

Introduction

Email is the main communication tool of most businesses. As such, email uptime is essential. If your email server goes down for a planned or unplanned outage, productivity, and financial loss can be significant.

All Sendio versions support an Email Continuity feature that allows your employees to send and receive email messages, and stay connected to business clients, even when your on-site mail server has an issue. Users can compose, reply, send, and receive emails from the same Sendio web user interface they already use to manage their “pending queue” of held messages. Email Continuity is available for purchase on all Sendio platforms:

- Hosted
- Appliance
- Virtual Appliance

For Sendio Hosted customers, Sendio Email Continuity protects against Internet outages to or from your corporate offices. It also protects against complete site failures at your office, such as those caused by power outages. Even if your mail server is already “in the cloud,” Sendio Email Continuity provides an additional level of protection should your email hosting service suffer a major outage.

Note: This manual assumes you have a license for Email Continuity. If you do not have a license, please contact sales@sendio.com.

Key Benefits

The following list summarizes the key benefits of Sendio Email Continuity:

- Can be activated in minutes, providing users with email access during an outage.
- Delivers quick restoration of sent and received email data to your mail server.
- Administrators can enable Email Continuity for the entire system or for specific domains, accounts, or email addresses.
- Continuity Inboxes retain inbound email for 28 days in continuity mode. Emails can be replied to or forwarded as in a webmail interface.
- Feature-rich email editor provides tools for creating professional emails during the mail server outage.
- Any “Local Password” set for an Account in Sendio will continue to work for access to the user’s Continuity Inbox.
- All emails spooled or sent with Continuity Inbox enabled are forwarded to your mail server automatically after you disable Email Continuity.
- Comes with password caching feature, which stores a user’s last login password securely for months or years prior to an email outage.

Conventions in this Manual

Note: A note is information that deserves special consideration.

Troubleshooting Tip: A Troubleshooting Tip provides information that has been known to help solve various problems.

Warning: A Warning identifies information that could lead to unintended consequences if not properly considered.

Menu Commands

Sendio's web interface has menu commands that you follow to change display pages, open dialog boxes and initiate certain actions. Primary menu commands (or paths through the interface) are shown in bold type in the format Admin > System > Outbound Control.

The options on drop-down menus, such as *Accept Contacts only*, are shown in italics.

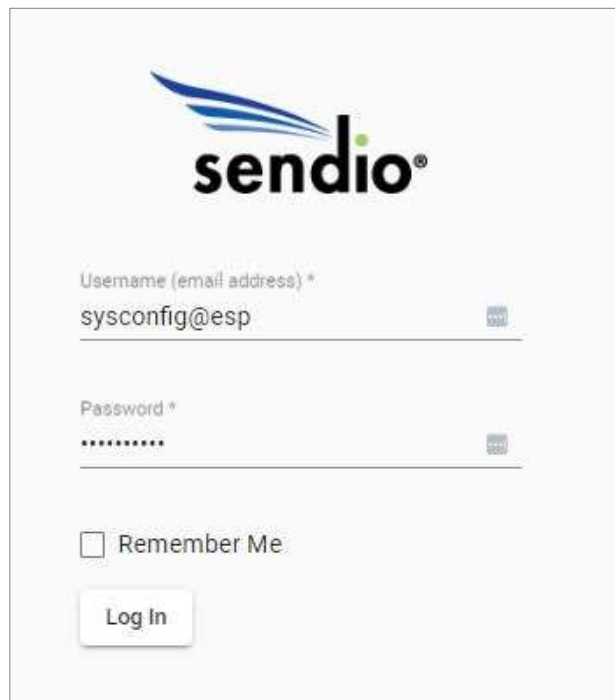
Sendio Terminology

Words that have special meaning within the context of Sendio operations are shown in italics, such as *Accept-List*, *Established*, or *Waiting*.

Section 1: Logging In

To configure the Sendio password caching and Email Continuity features, log in as the Sendio Administrator.

1. At the Login window, enter your administrator email address and password in the appropriate fields. For security, each typed password character is masked with an asterisk (*).
2. If the Remember Me option is shown, check it to have Sendio “remember” the email address authentication for a configurable period, so that this login step can be skipped in the future.
3. Click OK.



The image shows a login form for Sendio. At the top is the Sendio logo. Below it are two input fields: 'Username (email address) *' with the value 'sysconfig@esp' and 'Password *' with masked characters '*****'. There is a 'Remember Me' checkbox which is currently unchecked. At the bottom is a 'Log In' button.

For more information about logging in, refer to the Sendio Administration Manual

Section 2: Password Caching

Email Continuity comes with a password caching feature that stores a user's last login password securely. If your onsite Lightweight Directory Access Protocol (LDAP) or Active Directory server is not accessible by Sendio for a single sign-on handshake, password caching allows or disallows a user's login, based on the previously cached password. In this way, password caching ensures seamless access to the Sendio pending queue and Continuity Inbox.

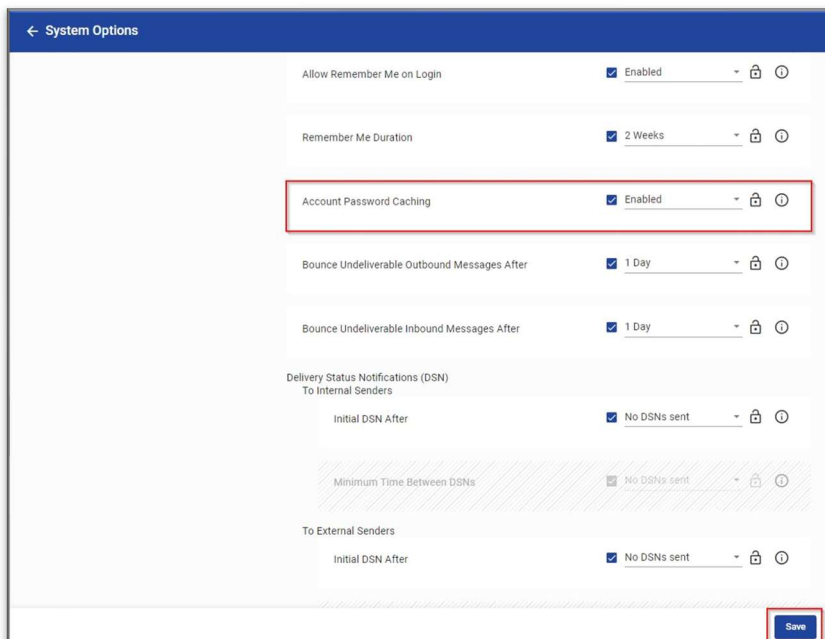
Best practices dictate that you enable password caching well in advance — months or years before an email or site outage occurs. Password caching is configured at the system level and account level. By default, password caching is disabled.

Enabling/Disabling Password Caching

Enabling Password Caching for the System

To enable password caching for the system:

1. Once logged in as an administrator, the System page appears.
2. Click the Options tab.
3. Scroll down to Account Password Caching, Check the box and change setting to Enabled.
4. Click Save.

