rediff MAILPRO

Mail Access Restriction

Proposed by:

rediff.com

Introduction

Recent studies have revealed that corporate email contains around 70% to 80% of business information. Email has become a critical business tool, but it is also the easiest way to leak the information from the confines of a business.

Traditionally administrators have focused on securing the network from external threats. However, studies have concluded that more often the security is breached and data is leaked by internal employees knowingly or unknowingly. Company emails systems are not only used by internal employees but also sub-contractors, outsourced services partners, channel partners, etc. All of them have access to corporate information and sensitive data that could harm the organization or prove useful to competitors.

Mobile messaging devices have blurred the line between personal and business use. This has increased the security threat as users can store the mails on their personal handheld devices.

To protect the sensitive information, administrator should be able to control who is accessing the mails and how they are accessing it.

Mail access restriction

Rediff's mail access restriction feature allows administrator to control users' access to mails through multiple settings. These settings can be done for entire domain as well as individual users.

1. Restricting users from accessing mails from mail client such as outlook, thunderbird

Mail clients such as outlook, thunderbird or a native mail client on mobile allows user to download mail data on the device. In case, these devices are lost or stolen, the entire email data on that machine is at risk. Such situations can be avoided by allowing users to access mails only on the webmail through browser.

Mail clients use POP or IMAP protocol to receive mails and SMTP protocol to send out mails. Administrator can restrict mail access to certain users or entire domain by restricting mail access using POP (port 25, 110), IMAP (port 143), SMTP Auth (port 587) and POP before SMTP (port 25).

2. Restricting users from accessing mails on webmail

As a company policy, administrators do not want mails to be accessed from web browser for certain users. Administrator can restrict such users by denying access to mails using HTTP protocol.

3. Restricting users from accessing mails from unsecured channel

When the email is send or received over unsecured channel, the data transmission happens in a plain text. If anyone tapping your network can easily know the content of mail.

As an administrator if you want to enforce that mail access on secure channel only, you can do so by restricting all other mail access channels except for secure HTTP (HTTPS), secure POP (POPS, secure IMAP (IMAPS) and secure SMTP (SMTPS). Once you set these restrictions, users' attempts to access mails from unsecured channel will not succeed. Even if users manually change the URL from https to http in browser, he will be immediately logged off.

5. Restricting users from accessing mails from outside company network

Organization's confidential data should remain within the confines of company network. In such cases, administrators do not want certain employees or contractual workers to access the mails outside company premises.

With Rediff's mail access restriction feature you can specify the list of allowed IPs. Employees will be able to access mail only from these sets IPs. They will not be able to login to mailbox if they try to access mails from any other IP. You can specify as many IPs as you want separated comma ','.

