

MailEnable Multi-Factor Authentication

Multi-Factor authentication provides MailEnable users with additional security for Web Mail and Web Administration. It will prompt users for an additional challenge when they have successfully logged in with their traditional credentials.

The challenge can be configured to occur every time they login, or whenever they attempt to authenticate from a new IP address or location.

Client Login Sequence

If a mail user has been configured with Multi-Factor Authentication, they the login screens will apply an additional validation step.

An example for a TOTP client (Google Authenticator) with the MailEnable Web Mail Client is shown below:



The screenshot displays the MailEnable 'Sign In' interface. On the left is a vertical banner with the MailEnable logo and a blue sky with clouds background. The main form area is titled 'Sign In' and contains the following elements:

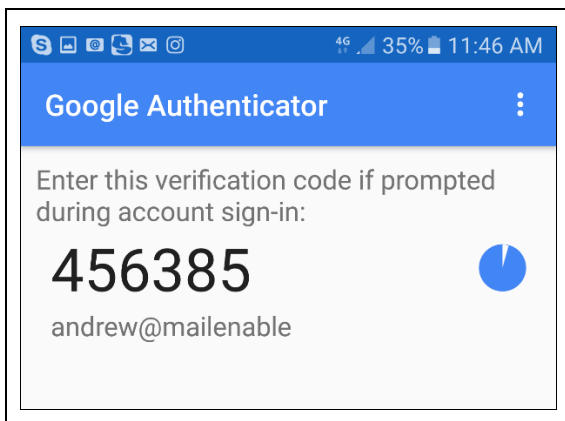
- A text input field containing the username 'emptytest'.
- A password input field with four dots and a toggle icon for visibility.
- Two dropdown menus: 'Language:' set to 'English' and 'Skin:' set to 'Arctic'.
- A checked checkbox labeled 'Remember my settings for this computer'.
- Two buttons: a blue 'Login' button and a grey 'Reset' button.
- A link for 'Mobile Version' at the bottom.

If the mail user has been configured to use TOTP, but does not have a secret assigned, the user will be prompted to configure the secret code with a TOTP client (like Google Authenticator).


Google authenticator can scan the generated QR Code and will generate Key Codes that can be entered into MailEnable.



In this example, the user has used the Google Authenticator to scan the above QR code, which then generates security keys every 30 seconds.



The user can then use the resulting Key to continue the login. Subsequent login attempts will require that the TOTP client generated key is used.



