.

2. Simply drag and drop the tiles, rearranging them to align with your working preferences.

Feel free to experiment with the layout to create a dashboard that best fits your needs.

5. Viewing and Customizing Your Domain Portfolio

To access and view your domain name portfolio:

1. Navigate to the “Domains” tab.
2. Click on the “Portfolio” option.

This action will display your entire domain portfolio.

To customize the way, you view your domain portfolio:

1. Find the Cog icon in the last column of the portfolio view.
2. Click on the Cog to access display options.
3. From here, you can choose various data points to display. Select or deselect the desired data points as needed.
4. Once you've made your selections:
5. Click “Done” if you want this view temporarily.
6. Choose “Set as default” if you'd like to make this your standard portfolio view moving forward.

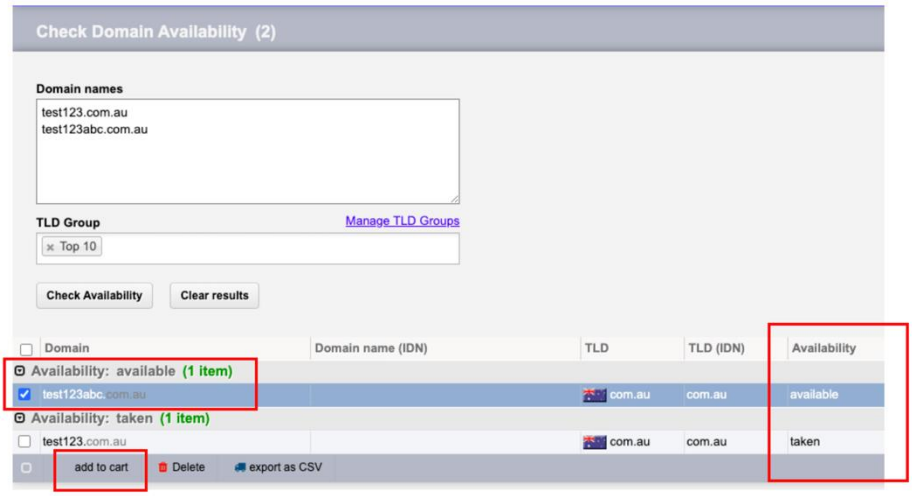
Remember, you can always return to these settings and adjust your view preferences by following the steps above.

6. Registering Multiple Domain Names

Initiating the Registration:

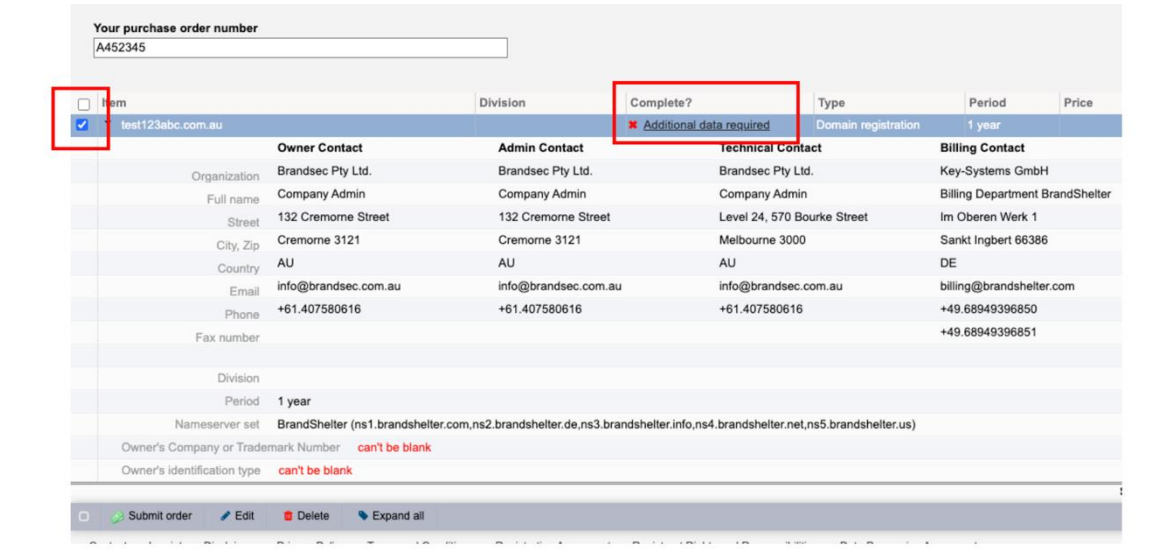
1. Navigate to the “Domains” tab.
2. Click on “Register”.

Checking Domain Availability:



3. Enter your desired domain names. To check multiple domains at once, separate them using commas or place each domain on a new line.
4. Click “Check Availability”.
5. You'll see if each domain is “Available” or “Taken”.
6. To proceed with available domains, check the corresponding boxes and click “Add to Cart”.

Providing Necessary Registration Details:



1. Select the domain names you intend to register. Areas that require information will be highlighted in red.
2. Click on “Additional Data Required” to input the necessary information.

3. Alternatively, if you wish to modify the existing whois data for any domain, click “Edit” next to that domain and follow the on-screen instructions.

Filling Out Additional Data:

1. Once you select the “Additional Data Required” link for a domain, a pop-up window will emerge.
2. Complete the fields highlighted in red.
3. Click “Save” when finished

Reviewing Your Shopping Cart:

1. After providing the necessary details for all selected domains, you'll be redirected to the Shopping Cart.
2. Make sure each domain name you want to register displays "No additional data required" in the "Complete?" column, highlighted in green.

Completing the Purchase:

1. Select the checkboxes next to the domain names you are ready to register.
2. Click the “Submit Order” button to finalize and confirm your domain registration(s).

7. Transferring Domains

Navigate to Transfer Option:

1. Under the "Domains" tab, select “Transfer”.

Input Domain Details:

1. Type in the Domain Name(s) you're looking to transfer.

Authorization Code Entry:

1. For the domain you entered, click on the “Requires Authcode” column marked in red.
2. Provide the necessary Authcode for the domain.

Add to Cart:

1. After entering the Authcode, highlight the domain and click “Add to Cart”.

Verify Information:

1. Domains needing more information will be indicated in red.
2. Those ready for transfer will be marked in green.

Finalize Transfer:

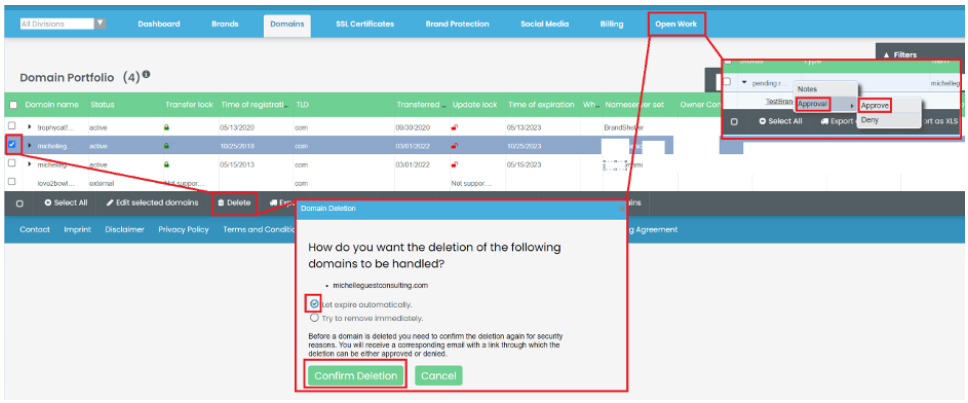
1. Highlight the domain you wish to transfer and press “Submit Order”.

Note: For specific guidelines on managing .com and .net domain transfers, including the use of P-Handles, and a crucial reminder for upcoming bulk domain transfers, please refer to the "Miscellaneous" section below.

8. Setting Domains for Automatic Expiration

1. Navigate to "Domains” followed by “Portfolio”.
2. Select the domains you'd like to set for automatic expiration.
3. Click on 'Delete'.
4. Choose 'Let Expire Automatically' (It's possible to select 'Instant Delete', but it's advisable to be cautious given that clients may reconsider).
5. Click 'Confirm Deletion'.
6. Navigate to 'Open Work'.