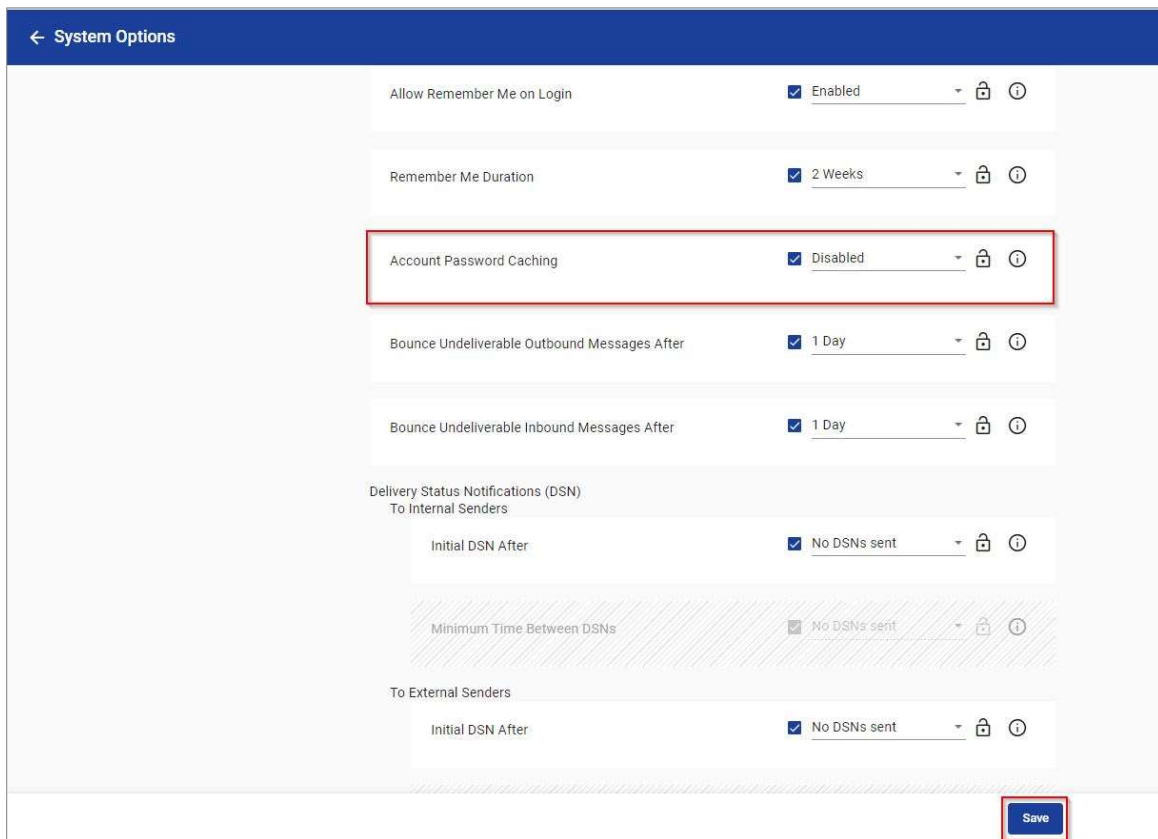


Enabling password caching for the system also enables it for all accounts automatically. However, you can enable/disable caching for individual accounts. That is explained later in this manual.

Disabling Password Caching for the System

To disable password caching for the system:

1. Login as an administrator, the System page appears.
2. Click the Options tab.
3. Scroll down to Account Password Caching, change the setting to Disabled.
4. Click Save.



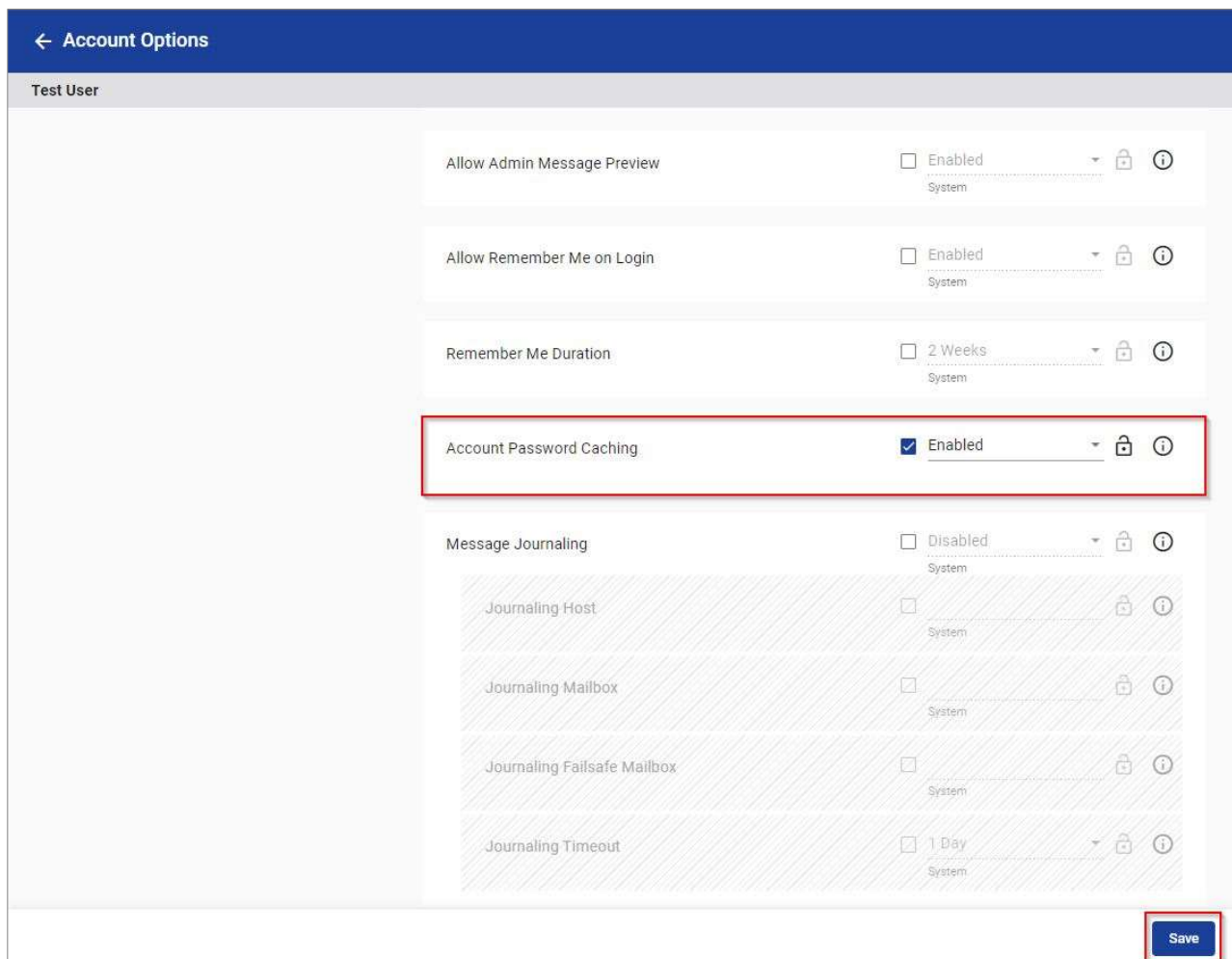
The screenshot shows the 'System Options' configuration page. The 'Account Password Caching' setting is highlighted with a red box and is set to 'Disabled'. Other settings include 'Allow Remember Me on Login' (Enabled), 'Remember Me Duration' (2 Weeks), 'Bounce Undeliverable Outbound Messages After' (1 Day), and 'Bounce Undeliverable Inbound Messages After' (1 Day). The 'Delivery Status Notifications (DSN)' section is also visible, with 'Initial DSN After' set to 'No DSNs sent' for both internal and external senders. A 'Save' button is located at the bottom right of the page.

Setting	Value
Allow Remember Me on Login	Enabled
Remember Me Duration	2 Weeks
Account Password Caching	Disabled
Bounce Undeliverable Outbound Messages After	1 Day
Bounce Undeliverable Inbound Messages After	1 Day
Delivery Status Notifications (DSN)	
To Internal Senders	
Initial DSN After	No DSNs sent
Minimum Time Between DSNs	No DSNs sent
To External Senders	
Initial DSN After	No DSNs sent

Enabling Password Caching for Accounts

To enable password caching for accounts:

1. In the left pane of the Sendio Administrator interface, click Accounts. The Accounts page appears.
2. In the Accounts page, double-click the account for which you want to enable password caching. The Account Details page appears.
3. Click the Options tab.
4. Scroll down to Account Password Caching, and then check this option's check box.
5. Using the Account Password Caching drop-down list, click Enabled.
6. Click Save.



