

IP Restrictions

Overview

Every device connected to the Internet has a unique number assigned to it - an IP address. An IP address is used for targeted transport of data from the sender to the recipient.

You can control access to your website and Backstage for certain IP addresses with the following restrictions:

- **Global IP restrictions:** You can deny access to your website or Backstage to users with certain IP addresses (*Negative*) or allow access to certain IP addresses (*Positive*). For example, this allows you to block IP addresses from countries with high abuse rate.
- **Access-related IP restrictions:** You can apply IP restrictions to specific accesses or access groups. This is particularly useful when you want to ensure that access from a certain group is only permitted from a defined IP range. For example, to verify that requests are genuinely originating from a specific company.
- **Automatic IP restrictions (block):** If a user exceeds a predefined number of failed login attempts within a specified time period, their IP address can be automatically blocked from further access.

Set up IP restrictions

To configure global and access-related IP restrictions, proceed as follows:

1. Navigate to **Administration > IP Restrictions > Active IP Restrictions** and select **Edit > New**.
2. The new restriction setup window opens.
3. Enter a distinctive name for the restriction.
4. Enable the **Status** option to activate the IP restriction.
5. Select **Backstage** and/or **Webgate** option to define where the restriction should apply.
6. Enter the **IP address** or a specific subnet (in long notation) you want to restrict.
7. Select whether the IP restriction should be **Positive** (allow access) or **Negative** (deny access).

8. In the **Global** field, select **Yes** to apply the restriction globally or **No** to limit it to specific accesses or access groups.

- For the access-specific option, the system displays a list of accounts or access groups for you to select from.
 - Select accesses and click **Add**. Undo the selection with **Remove**.

9. Confirm with **Save**.

Active IP Restrictions / Restriction for IP '10.1.49.22/32'

▼ Master Data

Name:

Status: ☒

First, select the products you want to restrict for this IP address.
 Products:
 ☒ BACKSTAGE
 ☐ Webgate

Enter the IP address you want to restrict. You can also enter an IP range by entering the first complete IP address within the range and then by
 IP:
 . . . /
 Denial:
 ☒ Positive (Access allowed)
 ☐ Negative (Access denied)

If you make this IP Restriction "Global," then the restriction will be in effect for all Accesses. For example, if you create a Global Negative
 Global:
 ☐ Yes
 ☒ No

Not selected Accesses:

Quick Search	Filter	Sorting	Views	Export
ID	Access is Active	Username		
78		t.musterfotograf		
75		test.fotograf		

Add >>
 << Remove

Selected Accesses:

Quick Search	Filter	Sorting	Views	Export
ID	Access is Active	Username		
2	☒	picturemaxx-support		

Active IP Restrictions: Access granted to Backstage, specified IP address range, and only to selected Access

Note

You can also configure this IP restriction in the Authentication Restrictions section of a corresponding Access/Access Group.

Set up automatic IP blocking

If multiple attempts to login to your Webgate from the same IP address fail, the access from that IP address can be temporarily blocked. Both you and the affected user will automatically receive an email notification. Once blocked, the user will no longer be able to view media

content or access data. In some cases, other users sharing the same IP address may also be impacted.

To enable automatic IP blocking, proceed as follows:

1. Navigate to **Administration > IP Restrictions > Webgate Configuration**.
2. *Optional for multiple websites* From the **Select Website** dropdown, select a website to apply IP blocking.
3. Select **Enable IP blocking** to activate the feature.
4. In **Number of failed login attempts**, set the allowed number.
5. In **Timeframe in minutes**, set the time interval to consider the failed attempts.
6. Enable **E-mail alerts** to receive notifications when automatic IP blocking is triggered. Enter a name and recipient email address.
7. Click **Save**.

Configuration for Webgate

▼ Select Website

1 | Web 1.0 ▼

▼ Configure automatic IP Blocking

If a user makes multiple failed login attempts to your Website, their IP address can be blocked automatically as a security measure.

Enable IP Blocking: ☒

Number of Failed Login Attempts: *

Timeframe in Minutes: *

▼ Access blocking

In addition to blocking the IP, you can also specify whether the access where the login failures were detected should also be blocked.
If an access is blocked, you can unlock the access in the linked master data record under "Accesses".

☐ Activate additional lock for accesses

▼ IP block login window notice

Before the block occurs, a message indicating an impending IP block can be displayed in the login window.

☒ Display warning message in case of an impending IP block

Number of failed attempts before displaying the message *

▼ E-Mail Settings

Select the checkbox below and enter a name and email address in order to be alerted each time an automatic IP blocking goes into effect.

Email Alerts: ☒

Recipient Address: *

Name:

Revert

Save

Webgate Configuration: Automatic IP blocking

Note

When a user exceeds the allowed number of failed login attempts within the specified time, the system automatically blocks the IP address. You can view the restriction under **Administration > IP Restrictions > Active IP Restrictions** and manually remove it if needed.