Sign In

emptytest@mailenable

••••

Key

Language: English

Skin: Arctic

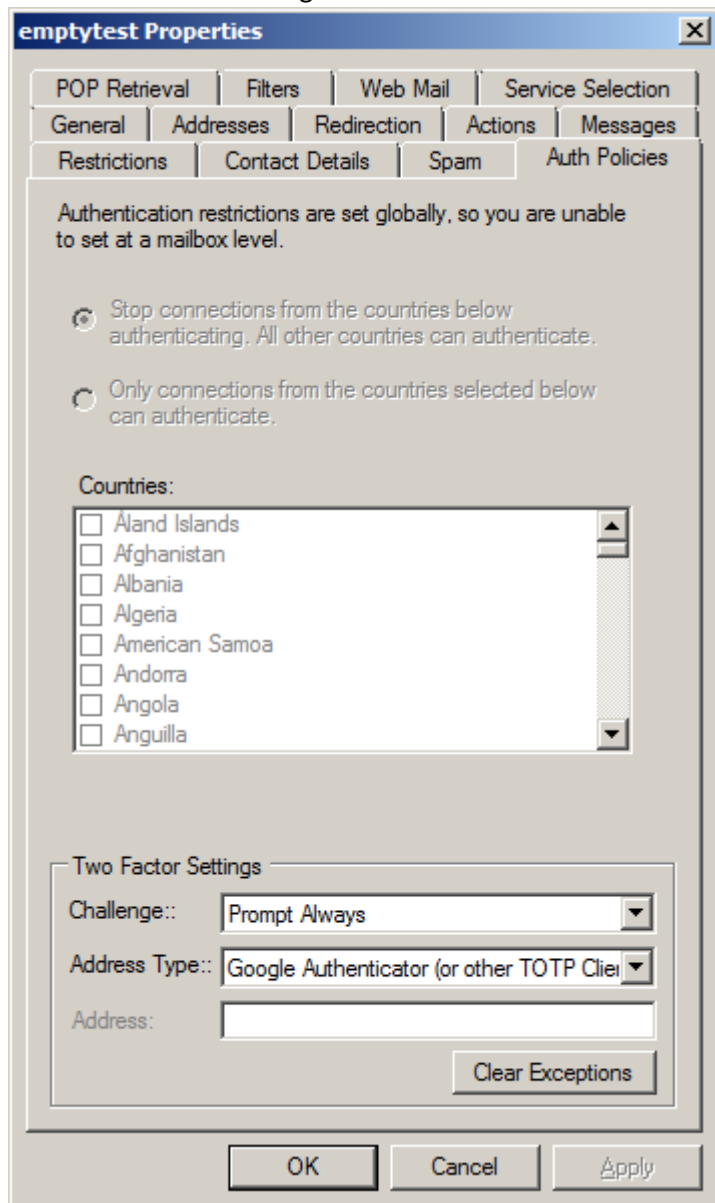
Remember my settings for this computer

Mobile Version

Note: The Key challenge will occur either every time, by IP address or location change.

Administering Mailbox Multi-Factor Authentication

Administrators can configure multi-factor authentication for users via the MMC or Web Administration.



The management of Two Factor settings can be configured under the management console for the properties of the mailbox. The challenge can be configured as follows:

Challenge	Meaning
Never	Do not prompt for a secondary challenge
Prompt Always	Always prompt for a secondary challenge
Prompt by IP Address	Only prompt whenever a successful username and password have been challenge occurs from a new IP address
Prompt by Country	Only prompt whenever a successful username and password have been challenge occurs from a new country/location

The screenshot shows the MailEnable Web Mail interface in Internet Explorer. The browser address bar displays `http://localhost:7582/NetWebMail_V5.0/Mondo/lang/sys/di`. The navigation bar includes icons for Email, Contacts, Calendar, Tasks, Statistics, Search, and Options. The left sidebar lists various settings categories: General (Account Settings, Regional Settings, Contact Details, Personalize, Client Settings), Login, Mail (Compose, Auto Response, Redirection, Email Signature, Whitelist, Blacklist), Calendar, and Advanced.

The main content area is titled "Options" and is divided into two sections:

- Login**: Contains four input fields: "Login:" (pre-filled with "Andrew@MailEnable"), "Current Password:", "New Password:", and "Confirm New Password:".
- Two Factor Authentication**: Contains two dropdown menus: "Challenge:" (set to "Prompt Always") and "Type:" (set to "Google Authenticator (or other TOTP Client)"). Below these is a QR code and a text label "QR Code:" with the alphanumeric code "3UTYHHOADF36FGYD".

At the bottom of the main content area are "Save" and "Cancel" buttons. The footer of the page shows "Account Usage: 149 KB of Unlimited".

The code can be delivered to users via TOTP clients like Google Authenticator as well as options to deliver the code via SMTP or SMS messages.

MailEnable - Login Details -- Webpage Dialog

Login Mailbox

Login: @MailEnable

Password:

Display Name:


Rights:

Status: Enabled

Two Factor Authentication

Challenge:

Address Type:

QR Code: 