← Account Options

Test User

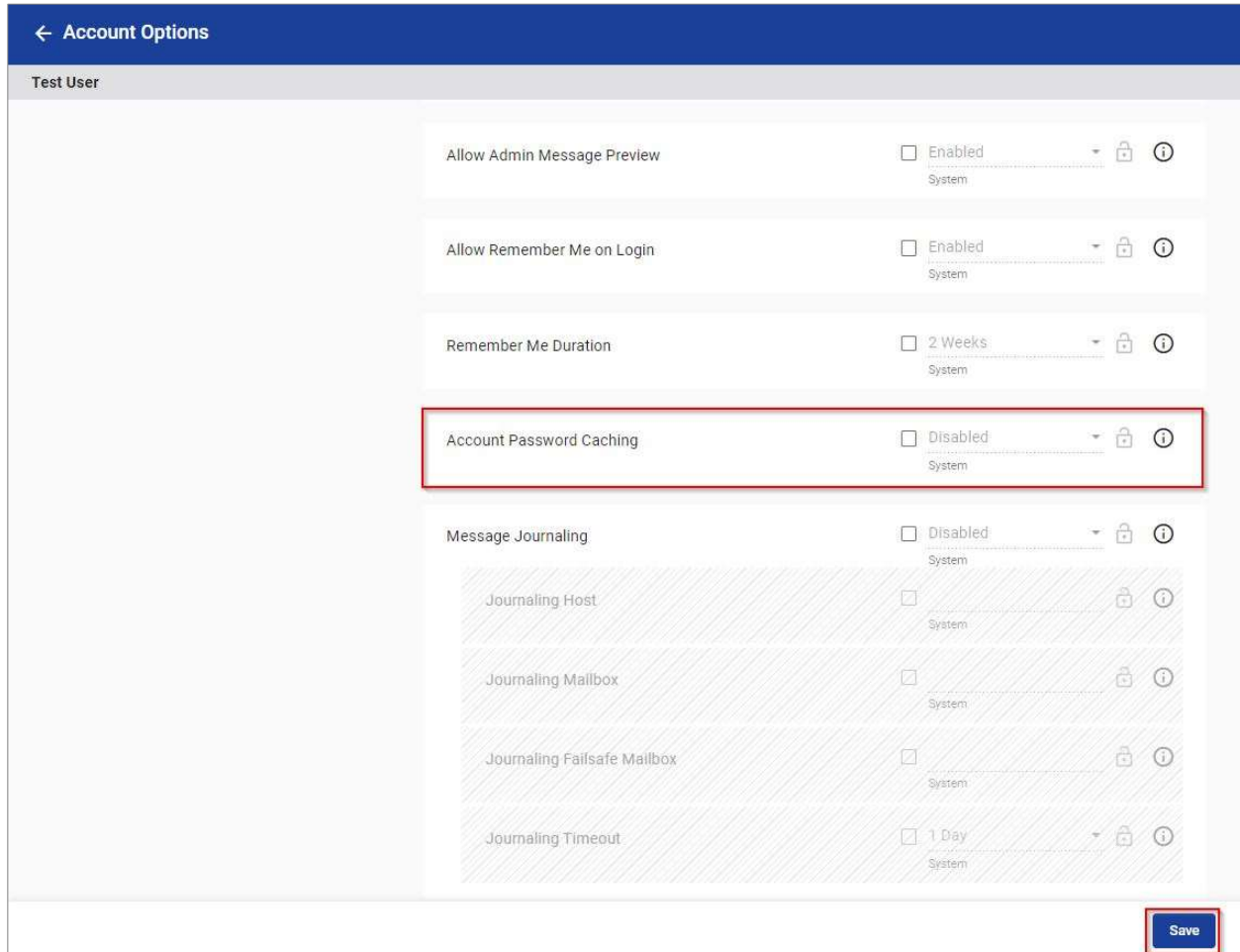
Allow Admin Message Preview	<input type="checkbox"/> Enabled	System	🔒	ℹ️
Allow Remember Me on Login	<input type="checkbox"/> Enabled	System	🔒	ℹ️
Remember Me Duration	<input type="checkbox"/> 2 Weeks	System	🔒	ℹ️
Account Password Caching	<input checked="" type="checkbox"/> Enabled		🔒	ℹ️
Message Journaling	<input type="checkbox"/> Disabled	System	🔒	ℹ️
Journaling Host	<input type="checkbox"/>	System	🔒	ℹ️
Journaling Mailbox	<input type="checkbox"/>	System	🔒	ℹ️
Journaling Failsafe Mailbox	<input type="checkbox"/>	System	🔒	ℹ️
Journaling Timeout	<input type="checkbox"/> 1 Day	System	🔒	ℹ️

Save

Disabling Password Caching for Accounts

To disable password caching for accounts:

1. In the left pane of the Sendio Administrator interface, click Accounts. The Accounts page appears.
2. In the Accounts page, double-click the account for which you want to disable password caching. The details page appears, with the Details tab displayed.
3. Click the Options tab.
4. Scroll down to Account Password Caching, uncheck the box for this feature and it will default to Disabled.
5. Click Save.



← Account Options

Test User

Allow Admin Message Preview	<input type="checkbox"/> Enabled	System
Allow Remember Me on Login	<input type="checkbox"/> Enabled	System
Remember Me Duration	<input type="checkbox"/> 2 Weeks	System
Account Password Caching	<input type="checkbox"/> Disabled	System
Message Journaling	<input type="checkbox"/> Disabled	System
Journaling Host	<input type="checkbox"/>	System
Journaling Mailbox	<input checked="" type="checkbox"/>	System
Journaling Failsafe Mailbox	<input checked="" type="checkbox"/>	System
Journaling Timeout	<input checked="" type="checkbox"/> 1 Day	System

Save

Section 3: Retry Duration

A “bounce” is an email message that is returned because it could not be delivered. There are several reasons why an email cannot be delivered. For example:

- The mailbox of the recipient might be full.
- The email address might no longer be valid.
- The email address might be disabled temporarily.
- The email address might be misspelled.

Sendio provides a customer-configurable retry duration feature that automatically sends an “Undeliverable” Postmaster bounce-back to the sending email address if an inbound or outbound email cannot be delivered within the time period configured by the administrator. This feature is available even for customers that have not purchased Email Continuity. Further explanation is explained later in this manual.

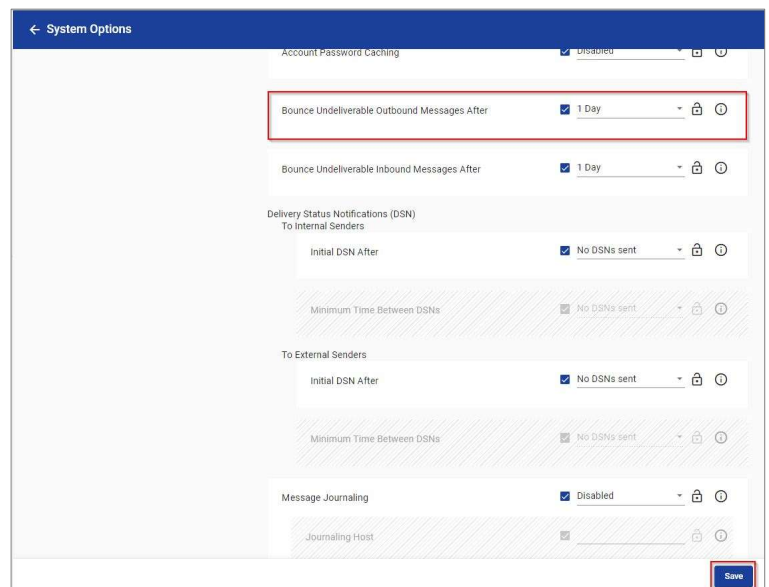
Configuring Retry Duration

Sendio provides a retry duration feature for inbound and outbound email. The default setting for both is 1 day. If you need to change this setting, use the following procedure. For retry duration best practices, see “SECTION 5: Email Continuity Guidelines”.