7. Select 'Approval' and then click on 'Approve'.



9. Adding New Nameserver Sets

The Portal operates based on predefined Nameservers. To modify a domain's Nameserver, you first need to establish a new set.

Navigating to Nameserver Sets:

1. Head to Domains > Nameserver Sets.

Initiating a New Nameserver Set:

1. Click on “Create new nameserver set”.

Inputting Nameserver Details:

1. Enter the details of the new Nameservers.
2. Proceed by clicking “Create Nameserver set”.

Optional Default Setting:

You can choose to make this new set the default Nameserver for future domain name registrations. Note that this action won't affect the Nameserver settings of your existing domain portfolio.

10. Setting the Default Nameserver in SafeBrands

Both accounts and individual users can have a default nameserver set.

a. If a user lacks a specified default nameserver, the account's setting is utilized.
b. However, if a user has a designated default nameserver, the system bypasses the account's default.

If you establish a nameserver set as the default by modifying it, this adjustment only affects the active user, leaving other users unchanged. Please note, there's currently a glitch where this function isn't working as intended. Changing the default nameserver for a user who has transitioned to another account might also cause issues.

- To modify the account's default setting, navigate to User Menu → Settings → “Domain Preferences (Account)” tab, and adjust it there.

11. Editing a Domain's Nameserver

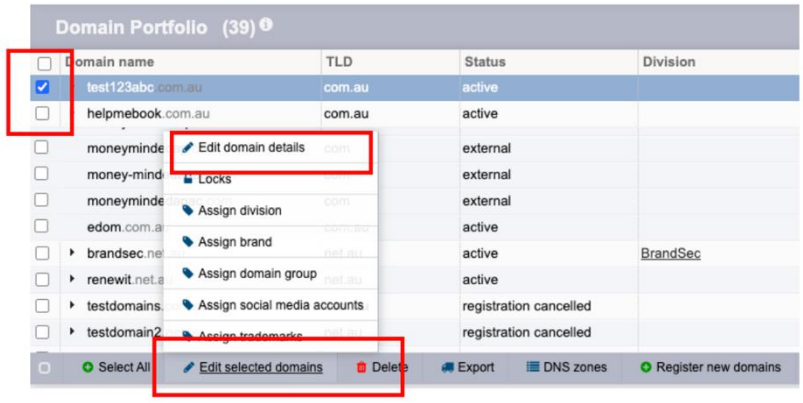
Accessing Domain Portfolio:

1. Navigate to “Domains” and then choose “Portfolio”.

Selecting the Domain:

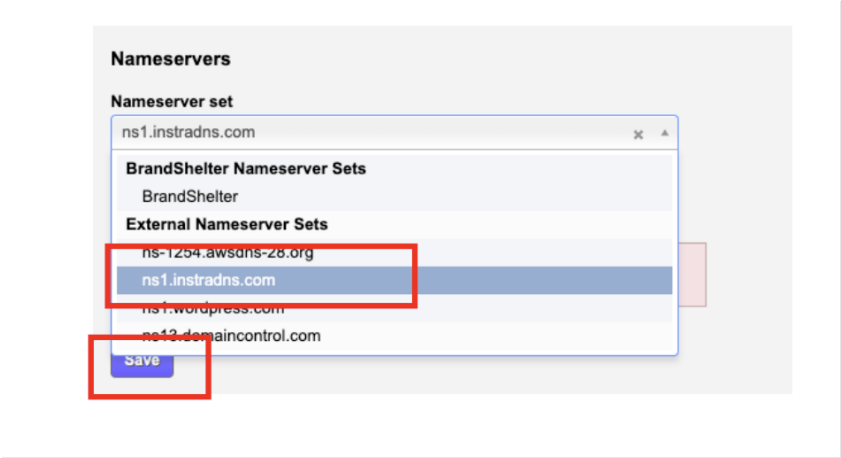
1. Identify and select the domain name you want to edit.

Accessing Domain Details:



1. Hover over the option “edit selected domains” and then click on “Edit domain details".

Changing the Nameserver:



1. Scroll to find the Nameserver section. Choose the desired Name Server Set from the options available.

Confirmation:

1. Click “Save”. Upon successful modification, you will receive an email confirming the changes to the Nameserver.

12. Managing Nameserver Glue Records

What is a Glue Record (or Additional record)?

A glue record (or additional record) also known as A Record (or IP Address) is a type of DNS record that associates a domain name with an IP address, allowing the domain name to be translated into the appropriate IP address when it is accessed. Setting up "glue records" is the act of showing the IP address of authoritative DNS servers on a domain name at the registry level in addition to the host names.

12.1 Why are Glue Records Important?

When configuring a domain’s DNS settings, it's common to assign nameservers that are subdomains of the domain itself. For example, for the domain mydomain.com, the nameservers might be ns1.mydomain.com and ns2.mydomain.com. In such cases, a query for the domain name might result in a circular reference, where to know the IP address of ns1.mydomain.com, one needs to know the IP address of mydomain.com first, creating a loop.

Glue records break this loop by providing the IP address of the nameservers directly, allowing for the correct resolution of the domain name and its associated subdomains. They ensure the stability and reliability of the domain’s DNS configuration, preventing potential accessibility issues.

12.2 When do you need a glue record?

Glue records are particularly important when the nameservers (eg. ns1, ns2) for a domain name (eg. domain.com) are the subdomains of the domain name itself.

Example

Domain name: mydomain.com

Nameservers: alfred.cloudflare.net, jessie.cloudflare.net

No Glue Record required

Domain name: mydomain.com

Nameservers: ns1.mydomain.com, ns2.mydomain.com

Glue Records required for ns1.mydomain.com and ns2.mydomain.com

~~Navigating to the section where you can modify or establish Nameserver Glue records is straightforward. After submission, the modifications take effect almost immediately.~~

12.3 Updating Existing Glue Records

1. Go to **Domain Tools**.
2. Select **NameServer Glue Records**.
3. Click on **Edit**.
4. Choose **Update IP Address**.
5. Finally, click on **Update Nameserver**.

12.4 Setting Up New Glue Records

1. Navigate to **Domain Tools**.
2. Choose **NameServer Glue Records**.
3. Select **Register New Nameserver**.
4. Enter the necessary Nameserver details.
5. Click on **Create Nameserver** to finalize.

13. Steps to Add DNS

Accessing the Domain Menu:

1. Go to "Domains", find the desired domain name, hover over its burger lines icon, and click “Open Action Menu”. Then, select the “DNS” option.

Creating a New Resource Record:

1. Click on “New resource record”.

Setting Record Details:

1. Choose the desired record type.
2. Input the necessary DNS content. If you intend to inform others about this new DNS record, simply add their details in the provided request section.

Finalizing the Resource Record:

1. Click “Create resource record”. Remember, this action will only create the record and won't publish it immediately.

Publishing the DNS Record:

1. Click on “Show local changes” to view the newly added record.
2. Review all the changes, and if everything looks accurate, click the “Publish” button to make the DNS record live.

13.1 Steps to Edit DNS

Accessing the Domain's DNS Menu:

1. Navigate to the "Domains" tab.
2. Find the domain name you want to modify, hover over its burger lines icon, and click “Open Action Menu”. From the dropdown, select “DNS”.

Selecting the DNS Record to Edit:

1. Hover over the burger lines next to the specific DNS record you intend to edit and click on “Edit”.

Updating the Record Details:

1. Make the necessary modifications to the DNS record.
2. Click “Update Record”. Remember, this action only initiates a change request and doesn't apply the modifications immediately.