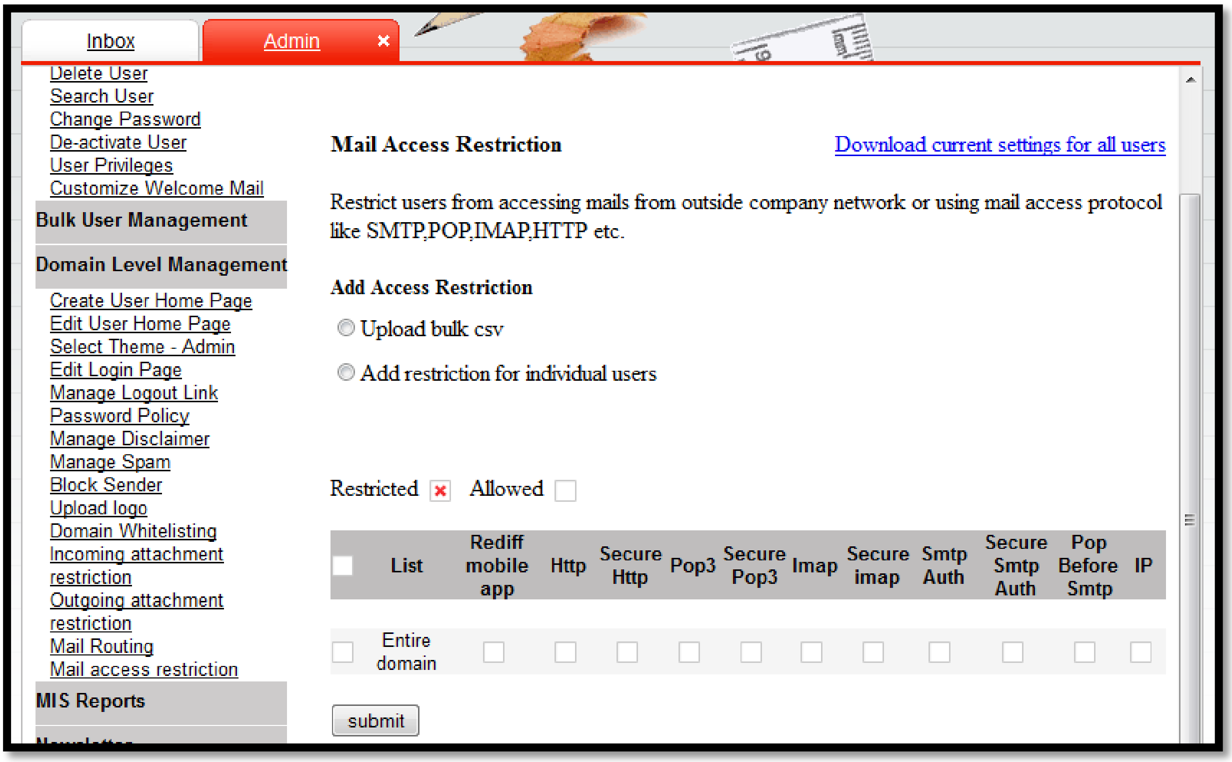
6. Restricting users from storing mails on mobile

Organizations are now encouraging 'bring your own device' (BYOD) policies. This however has increased the data leak threat by multiple folds. There is no foolproof method to enforce mail access restriction on mobile as users can access mails on native client or mobile browser.

Nevertheless, administrator can make sure that mails are not being downloaded on mobile device by restricting user access to IMAP and POP protocol. Users can now access mails only using mobile browser or using Rediff's mobile application. In both cases, the mails are not stored on mobile devices in human readable format.

How to use mail access restriction feature

Mail access restriction feature is available under ‘domain level management’ section. By default, no mail access restriction is applied to any user or domain.



Mail Access Restriction Download current settings for all users

Restrict users from accessing mails from outside company network or using mail access protocol like SMTP,POP,IMAP,HTTP etc.

Add Access Restriction

○ Upload bulk csv

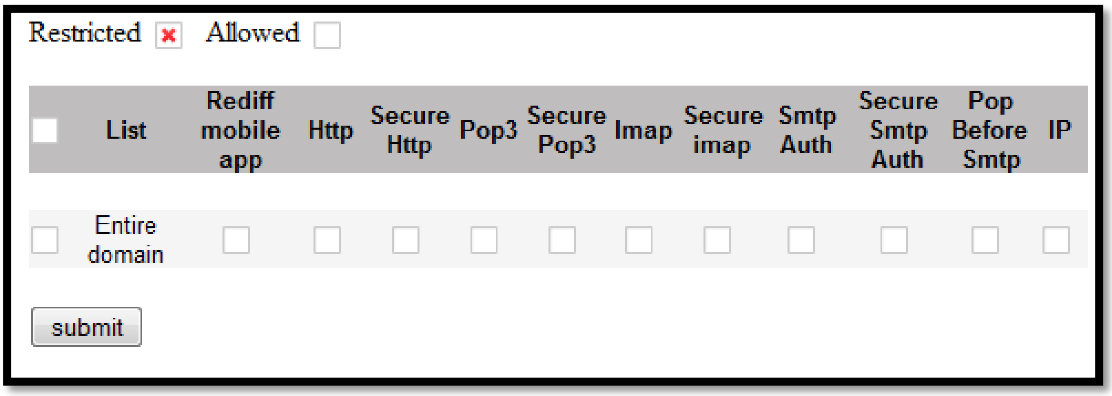
○ Add restriction for individual users

Restricted ☒ Allowed □

□	List	Rediff mobile app	Http	Secure Http	Pop3	Secure Pop3	Imap	Secure imap	Smtp Auth	Secure Smtp Auth	Pop Before Smtp	IP
□	Entire domain	□	□	□	□	□	□	□	□	□	□	□