1. In the left pane, click System. the System page appears, Click the Options tab.
2. To configure the retry duration for outbound messages:

a. Scroll down to Bounce Undeliverable Outbound Messages After, and then check this option’s check box.

b. Use the drop-down list to select the time period during which the outbound email message will be sent. If this time period is reached without the email being sent successfully, a bounce message is sent to the sender and the email message is discarded.

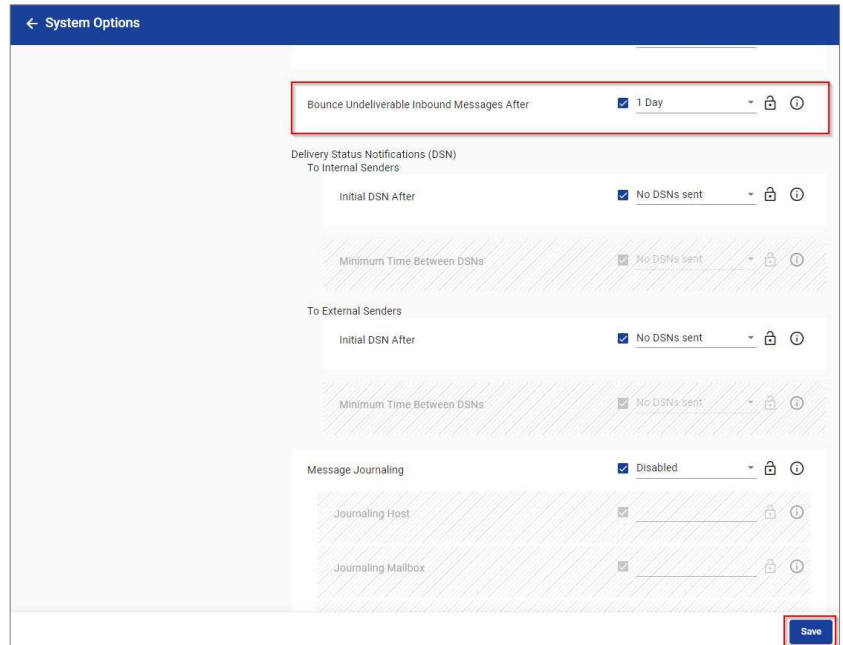


3. To configure the retry duration for inbound messages:

a. Scroll down to Bounce Undeliverable Inbound Messages After.

b. Check the check box. c. Use the drop-down list to select the time period during which the inbound email message will be sent. If this time period is reached without the email being sent successfully, a bounce message is sent to the sender and the email message is discarded.

5. Click Save.



The screenshot shows the 'System Options' configuration page. The 'Bounce Undeliverable Inbound Messages After' setting is highlighted with a red box and is set to '1 Day'. Below this, the 'Delivery Status Notifications (DSN)' section is visible, with 'To Internal Senders' and 'To External Senders' both set to 'No DSNs sent'. The 'Message Journaling' section is set to 'Disabled'. A 'Save' button is located at the bottom right of the page.

Setting	Value
Bounce Undeliverable Inbound Messages After	1 Day
Delivery Status Notifications (DSN) - To Internal Senders	No DSNs sent
Delivery Status Notifications (DSN) - To External Senders	No DSNs sent
Message Journaling	Disabled

Section 4: Email Continuity

Sendio's Email Continuity feature delivers email availability during planned or unplanned email system outages.

Administrators configure Email Continuity using the Continuity Inbox option at various levels within the Sendio Administrator interface. These levels follow a parent-child model, where the "child" inherits the Email Continuity setting of its "parent."

For example:

- **System level.** System is the highest level in the hierarchy. The Email Continuity setting set here is inherited by all domains, accounts, and email addresses.
- **Domain level.** Domains are the second-highest level in the hierarchy. The Email Continuity setting set here is inherited by all email addresses associated with the domain.
- **Account level.** Accounts are the third-highest level in the hierarchy. The Email Continuity setting set here is inherited by all emails associated with the account.
- **Email level.** Email is the lowest level in the hierarchy. At this level, the Email Continuity setting is configured for selected email addresses.

Although children inherit the Email Continuity setting from their parents, you can override the setting for individual children. For example, if you enable Email Continuity for the system, you can disable it for individual accounts or email addresses. Similarly, if Email Continuity is disabled for the system, you can enable it for individual accounts. Enabling Email Continuity for an individual account or email address is often helpful for IT personnel that want to learn how the feature works, without affecting other users.

After you enable Email Continuity, new inbound emails from internal and external senders will be available in each user's Continuity Inbox for up to 28 days. When your mail server outage ends, all sent and received messages for each user are forwarded from Sendio to your mail server automatically.

Note: Once you enable Email Continuity using the **Continuity Inbox** option for the system, domain, account, or email address, Sendio no longer tries to deliver the associated inbound messages to your mail server. To resume standard inbound delivery, you must disable Email Continuity using the same **Continuity Inbox** option.

The following sections describe how to enable or disable Email Continuity using the Continuity Inbox option at various levels within the Sendio Administrator interface. For Email Continuity best practices, see "SECTION 5: Email Continuity Guidelines".

Enabling/Disabling for the System

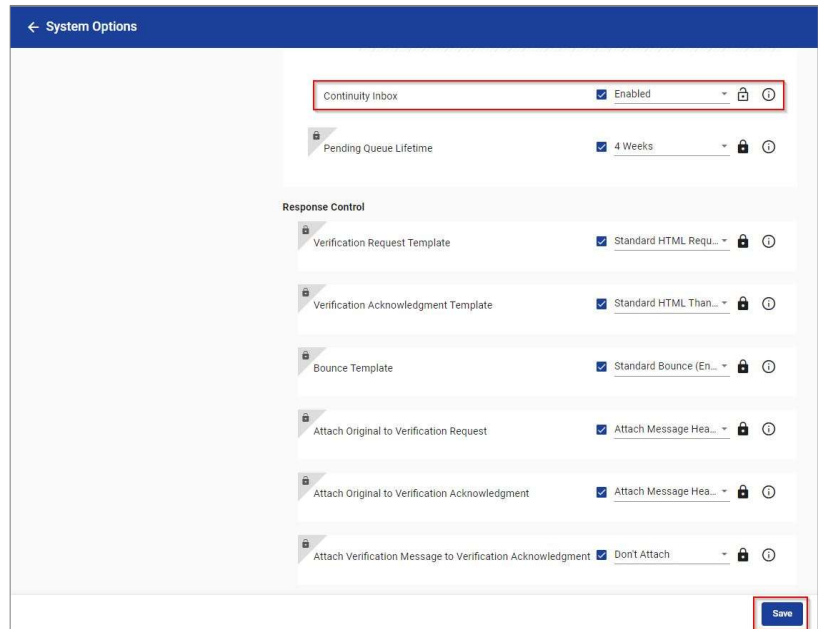
Enabling Email Continuity at the system level enables the feature for all domains, accounts, and email addresses automatically. After enabling Email Continuity for the system, you can disable it for individual domains, accounts, and email addresses (see the appropriate topic in this section).