Publishing the Modified DNS Record:

1. To finalize and apply your changes, click on “Show local changes”.

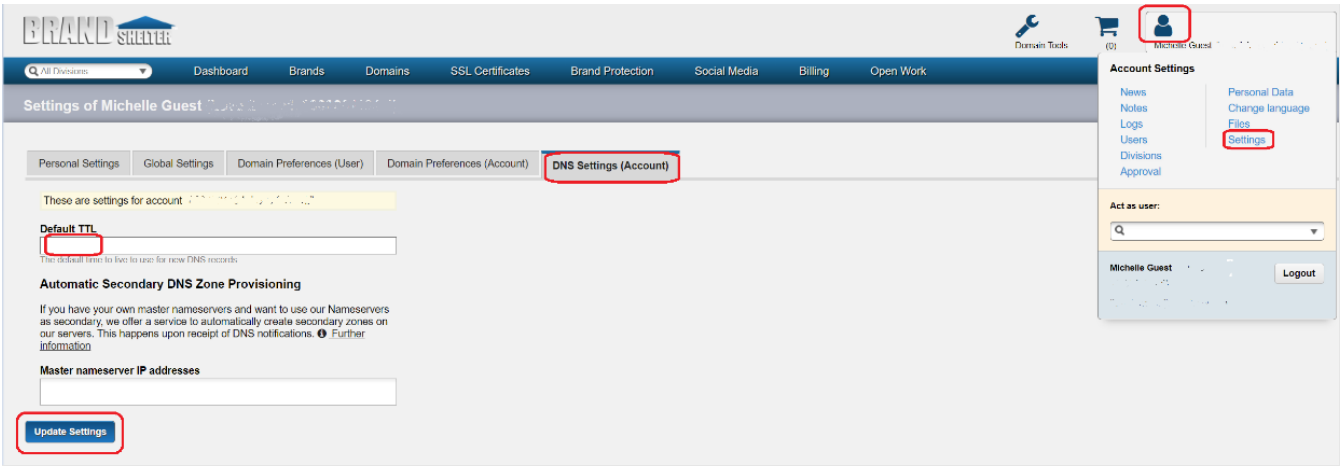
2. Review your edits and if they're accurate, click “Publish Changes” to update the DNS record.

14. Adjusting the Default TTL for DNS Records

1. Navigate to the Human Silhouette icon and hover over it.
2. Select "Settings" from the dropdown.
3. Access the "DNS Settings (Account)" tab.
4. Input your desired TTL value. (Note: The default for both SafeBrands and UltraDNS is 300.)
5. Confirm your changes by clicking "Update Settings."

Important Considerations:

- Modifying the default TTL won't affect the TTL of previously established records. To adjust the TTL for existing records, please edit them directly within the zone.
- The TTL adjustment will apply only to the "SafeBrands" Name Server set marked as the default during the update. For instance, if UltraDNS is the default, the change will solely affect UltraDNS. However, if a third-party Name Server set is the default, the TTL will be updated across all SafeBrands Name Server sets linked to that client account, such as SafeBrands Standard, UltraDNS, Premium DNS, and more.



15. Ordering an SSL Certificate

Starting the Order:

1. Navigate to the SSL tab.
2. Click “New SSL Certificate”.

Choosing an SSL Certificate:

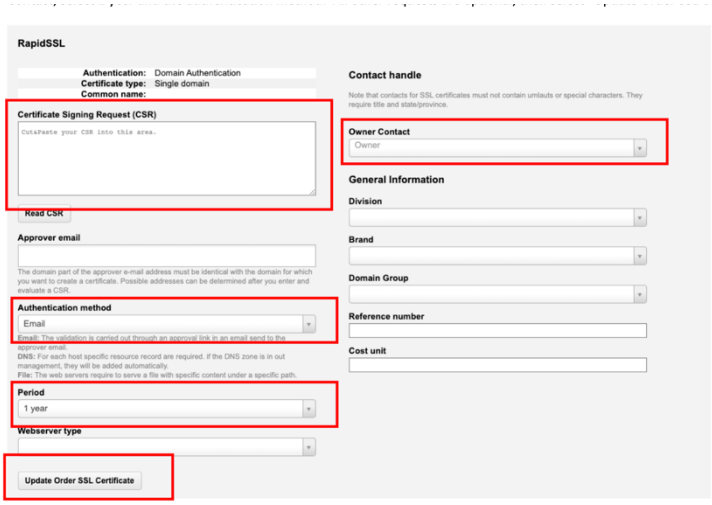
1. SSL certificates can be viewed by either ‘Brand’ or by ‘Validation’ type.
2. Pick the SSL you need and click ‘Put into cart’.

**About Validation Types:

- Domain Validation (DV): Confirms that the applicant has administrative rights to the domain in the certificate.
- Organization Validation (OV): Authenticates business identity, verifies the domain name, and ensures the organizational contact is an authorized employee.
- Extended Validation (EV): Offers the highest level of authentication and requires an acknowledgment or agreement from the corporation.

Note: For guidance on selecting the appropriate SSL validation type, refer to this section.

Providing Necessary Data:



1. Click on the “Additional data required” link under the “Complete?” column.
2. Input the CSR into the provided space and then click “Read CSR” to verify the details.
3. Add an Owner Contact, choose the duration for 1 year, and specify the authentication method. Other inputs are optional. Finally, click “Update Order SSL Certificate”.

Approval Email Details:

The approval email address should match the domain's WHOIS record for the certificate creation. Upon evaluating a CSR, potential email addresses will become apparent. If our system can retrieve an email from the domain's WHOIS automatically, it will display the WHOIS Admin email.

For convenience, the following predefined approver email addresses can also be used:

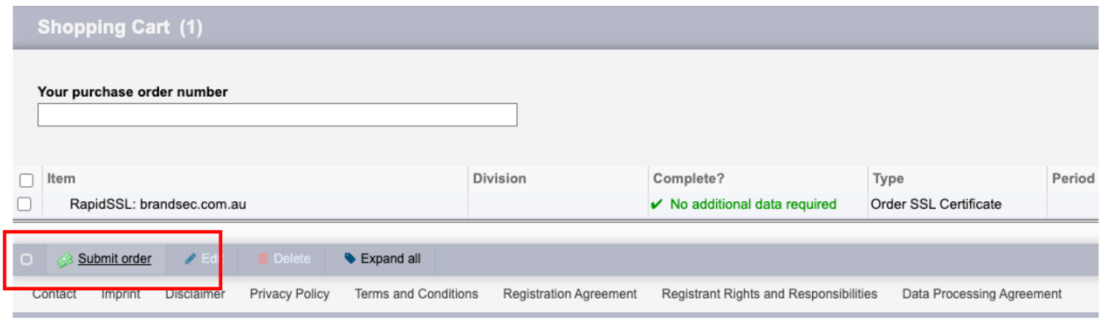
admin@...
administrator@...
hostmaster@...
webmaster@...
postmaster@...

Domain Validation Methods:

- **Email**: An approval link is sent to the approver email.

- **DNS**: Specific resource records are needed for each host. These records will be added automatically if the DNS zone is managed by us.
- **File**: A specific file with certain content must be hosted under a particular path on web servers.

Finalizing the Order:



1. Choose the domain name.
2. Click “Submit Order”.

SSL Renewals

**SSL Renewal Alert Emails

We send out two distinct email notifications based on your renewal settings: one for manual renewal and another for automatic renewal. Both types are dispatched starting from 8 weeks before the SSL certificate expires.

For Manual Renewal:

- Notification at 6 weeks before expiration.

For Automatic Renewal:

- 8 weeks before: "Certificate Expiration Alert"
- 6 weeks before: "Second Certificate Expiration Reminder"
- 5 weeks before: "Final Certificate Expiration Reminder"

16. User Management: Setting Up and Deleting Users

16.1 Creating a New User

1. Hover over your name and choose “Users”.
2. Click on “Create new subuser”.
3. Fill in the User Details. Ensure you provide at least the “First Name”, “Last Name”, “Organization”, address, a valid email address, and mobile (cell) phone number.
4. After entering the details, click on “Create User”.
5. An email containing password setup instructions and a link will be automatically sent to the new user. Please note, this link will expire after 72 hours.
6. If needed, admins can also prompt a password reset by clicking on the burger icon next to the user’s name and selecting “Trigger Password Reset”.

16.2 Deleting a User

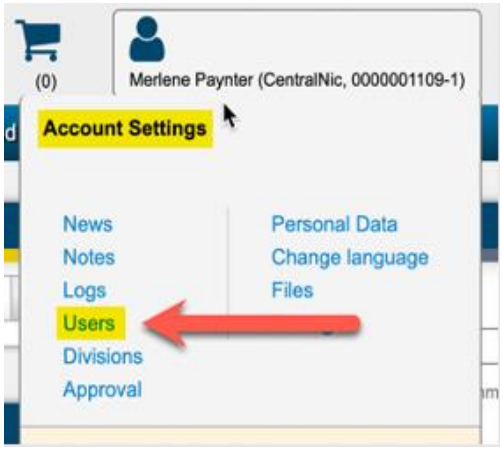
- Navigate to “Account Settings.”
- Click on “User” to view all users on your SafeBrands platform.
- Locate the user you wish to remove.
- Right-click on the desired user.
- Select the 'delete' option.
- Confirm your decision, and the user will be removed from the platform.