Activate access blocking

In addition to IP blocking, you can also choose to block the specific access where the failed login attempts occurred. This access block becomes active if a successful login was recorded within the past two days, indicating a potential breach. If an access is blocked, you can lift the restriction in the associated master data record under **“Accesses.”**

To enable this feature, follow these steps:

1. Navigate to **Administration > IP Restrictions > Webgate Configuration**
2. *Optional for multiple websites* From the **Select Website** dropdown, select a website to apply access blocking.
3. Enable **Activate additional lock for accesses.**
4. Confirm with **Save.**

Configuration for Webgate

▼ Select Website

1 | Web 1.0 ▼

▼ Configure automatic IP Blocking

If a user makes multiple failed login attempts to your Website, their IP address can be blocked automatically as a security measure. You can opt to be notified by email when this happens. When the IP blocking goes into effect, the user will not be able to view your

Enable IP Blocking: ☒

Number of Failed Login Attempts: *

Timeframe in Minutes: *

▼ Access blocking

In addition to blocking the IP, you can also specify whether the access where the login failures were detected should also be blocked. If an access is blocked, you can unlock the access in the linked master data record under "Accesses".

☒ Activate additional lock for accesses

Webgate Configuration: Additional access blocking

Customers / Editing 'KU10005 User, Test' Customer

« < 6 (6) > » Back to Master Data Overview Edit ▾ Templates ▾

Master Data	Contacts	Contact History	Accesses	Outputs	Prices	Financial Doc
-------------	----------	-----------------	-----------------	---------	--------	---------------

« < 1 (1) > » Back to Accesses Overview Manage Access ▾

▼ General Data

Name: *

This Access is blocked and cannot log in.

Access is Active: ☐ Active

Username: *

Password: *

Contact Person: ▾

Outputs: ..

Comments:

Customer master data window: Blocked access notification

Note

The blocked access message appears in the customer, partner, or user's master data record under the **Accesses** tab. You can remove the block directly from there by enabling the **Access is Active** option.

Activate IP block warning upon login

If multiple attempts to login to your Webgate from the same IP address fail, you can temporarily block access from this IP address. If the user is unsure about their password, we recommend using the "Forgot your password" feature. You can display a warning message in the login dialog after a specified number of failed attempts.

To display the warning, proceed as follows:

1. Navigate to **Administration > IP Restrictions > Webgate Configuration**.

2. *Optional for multiple websites* From the **Select Website** dropdown, choose a website to apply IP blocking.
3. Enable **Display warning message in case of impending IP block** to activate the feature.
4. Set the number of failed attempts allowed before displaying the warning.
5. Click **Save**.

▼ IP block login window notice

Before the block occurs, a message indicating an impending IP block can be displayed in the login window.

☒ Display warning message in case of an impending IP block

Number of failed attempts before displaying the message *

Webgate Configuration: Activate IP block message in the Webshop login dialog

Login



Your login was unsuccessful. Please re-enter your credentials, or click "Forgot password" to retrieve a new password.

Warning: 4 attempts left until your access will be blocked.

Username:

Password:

☐ Remember me

☐ I have read and agree to the [General Terms and Conditions](#). *

[Forgot password?](#)

Login

IP block message in the Webshop login dialog

Note

The warning text also displays the number of tries left.

Configure messages for blocked users

When an IP address is blocked, the user with this IP address will see a system message. You can tailor a message for global, automatic, and access-related IP restrictions.

1. Navigate to **Administration > IP Restrictions > Message Configuration**.
2. *Optional for multiple websites* From the **Select Website** dropdown, select a website to apply the message.
3. Activate the areas where you want to display the message:
 - **Custom message for global IP restrictions**
 - **Custom message for automatic IP blocking**
 - **Custom message for access-related IP restrictions.**
4. Enter a heading and the message text for each activated language.
5. Confirm with **Save**.

Configuration for Messages

Select Website

01 Website Manager (...)

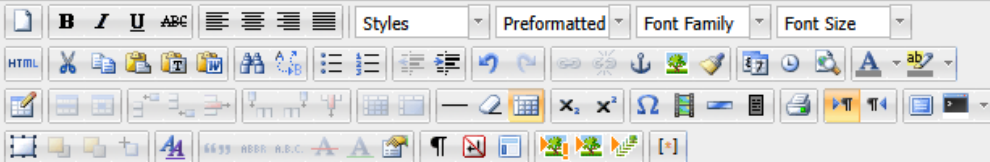
Message Configuration

When an IP address is blocked, the user with this IP address will see a system message. You can create three different messages: for global, automatic, and access-related IP restrictions. Customize the messages using the Content Editor below.

Message for global IP restrictions

☒ Custom message for global IP restrictions

English (USA)

Headline	Your IP address is blacklisted
Content	 Dear User, Your IP address has been added to our blacklist. Please contact us if you would like us to remove it from the list. Maxx Image support@maximage.com Path: pre.tw-data-text tw-text-large tw-ta » span.Y2lQFc

French

German

Configuration for messages: Customize system messages for blocked users

Manage IP restrictions

You can view a list of IP restrictions in **Administration > IP Restrictions > Active IP Restrictions**.

Create new IP restriction

- **Edit** menu > **New**.

Edit existing IP restriction

- Double-click or select a restriction name and **Edit > Open**.
- Make changes and click **Save**.

Delete existing IP restriction

- Select an IP restriction and **Edit > Unblock**.

Note

The integrated table functions allow you to search, filter, and sort records. For more information on these functions, as well as how to set up custom views and use the export function, see [Advanced Table Views](#).