submit

1. Imposing mail access restriction on entire domain



Restricted ☒ Allowed □

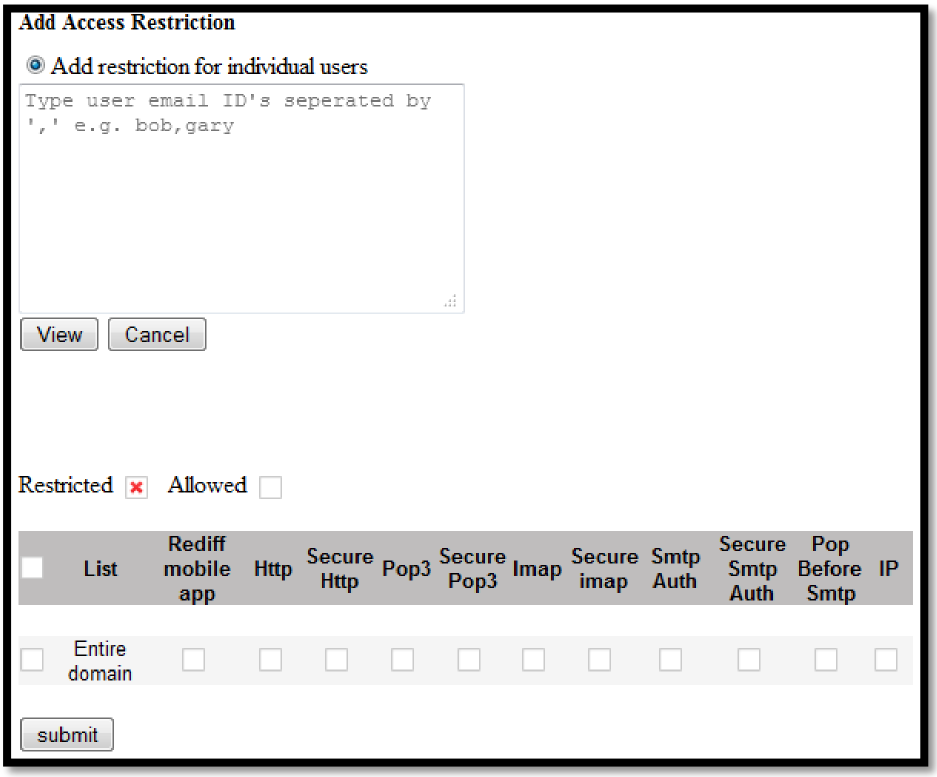
□	List	Rediff mobile app	Http	Secure Http	Pop3	Secure Pop3	Imap	Secure imap	Smtp Auth	Secure Smtp Auth	Pop Before Smtp	IP
□	Entire domain	□	□	□	□	□	□	□	□	□	□	□

submit

a. Click on restriction type (ex. POP, secure POP, etc.) and a cross would appear. ‘Cross’ indicates restricted access and blank checkbox indicates no restriction.

b. Click on submit to save the changes

2. Imposing mail access restriction to individual users



Add Access Restriction

● Add restriction for individual users

Type user email ID's seperated by ',' e.g. bob,gary

Restricted ☒ Allowed □

□	List	Rediff mobile app	Http	Secure Http	Pop3	Secure Pop3	Imap	Secure imap	Smtp Auth	Secure Smtp Auth	Pop Before Smtp	IP
□	Entire domain	□	□	□	□	□	□	□	□	□	□	□