17. User Permission Configuration

Setting up user permissions is a pivotal component in managing access within your portal. This process is primarily about determining what each user can and cannot do within the account.

Step 1: Set Up User Permissions

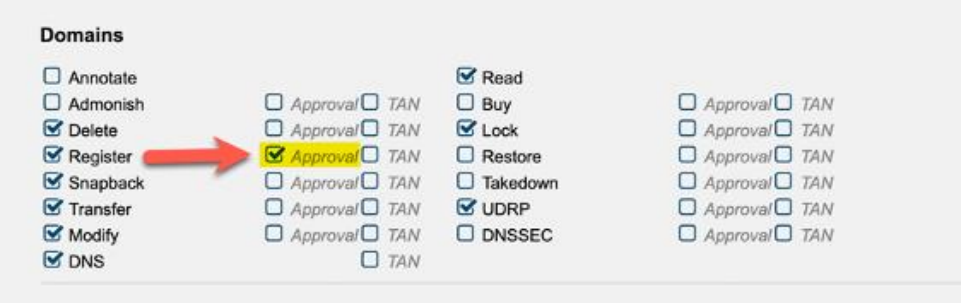
1. Navigate to Account Settings > Users.



2. From the list of users, select the one you wish to assign approval rules to.
3. Right-click and opt for Edit permissions from the dropdown menu.

4. In the permissions interface, locate the "Domains" section. This area lets you define which actions the user can perform directly, and which ones need higher approval. Adjust the settings by checking the appropriate boxes. (For a detailed understanding of each permission, refer to the portal function definitions).
5. After setting up user permissions, you may optionally define general account approval guidelines. Tailor them for specific users as needed.

This is not a mandatory step, but it can add an additional layer of control and security to user actions within the portal.

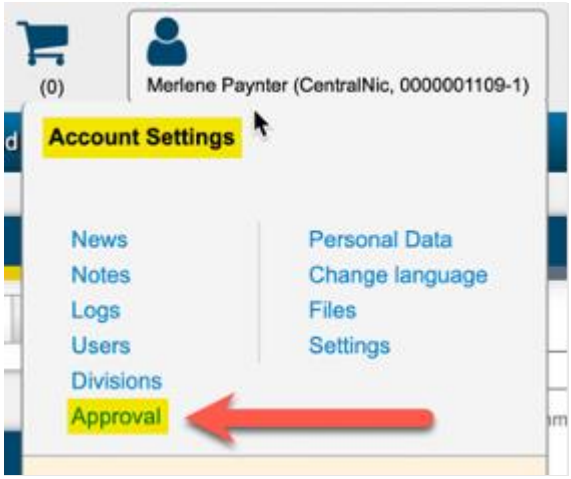


***When assigning these permissions:*

1. *Opt for "Select all" to grant the user comprehensive access throughout the portal. This is generally suggested only for portal admins.*
2. *Use "Select all" at the specific function level to provide complete access to that function. Typically recommended for System Admins.*
3. *Alternatively, specify the access level individually for each function. This selective assignment is the recommended approach for most users.*

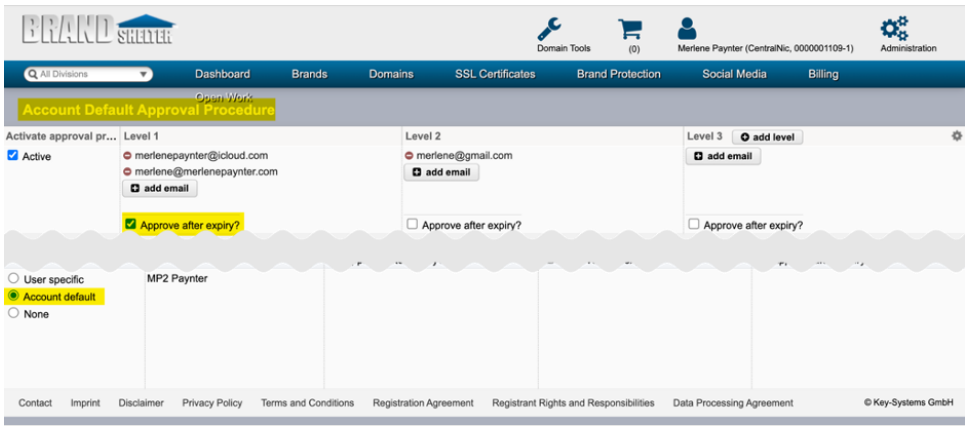
Step 2: Creating Approval Rules

1. Go to Account Settings" >Approval.



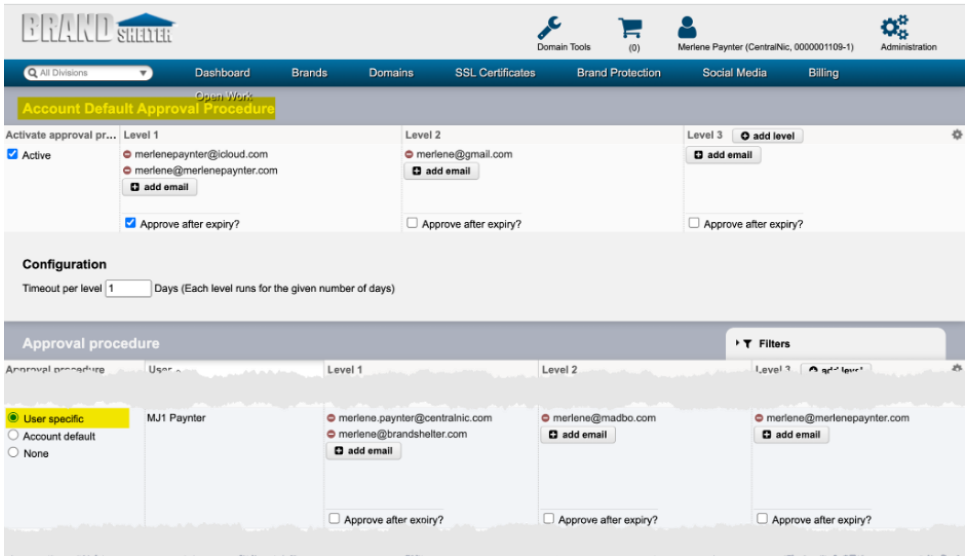
2. Here, you'll have the option to institute an "**Account Default Approval**" Procedure. This allows you to specify one or multiple email addresses

that will receive an approval notification for actions like domain registration.

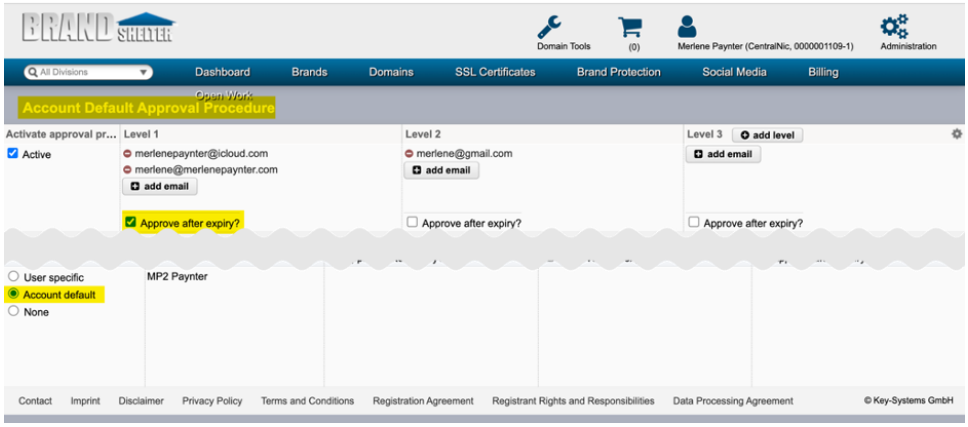


This approval method can be multi-tiered, where an email recipient at one level must grant permission before the next level recipient is approached for their consent.