Enabling Email Continuity for the System

To enable Email Continuity at the system level:

1. Login as an administrator, the System page appears, click the Options tab.
2. Scroll down to Continuity Inbox, and then check this option's check box.
3. Using the Continuity Inbox drop-down list, click Enabled.
4. Click Save.

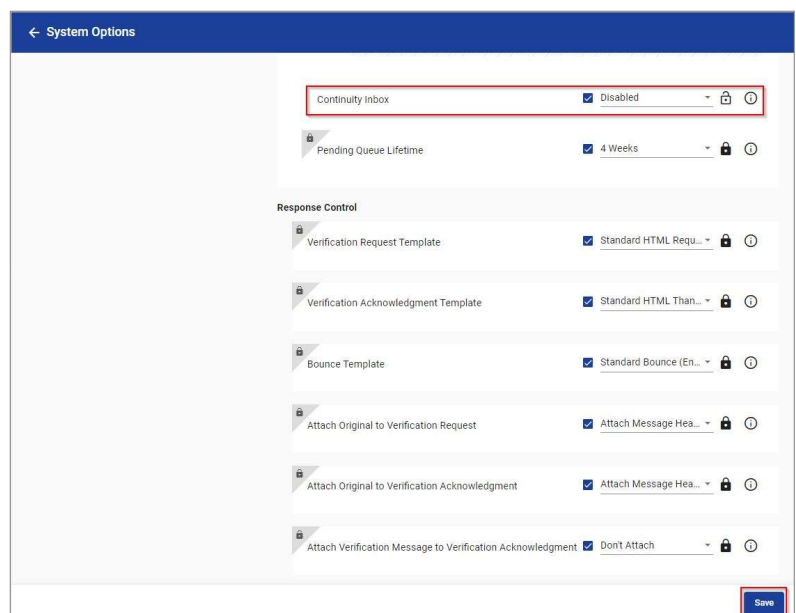
Note: If the **Continuity Inbox** check box is gray and unavailable, you do not have a license for Email Continuity. Please contact sales@sendio.com



Disabling Email Continuity for the System

The following procedure describes how to disable Email Continuity at the system level. If you disable Email Continuity, all the emails in the inbox are sent/forwarded to the mail server whose Email Continuity setting is disabled.

1. Login as an administrator, the System page appears, click the Options tab.
2. Scroll down to Continuity Inbox.
3. Using the Continuity Inbox drop-down list, click Disabled.
4. Click Save.



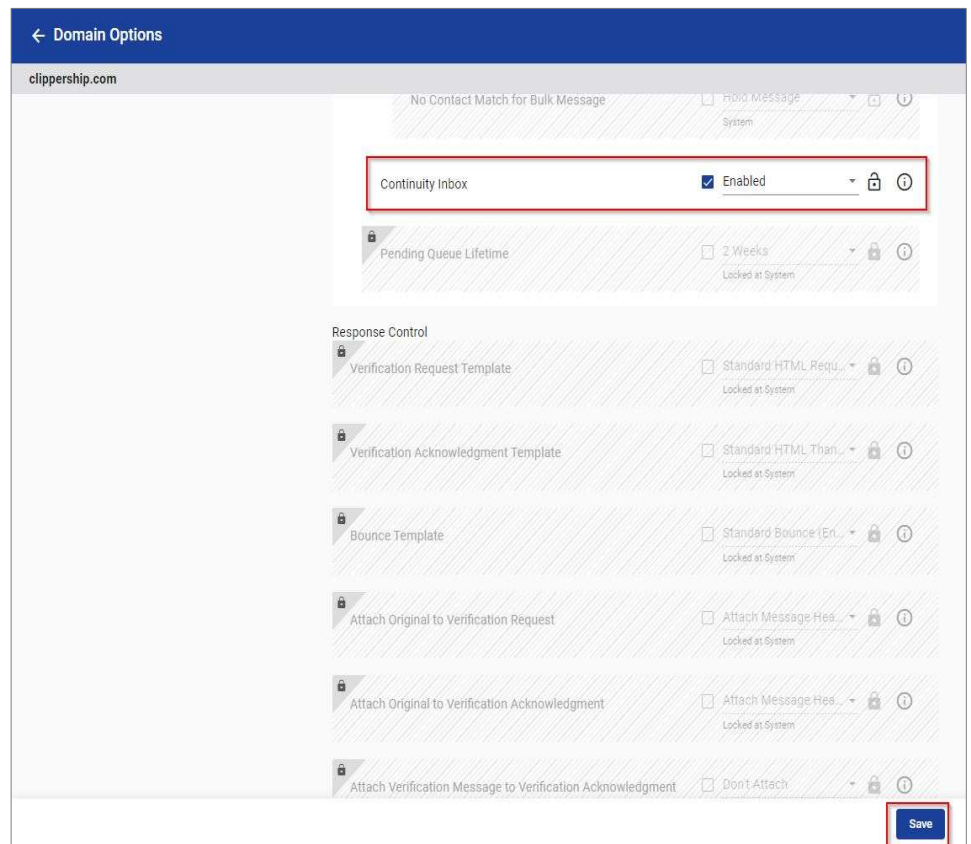
Enabling/Disabling for Domains

Enabling Email Continuity at the domain level enables the feature for all email addresses associated with that domain. After enabling Email Continuity for a domain, you can disable it for individual email addresses (see the appropriate topic in this section).

Enabling Email Continuity for Domains

To enable Email Continuity at the domain level:

1. In the left pane, click Domain. The Domains page appears.
2. In the Domains page, double-click the domain for which you want to enable Email Continuity. The domain page appears, with the Details tab displayed, click the Options tab.
3. Scroll down to Continuity Inbox, and then check this option's check box, change to Enabled.
4. Click Save.

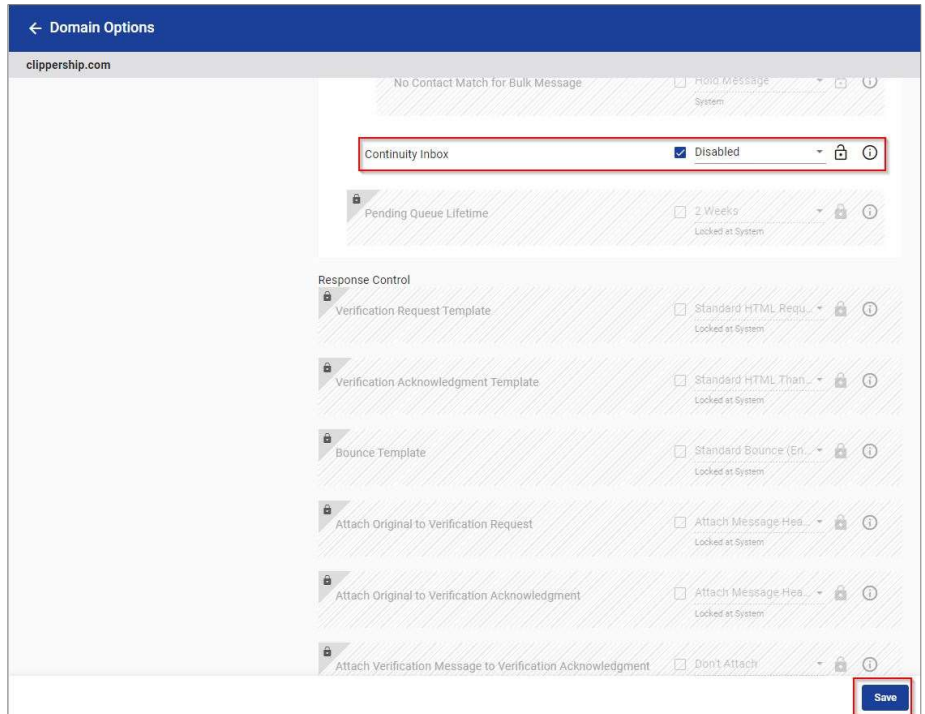


Note: If the Continuity Inbox check box is gray and unavailable, you do not have a license for Email Continuity. Please contact sales@sendio.com.