a. Select ‘Add restriction for individual users’ radio button

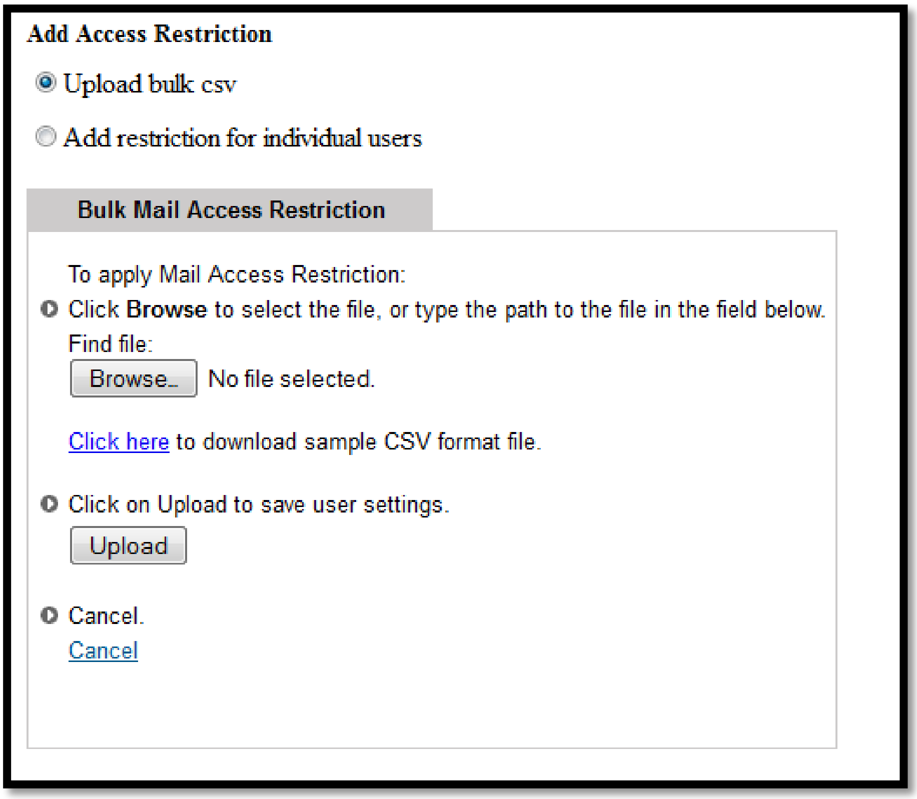
b. Specify the user email ID without domain name. You can specify multiple email IDs separated by comma ‘,’

c. Click on view and current mail access restriction settings for all the specified users will be displayed.

d. Click on restriction type (ex. POP, secure POP, etc.) and a cross would appear. ‘Cross’ indicates restricted access and blank checkbox indicates no restriction.

e. Click on submit to save the changes

3. Imposing mail access restriction using bulk upload facility



Add Access Restriction

● Upload bulk csv

○ Add restriction for individual users

Bulk Mail Access Restriction

To apply Mail Access Restriction:

- Click **Browse** to select the file, or type the path to the file in the field below.

Find file:

No file selected.

Click here to download sample CSV format file.

- Click on Upload to save user settings.

- Cancel.

Cancel

a. Click on ‘Upload bulk csv’

b. Download sample CSV file

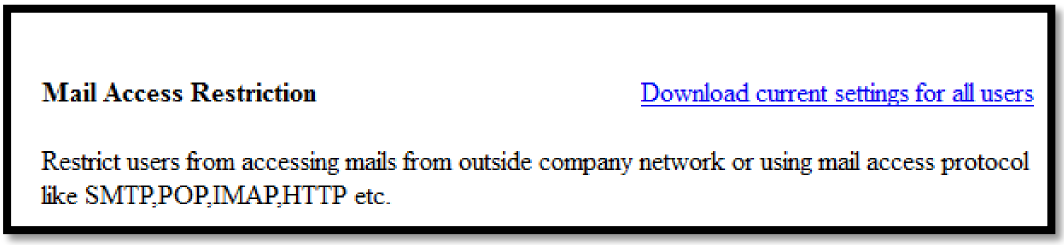
c. Specify the user ids along with restriction type in the format provided in sample CSV file. Please note‘0 ’indicates no restriction and‘1’ indicates access restricted. You can specify the multiple allowed IPs separated by semi-colon ‘;’.

d. Click on browse button and locate the file

e. Click on upload to apply mail access restriction settings on users specified in csv file

f. You will get a summary report of bulk mail access restriction activity

4. Downloading current mail access restriction settings of all users



Mail Access Restriction Download current settings for all users

Restrict users from accessing mails from outside company network or using mail access protocol like SMTP,POP,IMAP,HTTP etc.

a. Click on ‘Download current settings of all users’

b. A csv file will be downloaded with list of all active users and current mail access restriction settings applied to each of them.