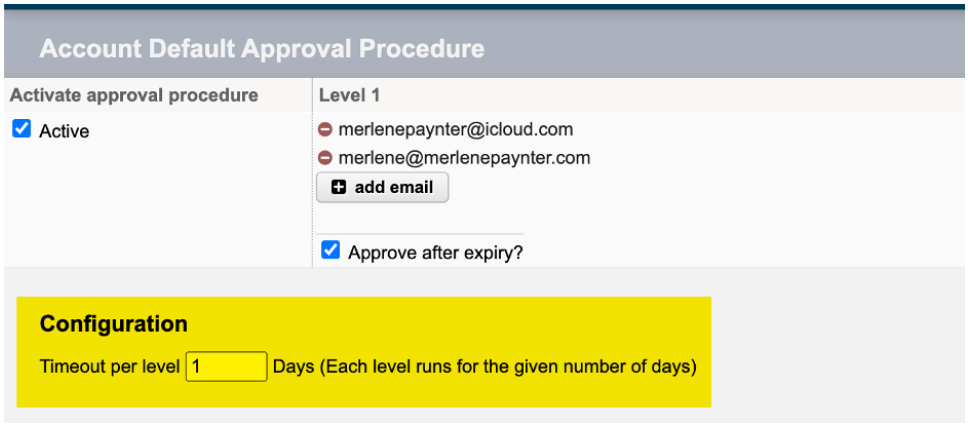
3. For certain users, you might wish to apply unique approval guidelines tailored to them. To achieve this, choose the "user-specific" option within the approval procedure section for that individual.



4. Occasionally, you might want the procedure to progress even if not all approvers have responded. To do this, ensure the “**Approve after expiry**” box is checked. This means that, after a certain time, the approval request will move up to the next level.

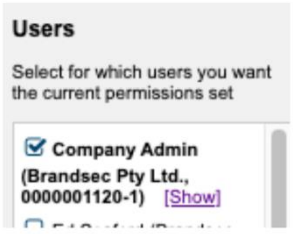


5. To determine how long an approval request waits before it's either rejected or advanced to the next level, set your preference under **Configuration > Timeout per level**.



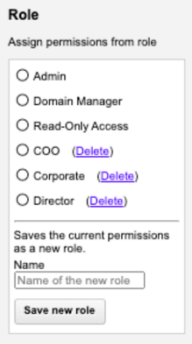
17.1 Permission Management Hacks

Bulk User Permissions:



- For setting permissions for multiple users simultaneously, simply click on the relevant users listed on the right-hand side.

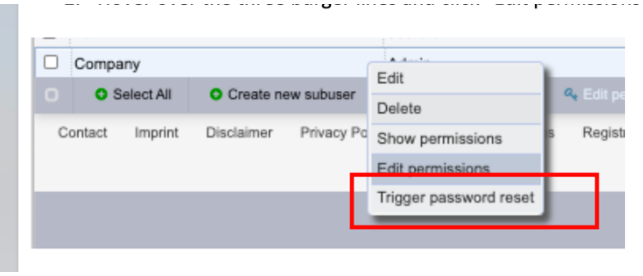
Role-Based Permissions:



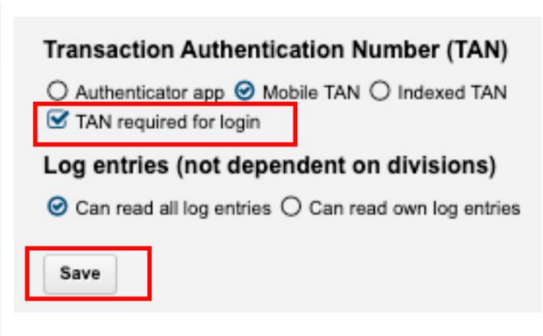
- Enhance permission management efficiency by defining permissions based on roles. To do this, either click on an existing role or create a new one to assign specific permissions.

18. Setting Up 2-Factor Authentication (2FA)

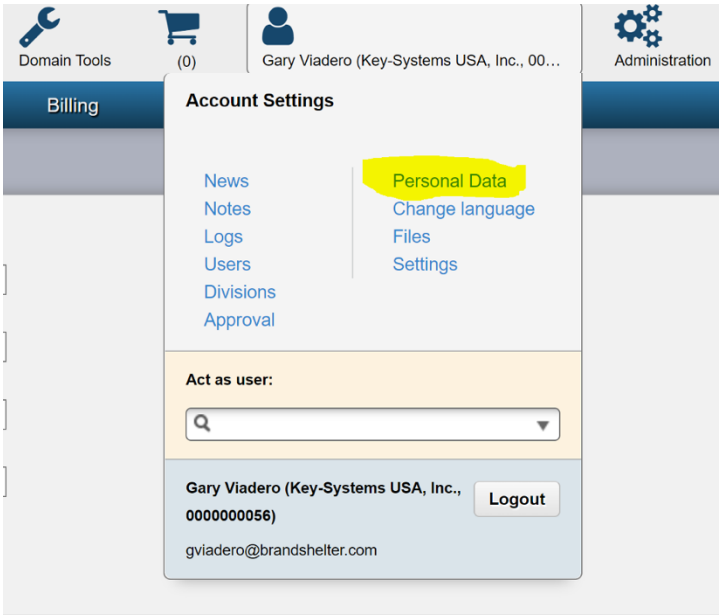
2-Factor Authentication (2FA) adds an extra layer of security, ensuring that even if someone obtains your password, they can't access your account without a second verification step. By enabling 2FA on SafeBrands, users significantly fortify their defense against unauthorized access and potential cyber threats.



1. Navigate to “Account Settings” followed by “User”.
2. Hover over the three burger lines and click “Edit permissions”.
3. Scroll to the bottom of the page and locate the Mobile TAN section.
4. Check the box labeled “TAN required for login” to enable 2FA.
5. Click the Save button to finalize changes.



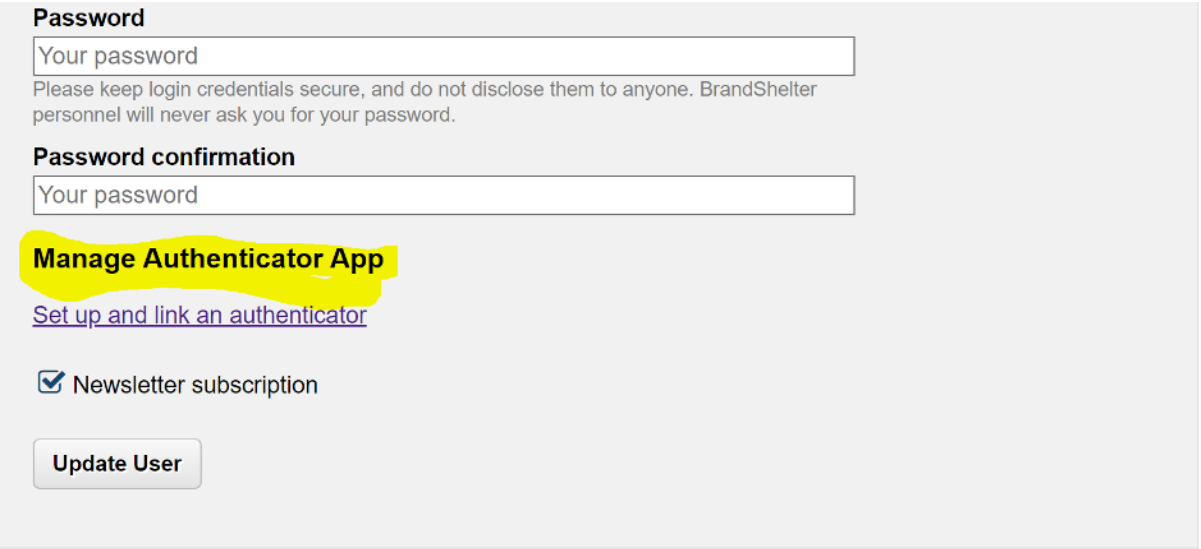
18.1 Setting Up 2FA Using Google Authenticator



1. Setup in SafeBrands:

Access Authenticator Settings:

1. Go to “Account Settings” and then “Personal data”.
2. Scroll down and choose “Manage Authenticator App”.
3. Click on “Set up and link an authenticator”.