Disabling Email Continuity for Domains

The following procedure describes how to disable Email Continuity at the domain level. If you enabled Email Continuity at the system level, you can use this procedure to disable Email Continuity for individual domains.

1. In the left pane, click Domain. The Domains page appears.
2. In the Domains page, double-click the domain for which you want to enable Email Continuity. The
3. Scroll down to Continuity Inbox, and then check this option's check box, change to Disabled.
4. Click Save.



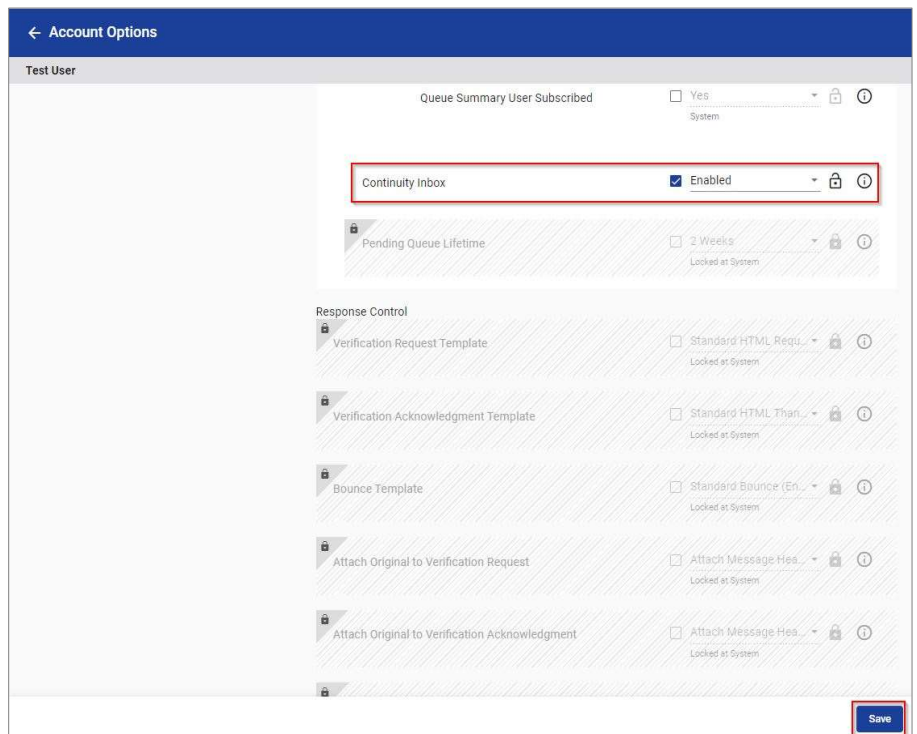
Enabling/Disabling for Accounts

Enabling Email Continuity at the account level enables the feature for all email addresses associated with that account. After enabling Email Continuity for an account, you can disable it for individual email addresses (see the appropriate topic in this section).

Enabling Email Continuity for Accounts

To enable Email Continuity at the account level:

1. In the left pane of the Sendio Administrator interface, click Accounts. The Accounts page appears.
2. In the Accounts page, double-click the account for which you want to enable Email Continuity. The details page appears, click the Options tab.
3. Scroll down to Continuity Inbox, and then check this option's check box and change to Enabled.
4. Click Save.



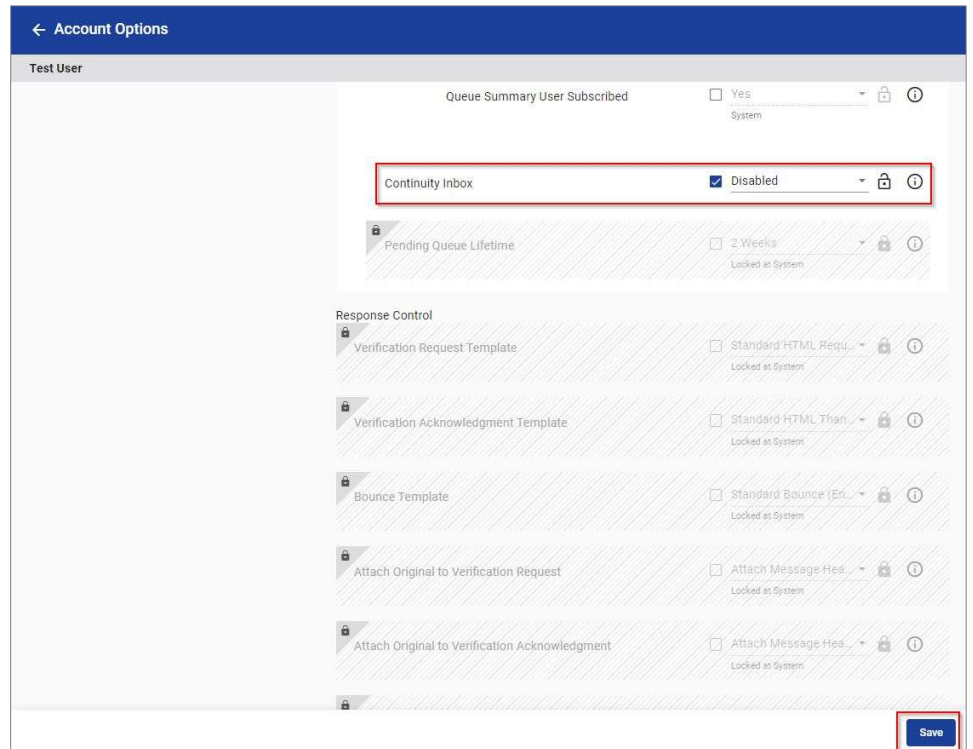
The screenshot shows the 'Account Options' page for a 'Test User'. The 'Queue Summary User Subscribed' section has a 'Yes' checkbox. The 'Continuity Inbox' setting is highlighted with a red box and is set to 'Enabled' with a checked checkbox. Below it, the 'Pending Queue Lifetime' is set to '2 Weeks'. The 'Response Control' section includes several templates (Verification Request, Verification Acknowledgment, Bounce, Attach Original to Verification Request, Attach Original to Verification Acknowledgment) with their respective settings (Standard HTML, Standard HTML Thank You, Standard Bounce, Attach Message Header) all set to 'Locked at System'. A 'Save' button is located at the bottom right.

Note: If the Continuity Inbox check box is gray and unavailable, you do not have a license for Email Continuity. Please contact sales@sendio.com.

Disabling Email Continuity for Accounts

The following procedure describes how to disable Email Continuity at the account level. If you enabled Email Continuity at the system or domain level, you can use this procedure to disable Email Continuity for individual accounts.

1. In the left pane of the Sendio Administrator interface, click Accounts. The Accounts page appears.
2. In the Accounts page, double-click the account for which you want to disable Email Continuity. The details page appears, click the Options tab.
4. Scroll down to Continuity Inbox.
5. Using the Continuity Inbox drop-down list, change setting to Disabled.
6. Click Save.