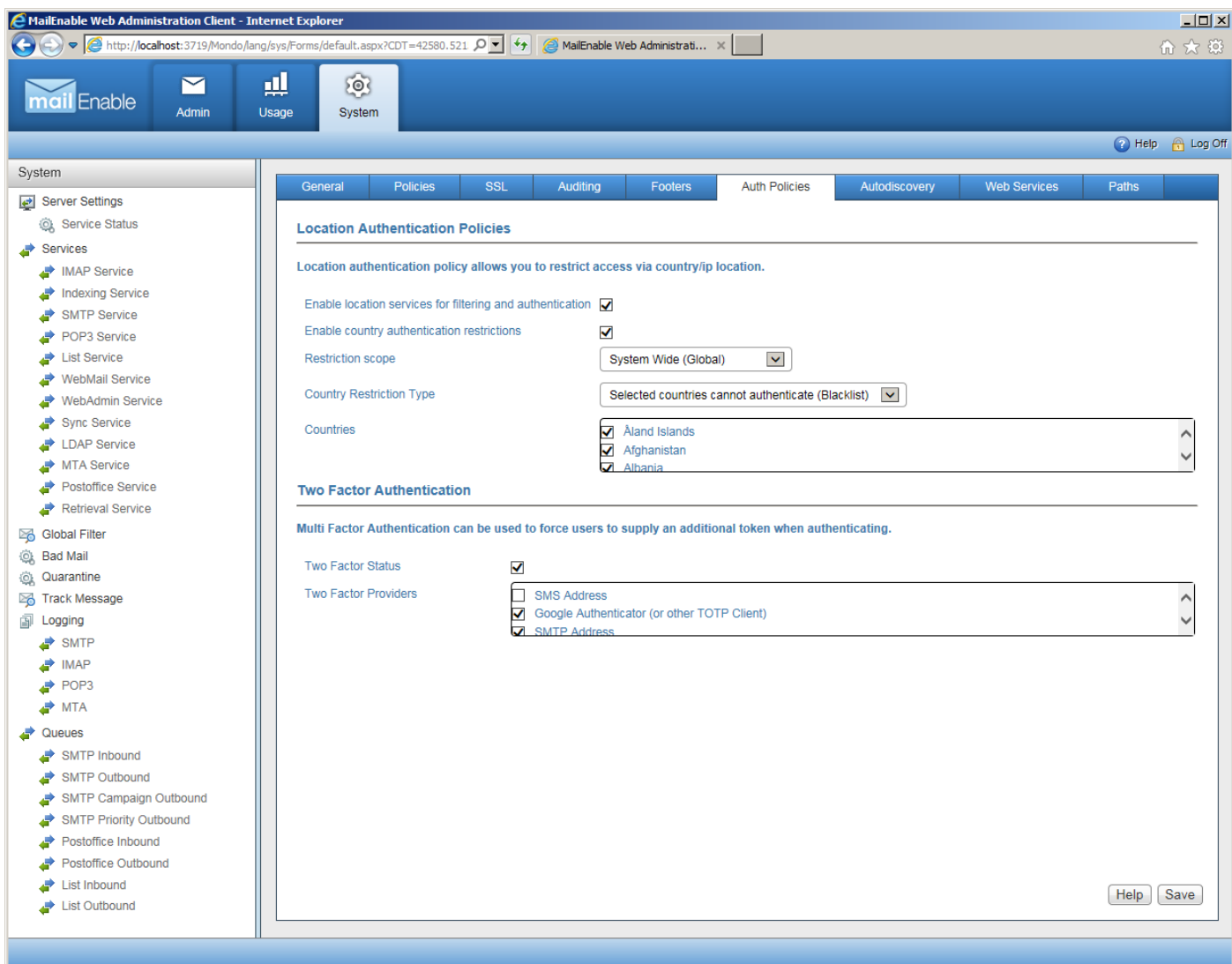
V7N2O27J3WNPOZPN

Administrators can reset the two factor code and any country exceptions and the webmail client generate and show the code to the user when they authenticate.

Configuring Multi-Factor Challenge Providers

MailEnable supports multiple challenge providers that can be configured to provide challenges.

The platform administrator can configure which of these providers can be configured by administrators end end-users.



Web Administration can be used to configure which multi-factor challenge can be configured for users. The following providers are available.

Challenge	Meaning
TOTP Client	This includes Google Authenticator, Windows Authenticator or any other TOTP key generator
SMS Address	Enterprise Edition and Premium Edition provide the SMS connector. Users can supply an SMS address for their account that can receive the temporary challenge code.
SMTP Address	Users can supply an alternate SMTP/Email address for their account that can receive the temporary challenge code.

The user can configure whether they are prompted for the security code every time they login, or whenever they attempt to authenticate from a new IP address or country.

If the QR code is blank, then the user is permitted to login still, but will be assigned a code when they authenticate.

Availability

Two Factor Authentication was introduced in MailEnable 9.5 Professional, Enterprise and Premium Editions.

These editions are available for download from the MailEnable web site.