Scan QR Code:

- Open Google Authenticator on your mobile device.
- Tap the “+” icon to add a new entry.
- Choose “Scan a QR Code” and scan the QR code displayed on SafeBrands. This process sets up SafeBrands within your Google Authenticator app, adding it to your list of authenticator applications.

Verify Setup:

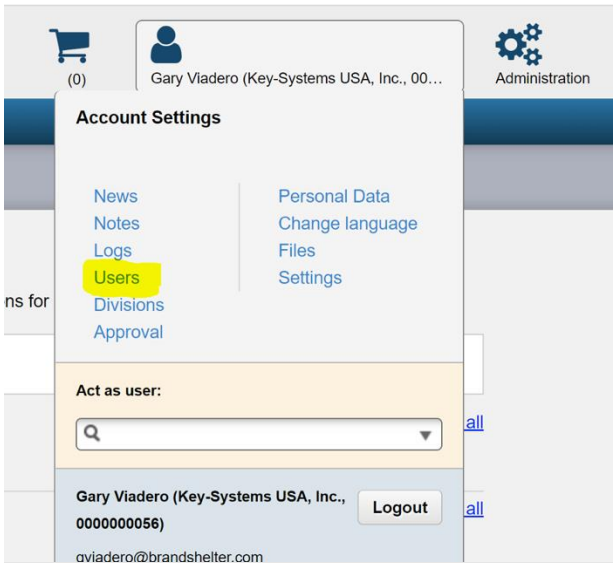
- View the newly added SafeBrands entry on Google Authenticator.
- The app will display a time-sensitive code for SafeBrands. This is the TAN code.
- Enter this TAN code into the Tan Field on SafeBrands to verify the setup.

Note Fallback Codes:

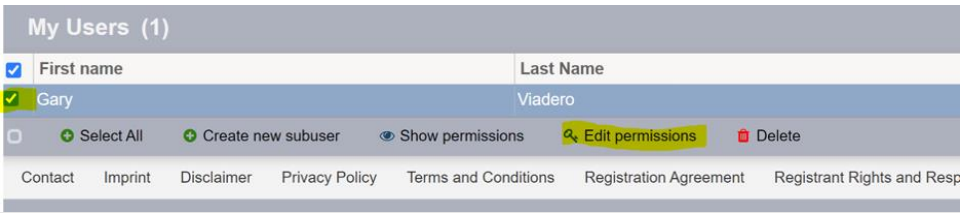
- SafeBrands will provide you with five "Fallback" codes.
- Save these codes securely; they’re for emergency access.

2. Enable TAN Login:

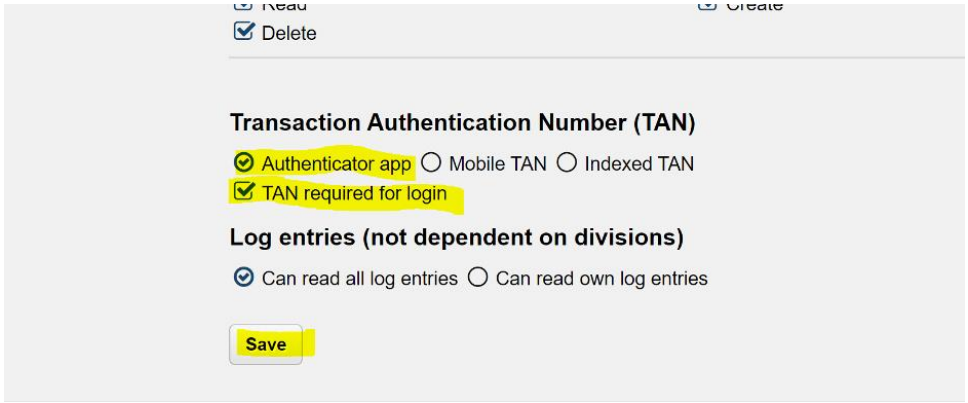
- Go to “Users” and select your account.
- Click “edit permissions”.
- Scroll to the bottom and toggle “TAN required for login”.
- Click “SAVE”.



- Select your Account and click "**edit permissions**"



- Scroll to the bottom of the screen and select "TAN required for login"
- Click SAVE



From your next login onward, after entering your password, you will be prompted for a TAN from your Google Authenticator app. Ensure to have your mobile device accessible for a smooth login process.

Note: Make sure to save the provided fallback codes when setting up the authenticator. These codes are essential if you need to set up the authenticator on a new device.

Miscellaneous

1. Guideline for Managing Domain Transfers

Background:
This guideline is designed to streamline domain transfers across various TLDs and to reduce administrative tasks post-transfer.

Adding P-Handles to Transfer Orders:

Importance:

- Including P-Handles during the transfer process allows our system to automatically update the P-Handles upon successful transfer.
- Additionally, with the domain associated with the P-Handles, the system locks the domain automatically.

Benefit:

- Decreases the number of domains listed under 'domains without transfer lock', ensuring efficient domain management.

1.1 Reminder for Bulk Domain Transfers

Action Needed:
For every domain you are transferring, ensure you add all necessary P-Handles before submitting the transfer order. For specific TLD requirements, refer to the Dashboard or consult your Account Manager.

Reasons:

- This helps avoid a multitude of support tickets and prevents unnecessary email broadcasts regarding urgent update requests.

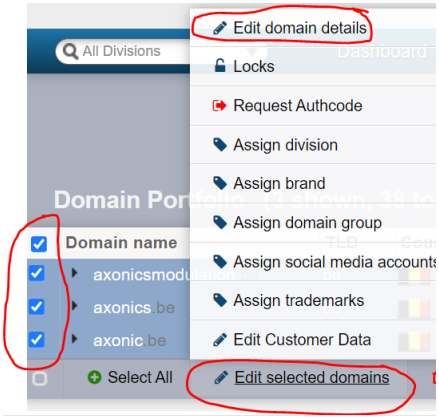
- Automatic domain locking occurs upon handle assignment, saving considerable working hours by reducing manual interventions post-transfer.

Procedure:
Assigning a predefined contact set takes less than 5 seconds. If you need to search for a specific handle, it might take up to 20 seconds. This minor time investment upfront greatly streamlines post-transfer processes.

Handle Selection:
It's crucial to decide on which contact handles to use in coordination with the Client and the Account Manager before initiating the transfer.

2. Procedure to Request Authorization Code for Domains

Search and Select:

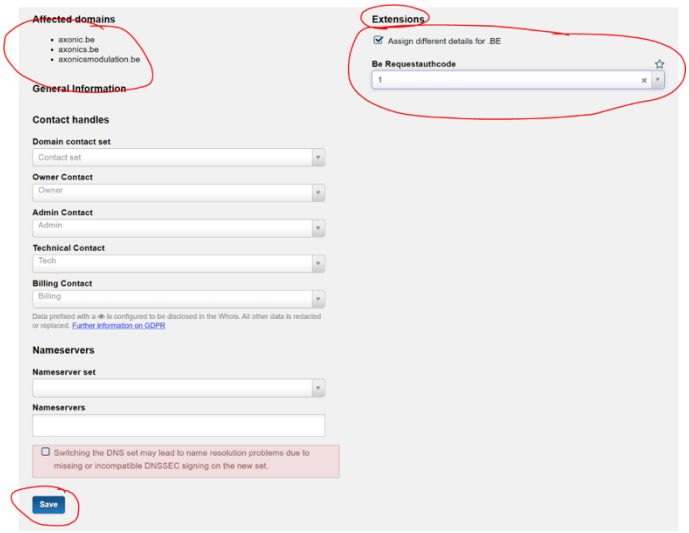


1. **Locate Desired Domains:** Utilize the search feature within the Dashboard to find the domains you intend to modify.
2. Once located, check the corresponding boxes next to them.
3. Click on "**Edit selected domains"** followed by "**Edit domain details"**.

Verify Domain Selection:

Quickly review to ensure you've selected the intended domains under "**Affected domains**".

Adjust Domain Extensions:



1. Navigate to “**Extensions”**.
2. Here, you can modify the details for specific domain extensions as per your requirements. Refer to the Dashboard or consult your Account Manager for specific details and requirements for each TLD.
3. Choose the option "1" (indicating 'Yes' for this process).
4. Click “**Save**” to apply changes.