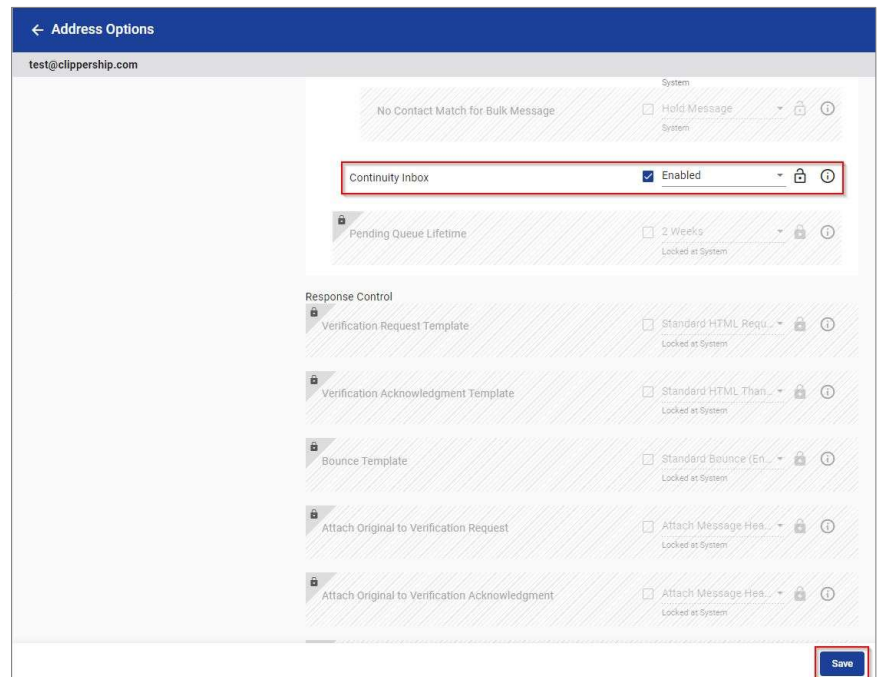
Enabling/Disabling for Email Address

Enabling Email Continuity at the email level enables the feature for individual email addresses. After enabling Email Continuity for individual email addresses, you can disable them using the procedure below.

Enabling Email Continuity for Email

To enable Email Continuity at the email level:

1. In the left pane, click Addresses.
2. In the Addresses page, double-click the email address for which you want to enable Email Continuity. The details page appears, with the Details tab displayed, click the Options tab.
3. Scroll down to Continuity Inbox, and then check this option's check box and change setting to Enabled.
4. Click Save.

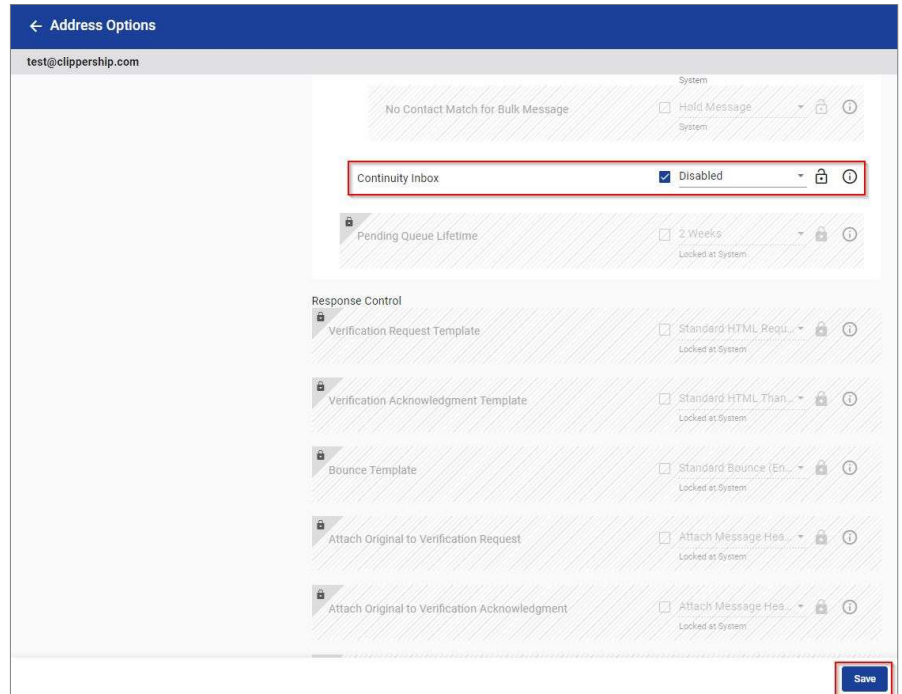


Note: If the Continuity Inbox check box is gray and unavailable, you do not have a license for Email Continuity. Please contact sales@sendio.com.

Disabling Email Continuity for an Email Address

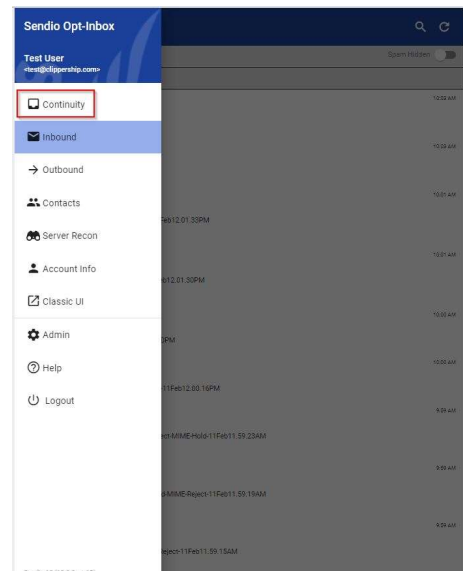
The following procedure describes how to disable Email Continuity at the email level. If you enabled Email Continuity at the system, domain, or account level, you can use this procedure to disable Email Continuity for individual email addresses.

1. In the left pane, click Addresses. The Addresses page appears.
2. In the Addresses page, double-click the email address for which you want to disable Email Continuity. The details page appears, with the Details tab displayed, click the Options tab.
3. Scroll down to Continuity Inbox, change setting to Disabled.
4. Click Save.



Continuity Inbox

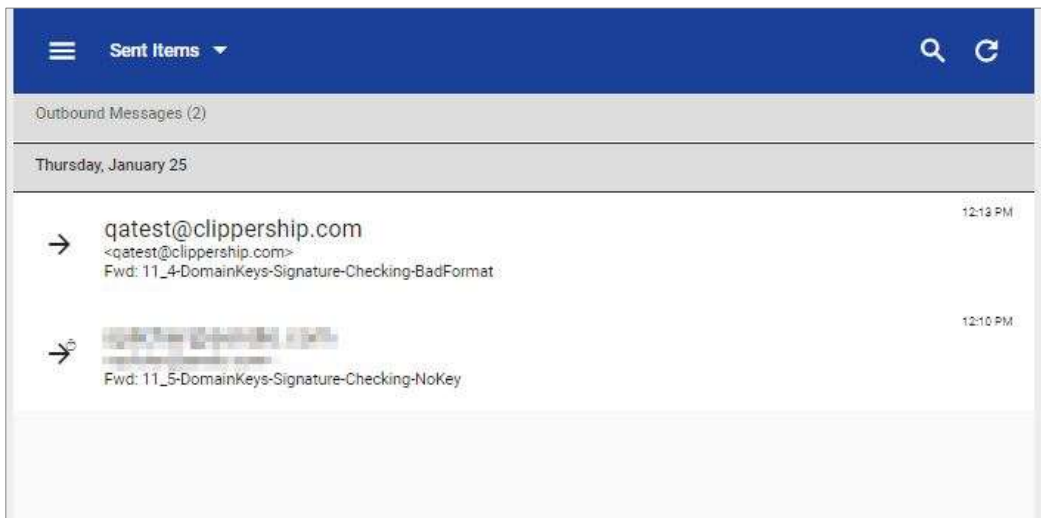
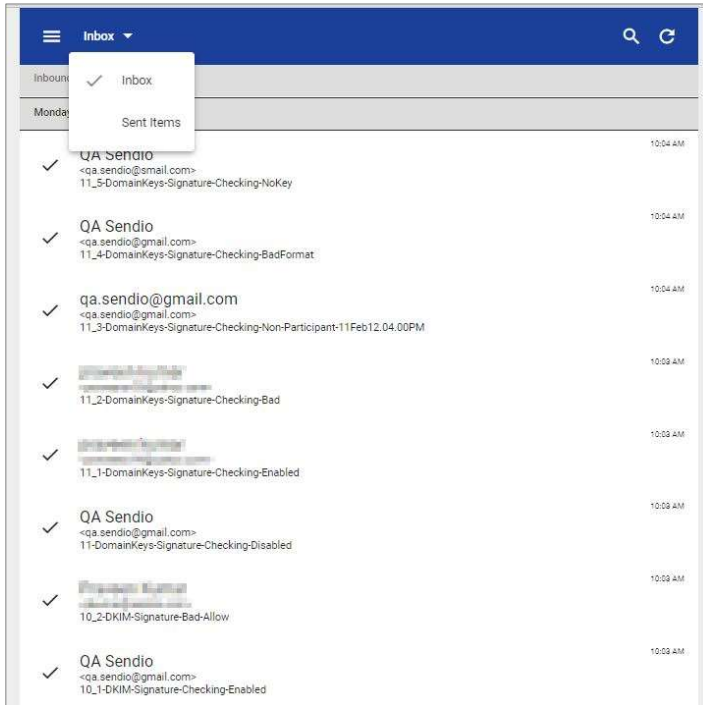
When you enable Email Continuity, Continuity appears at the top of the left pane of the associated user's Sendio web interface. Sendio users click this button to open the Continuity Inbox.