Awaiting Auth Code:

- Following your submission, the current domain holder will receive an email from the registry.
- This email will contain the auth code, composed of 5 groups with 3 numbers each, and the expiration date for the code.

3. Understanding SSL Certificates

SSL certificates serve as a protective shield for online data transfers, but not all certificates are created equal. Let's delve into the differences between the commonly used Standard SSL Certificate and the more rigorous Extended Validation Certificate.

Difference Between Standard SSL Certificate and Extended Validation Certificate

- **Validation Levels**: While both SSL certificate types offer industry-standard encryption, their level of validation differs. Typically, when referring to a "standard SSL", one means a single domain, domain validated (DV) SSL certificate. These certificates are swiftly registered, affordable, yet might not provide the desired level of trust for business-centric tasks. On the other hand, an Extended Validation (EV) certificate involves a meticulous validation process where the issuing authority verifies multiple facets of your company, ensuring a higher level of trust.

- **Pricing Disparity**: You might wonder why EV certificates come with a higher price tag compared to standard SSL certificates. The answer lies in the detailed validation process. The extra effort and resources expended by the Certificate Authority to vet and issue an EV certificate naturally translates to a higher cost.
- **Considerations for Extended Validation Certificates**: Before opting for an EV certificate, consider the following:
    - **Urgency**: Need a certificate in a jiffy or at a lower cost? A standard SSL might be your go-to.
    - **Trust Factor**: If instilling maximum trust in your visitors is pivotal, and you wish to showcase serious commitment to security, an EV certificate should be your choice.
    - **Nature of Your Site**: Sites handling ecommerce, finance, healthcare, or any sensitive data should ideally lean towards EV certificates for enhanced credibility and security.

4. Conducting an Owner Update for Domains with Trustee Service

When updating the owner of a domain that utilizes our Trustee service to a new owner contact, it is crucial to adhere to specific steps to avoid any discrepancies in the domain status and unnecessary charges for inactive Trustee services. The following process is applicable to all TLDs being transferred away from our Trustee services.

Steps to Follow:

- **Check Extension Field:** Before submitting the transfer order, ensure that the extension field is accurately filled in. This is crucial for processing the transfer successfully.
- **Avoiding Unnecessary Charges:** If the extension field is omitted, the trade may still process successfully (provided the new owner meets the registration criteria). However, in SafeBrands, the domain status might display as 'using the Trustee'. This discrepancy can lead to incurring charges for a Trustee service that is no longer active.

4.1 Finding Information on Specific TLD Requirements

For the specific requirements and details pertaining to the transfer of each TLD, especially those with Trustee service:

- **Dashboard:** Navigate to your SafeBrands dashboard where you can find comprehensive information and guidelines on transferring domains with Trustee service.
- **Shopping Flow:** During the transfer process, refer to the Shopping Flow section for specific instructions and requirements for each TLD.
- **Account Manager:** Consult with your Account Manager to gain insights and clarification on any specific details or requirements related to domain transfers with Trustee service.

5. SafeBrands Glossary

- **AnyCast**

A network addressing and routing method in IPv6 where multiple servers share the same IP address. When data is sent to that IP address, it is directed to the nearest or most optimal server based on factors like proximity or server load. This helps in efficient data routing and load distribution across a network.

- **A Record**

An A Record is a type of DNS record that maps a domain name or subdomain to its corresponding IPv4 address. It allows browsers and other clients to determine the IP address of a particular domain, facilitating the process of connecting to websites and other resources on the internet. For instance, if a user wishes to visit example.com, the A Record will direct the user's browser to the correct server IP address associated with that domain.

- **Backorder services (Snapback or Snap services)**

Services designed to monitor registered domains and register them immediately after deletion by the prior owner.

- **Brandjacking**

The act of hijacking a company's online identity to manipulate or harm its brand reputation. The term "Brandjacking" is a fusion of "branding" and "hijacking" and has been in use since around 2007.

ccTLD

Short for "country code top level domain", it represents a country-specific domain suffix. Every country has a unique two-letter code (ALPHA-2) based on ISO 3166 standards. Notable ccTLDs include .de (Germany), .uk (United Kingdom), and .us (USA).

Claims Period or Claims Phase

During this 90-day duration with the TMCH's "Trademark Claims" service, both the domain registrant and trademark holder are notified when someone tries to register a domain that's recorded in the TMCH database as a validated trademark.

Counterfeiting

Imitation of branded products, posing risks to brand reputation, sales, and consumer safety.

Cybersquatting

The act of registering domain names to which the registrant has no rightful claim, often brand names. Also termed "brandjacking".

Data Center

Facility housing central computer technology for one or multiple organizations.

DNS (Domain Name System)

DNS links domain names with their respective IP addresses, facilitating the resolution of full domain names, including TLDs. By translating domain names to IP addresses, DNS provides users with an easier way to access websites.

DNS Propagation

DNS propagation is the time it takes updates to DNS records to be in full effect across all servers on the internet. Changes don't take effect instantaneously because nameservers store domain record information in their cache for a certain amount of time before refreshing. Your domain won't experience downtime from properly planned record changes, but some users will still see a cached version of your site until all servers have propagated.

There's no set amount of time for propagation, but DNS typically propagates within a few hours. On occasion, it can take up to 72 hours.

Several factors determine the timeframe for propagation, including your internet service provider (ISP), your domain's registry and the Time to Live (TTL) values of your DNS records.

DNSSEC (Domain Name Systems Security Extensions)

An enhancement to the DNS, DNSSEC ensures the authenticity and integrity of DNS data. With DNSSEC, users can confirm that the retrieved zone information matches the original data as authorized by the zone creator. Note: DNS data remains unencrypted.

Domain Name (Fully Qualified Domain Name (FQDN))

An internet address or web address or an internet domain identifier such as safebrands.com is called a domain. It is part of the URL of a website (e.g. http://www.safebrands.com) and identifies computers on the Internet.

Domain Transfer

The process of moving a domain from one registrar to another, initiated by the receiving registrar. ICANN standardized guidelines in 2004 to ensure this transfer is both straightforward and secure.

dotBrand

ICANN is anticipated to open applications for new Top-Level Domains in the coming years. This will allow businesses and organizations to acquire their own brand-specific Top-Level Domain. SafeBrands assists throughout the ICANN application process and with the registry function setup.

DPML Plus

A service by Donuts Registry that blocks the registration of domain names listed as trademarks in the Trademark Clearinghouse (TMCH). It's an upgraded version of the earlier DPML service.

Dropped Domain

Domains that aren't renewed after their registration period ends and subsequently become available for new registration.

Grey Market

While the black market pertains to illegal trade, the grey market deals with goods traded through channels that aren't officially regulated, placing them in a legal "grey zone."

gTLD (Generic Top-Level Domain)

Domains such as .com, .xyz, or .club fall under gTLD.

IANA (Internet Assigned Numbers Authority)

A division of ICANN responsible for the assignment of numbers and names online. As the operator of the Domain Name System (DNS) and allocator of IP addresses, it's among the internet's foundational entities.

ICANN (Internet Corporation for Assigned Names and Numbers)

A non-profit that oversees the coordination of names and addresses online. As the primary internet authority, ICANN manages DNS, ensures unique IP address assignment, and maintains overall internet stability.

IDN (Internationalized Domain Name)

A domain name accommodating non-ASCII characters, such as umlauts or characters from non-Latin alphabets. The IDNA (Internationalizing Domain Names in Applications) standard allows for these characters, even though they weren't originally part of the DNS.

Internet Piracy

The unauthorized distribution, copying, or downloading of copyrighted digital content like films, music, or software.

Landrush Phase

A time-limited phase following the Sunrise phase in the rollout of a new Top-Level Domain. During this phase, registrants can apply for domain names, even those without trademark protection, with the domain's governing registry setting the requirements.

Local Presence Service

Some domain registration authorities may impose specific conditions on registrations. For domains requiring a local contact, SafeBrands offers "local presence services." We guide clients on whether a "trustee" is necessary and handle trust agreement processes with local partners.

Monitoring

Monitoring encompasses systematic tracking, observation, or surveillance of a procedure using technological tools. Brand Shelter's monitoring services, for instance, alert you when newly registered trademarks match your brand, safeguarding it from cybersquatting.

Name Server

A name server translates computer or service names into data that machines can understand, responding to domain name queries based on its DNS database. It's an integral component of the DNS.

Namespace

In informatics, a namespace prevents naming conflicts by organizing allocations hierarchically. The elements of a domain name, delineated by dots, indicate different hierarchical namespaces within the DNS. For instance, in the sequence top-level domain, second-level domain, and third-level domain, each represents a unique namespace. This arrangement enables the distinct registration of domains like SafeBrands.com and SafeBrands.co.uk.

New TLDs (Top-Level Domains)

New gTLDs are domain extensions that organizations proposed to ICANN, the foremost internet authority, in 2012. These extensions range from three to 63 characters. They include generic TLDs (e.g., .xyz, .website), geographic TLDs (e.g., .berlin, .london), and brand-specific TLDs (e.g., .bmw, .barclays).

P-Handles:

A P-Handle, or "Person Handle," is a unique identifier used within domain registration systems to reference a specific set of contact details. Instead of entering the full contact information every time you perform a domain-related action, you can simply use the P-Handle. This ensures consistent and accurate use of contact details, streamlining domain management tasks.

There are different types of contact handles for domain names, including:

- Owner Contact: Represents the legal owner of the domain.
- Administrator Contact: Refers to the person or entity responsible for administrative tasks.
- Technical Contact: Represents the individual or group handling technical aspects of the domain.
- Billing Contact: Pertains to the individual or entity responsible for billing matters.

Phishing

Phishing refers to fraudulent attempts to retrieve personal information from internet users via deceptive websites or emails. Once acquired, these details can allow cybercriminals to impersonate the victim, potentially accessing sensitive accounts.

Preorders

A domain preorder allows users to reserve a domain under a new, yet-to-be-launched top-level domain through a registrar. When the new top-level domain becomes available, the registrar endeavors to secure the requested domain name. Should the registration not be successful, the customer's prepaid registration fees are typically refunded.

Registrant

The registrant is an individual or entity that secures a domain. They either acquire it for personal use or on behalf of another domain owner, registering it through a registrar for a designated duration.

Registrar

Acting as an intermediary, a registrar facilitates domain registrations. They bridge the gap between the registry, which offers domains for purchase, and the registrant, who obtains the domain by registering it for a specified term via the registrar.

Registrar Lock

A registrar lock is a protective measure applied to a domain name. Issued by the registrar, this lock prevents alterations to the domain name. When activated, domain transfers, deletions, or modifications to contact information are prohibited. However, domain renewals remain feasible.

Registration

The act of domain registration involves both securing a domain for a set period and implementing it technically through a domain provider, registrar, or reseller.

Registry

A registry is an entity responsible for distributing domains under the umbrella of one or multiple top-level domains, adhering to specific allocation guidelines. Additionally, the registry oversees certain resources vital to the technical functionality of the Domain Name System (DNS).

Root

Root servers, pivotal components of the domain name system (DNS), are responsible for resolving names at the DNS's core level. They possess details about the names and IP addresses of all top-level domain (TLD) name servers. A range of institutions operate these servers, with ICANN overseeing coordination.

SAN

Supporting SSL-secured communication for servers with multiple domain names and host names, the SAN function enables multiple domains to be safeguarded under a single SSL certificate. By adding extra domain names to the "Subject Alternative Name (SAN)" field, a solitary certificate can shield

them. This feature is particularly advantageous for trademark owners managing multiple websites.

Second Level Domain

A domain name's second level (or second level domain, abbreviated as SLD) is its next-to-last segment. Positioned to the right of the dot, it constitutes the domain's second character set. In the domain name "SafeBrands.com", "SafeBrands" represents the SLD.

Snapback Services

Snapback or backorder services specialize in monitoring registered domains. They stand ready to swiftly register domains once they've been relinquished by their former holders.

SSL

SSL, standing for Secure Socket Layer, is a protocol that facilitates encrypted connections between servers and clients. This ensures the secure transfer of data between a website's domain and its visitors.

Subdomain

A subdomain exists hierarchically beneath another domain. It refers to domains positioned beneath the main second-level domain. For example, in the domain "support.SafeBrands.com", "support" is a third-level subdomain, "SafeBrands" is the second-level domain, and ".com" is the top-level domain.

Sunrise Phase

Preceding the launch of a new Top-Level Domain, the Sunrise phase grants exclusive registration rights to holders of trademarks and registered trademarks, allowing them to claim domains reflecting their protected terms.

This phase aims to deter unauthorized registrations of these terms. Once this phase concludes, the domains become accessible to the wider public.

Third Level Domain

Often termed a subdomain, the third level domain denotes the third character group in a domain name. In the domain "SafeBrands.co.uk", "SafeBrands" exemplifies this third level domain.

TIER 3

Data centers, as classified by the U.S. Uptime Institute's TIA-942 standards, have a guaranteed minimum uptime like 99.9%. TIER 3 exemplifies a high-reliability level, utilizing redundant components and servers, with multiple supply routes. This design promotes fault tolerance and allows in-operation maintenance.

TLD Launch

Introducing a new Top-Level Domain typically progresses through stages:

- Sunrise
- Landrush
- General Availability

TMCH

The Trademark Clearinghouse (TMCH) stands as a pivotal tool in ICANN's new gTLDs initiative, providing a centralized repository of authenticated brands connected to every fresh Top-Level Domain. For further insights into TMCH, visit: https://safebrands.com/brand-protection/trademark-clearinghouse/

Top-Level Domain

Abbreviated as TLD, a top-level domain represents a domain's concluding segment, appearing to the domain's right. For instance, the TLD in "SafeBrands.com" is ".com". This domain segment sits atop the hierarchy in name resolution.

Traffic Redirection

Traffic redirection, or URL redirect, navigates users from one URL to another. Such redirection may stem from varied reasons, ranging from company name alterations to website mergers. Moreover, typo-driven domains might be used for phishing endeavors or guiding traffic to rival websites.

Trustee Service (Linked to Local Presence Service)

Certain Top-Level Domain registration authorities mandate specific conditions for domain registration. When domain names necessitate a local representative, SafeBrands introduces its "local presence services". We tailor advice for every client on the need for a "trustee" and oversee the trust agreement's facilitation with our localized partner.

TTL (Time To Live)

TTL is a setting for domain-related information that determines how long that information is stored in a server's memory before it checks for any updates. It's like an 'expiry date' for data and is usually measured in seconds.

When someone visits your website, their internet provider asks the DNS server where to find your site. The server replies with the site’s address (an IP address) and the TTL, which is how long the provider should remember this address before asking again.

If you set a TTL of 86400 seconds (one day) for your website’s address, internet providers will store this address for one day before they check for any changes. If you’re planning changes to your website or moving it to a new address, you might lower the TTL to, say, 300 seconds (5 minutes), so updates are seen more quickly.

Typosquatting

"Typosquatting" encapsulates a cybersquatting variant wherein users mistakenly input a term into a web browser, leading to a "typo domain". Such websites might feature competing services, irrelevant advertisements, or other undesired material.

Uniform Domain Name Dispute Resolution Policy (UDRP) (Link this to Uniform Rapid Suspension (URS))

Uniform Rapid Suspension (URS)

URS, paired with the Uniform Domain Name Dispute Resolution Policy (UDRP), offers avenues to settle domain disagreements in trademark violation scenarios.

URL

Short for Uniform Resource Locator, a URL defines a standardized method to access specific content like websites. For instance, using the URL SafeBrands.com directs you to our site.

Web Interface

Accessible through the Hypertext Transfer Protocol (HTTP), a web interface might be a graphical user interface (GUI) letting users interact with a system via a browser, or it might offer data to other systems as a web service.

Web Space

This refers to storage availability on a server. Stored files here can be continuously accessed online. Users secure this digital storage from internet service providers for content like websites. The act of providing this online storage is termed 'webhosting'.

Whois

Whois is a system revealing details about a domain owner, such as company information and contact details. This info can be sourced from the relevant registry via a Whois lookup.

Withholding

In their terms of service, domain registrars might state that they retain the right to use or transfer a lapsed domain without making it available for fresh registration. This act is termed 'withholding'.

Zone

Within the Domain Name System (DNS), a 'zone' represents a segment of the domain hierarchy overseen by a specific name server. While the primary name server governs the zone, creating copies on various secondary name servers enhances reliability if the primary fails.