The Continuity Inbox has two tabs:

Inbox contains messages that were previously delivered, along with new messages that have yet to be delivered. Undelivered messages are held for 28 days and are then aged-out from the system automatically. Unread messages are indicated by a blue icon next to the message. Double-clicking the message opens the message and removes the blue icon.

Sent items contains all emails the user sends while Continuity Inbox is enabled. Disabling Continuity Inbox forwards these emails to the user's Inbox, so the user has a record of emails sent during the mail server outage.



Section 5: Email Continuity Guidelines

To get the most value out of the Sendio Email Continuity feature, observe the following recommendations and guidelines in the order described in this section.

- Develop a communication plan.
- Increase the Pending Queue Lifetime (if desired).
- Set the retry duration to a value that ensures non-bounced email.
- Create a defined plan for user login passwords.
- Have a plan for managing internal/external distribution lists.
- Set a proper SPF record (DNS TXT record) for your mail domains.

Develop a Communication Plan

It is important to have an overall plan for the Email Continuity event, so that users can gain access to Continuity Inbox as seamlessly as possible. After you enable the Continuity Inbox, users revert to their Continuity Inbox view automatically when they log in to their Sendio queue, and the purple Continuity button appears at the top of the left pane. This view alerts users that Sendio is acting as a temporary email interface for sending and receiving email. However, because users may login to Sendio only once or twice per day, best practices dictate that you develop an alternative method to inform users of a prolonged email outage.

Examples of mechanisms you can use to inform users include:

- A mass voice mail distribution.
- A predefined calling tree that hits all organizational units.
- Posting the incident and Sendio login instructions on an IT web page on your Intranet.

Increase the Pending Queue Lifetime (if Desired)

If you want users to have access to the largest number of emails for forwarding and replying when Continuity Inbox is enabled, set **Pending Queue Lifetime** in the **System > Options** page to the maximum value of four weeks. This configuration setting applies to previously delivered emails and held emails, and controls how quickly messages “age out” of the system. We recommend you set this value immediately after you purchase Sendio Email Continuity.

Set the Retry Duration

Sendio provides users with a retry duration setting for inbound email, even if they did not purchase Email Continuity (see “Section 3: Retry Duration”). This setting tells Sendio how long to try delivery of a message to your mail server before sending an “Undeliverable” Postmaster bounce-back to the sending email address.

We recommend you set this value to your desired setting immediately after you purchase Sendio Email Continuity. The default value is one day; however, you might want to configure a larger value. For example, if your email server encounters a problem on Sunday and you cannot enable Email Continuity until Monday, specifying a large value prevents emails from bouncing back to senders.

After you enable Email Continuity, the retry duration setting is ignored and emails awaiting delivery to your mail server are held for a full 28 days. After the 28th day, the email is deleted from Sendio.

Create a Plan for User Login Passwords

If your LDAP directory server or Active Directory server is down at the same time your mail server is down, the real-time directory sync single sign-on capability for Sendio login will not work. In small business setups, such as Microsoft Windows® Small Business Server (SBS), the mail server and directory server are the same server. To account for these configurations, you require a login plan for users that ensures easy login when the directory server is inaccessible.

Sendio's recommended solution is to enable password caching as soon as you purchase Email Continuity (see "Section 2: Password Caching"). As users log in to Sendio, the most recent successful login password is stored in an encrypted format in the Sendio database. If Sendio experiences a communication failure with your onsite directory, user passwords will be authenticated with the cached password.

An alternate solution for passwords in the event of a failure is to require users to provision a "Local" password on Sendio as soon as possible after your purchase Sendio Email Continuity. This password resides in the Sendio database and is completely independent from the password on your directory server. When users initiate a login to Sendio, they can click Account Info and use the Details tab to create a Local Password on Sendio (refer to the Sendio User's Guide).

Another alternative lets users take advantage of the existing Sendio "remember me" feature. If you have already enabled this feature users will see a "Remember Me" radio button on their login landing page that they can check before logging in. There is also a "Remember Me Duration" in System/Options that controls how long the token/cookie that Sendio inserts into a user's web browser lasts. The default value is two weeks, and the maximum value is four weeks.

The risk with relying solely on this feature when you enable Email Continuity is that some user's cache could expire 1 or 2 days after you start using Email Continuity. At that point the Administrator will have to assign a local password in order for the user to login and use his or her Continuity Inbox.

Having a Plan for Managing Internal/External Distribution Lists

For external distribution groups (that is, distribution group accounts that receive email from the Internet such as info@ or sales@), each distribution group will have its own Continuity Inbox on Sendio. Typically, a Sendio local password will be required for each distribution group, as most directories do not have separate passwords for a distribution group. Multiple members of the same group can have simultaneous login sessions to the same Continuity Inbox to view emails and send emails.

After Email Continuity is enabled, members of a distribution group will not receive new emails to the distribution group in their standard Inbox. For example, if sally@foo.com is a member of

sales@foo.com, and after Continuity Inbox is enabled, if an internal user or external party sends an email to sales@foo.com, that new email will be present only in the sales@foo.com Continuity Inbox. After your mail server is restored, the email to sales@foo.com is delivered to your mail server and sent to each member of the distribution group. Any person logged in to the sales@foo.com Continuity Inbox can send internal messages and external email messages. The address in the From field would be sales@foo.com.

For internal distribution groups, these email addresses may not be present in Sendio via the standard Directory sync. Therefore, after Email Continuity is enabled, these groups can neither receive nor send email. As a result, we recommend SECTION 5: EMAIL CONTINUITY GUIDELINES [4] Example of the Gold Key Next to Account Names SENDIO CONTINUITY ADMINISTRATION MANUAL PAGE 17 you develop a workaround. On an Intranet page, for example, members of key internal distribution groups could be listed; then, while Sendio Email Continuity is enabled, if someone in the company needs to send email of the group, each member of the group can be pasted into the To field of the email editor.

Set a Proper SPF Record

Set a Proper SPF Record A Sender Policy Framework (SPF) record is an optional Domain Name System (DNS) record that allows domains to inform the Internet community of permitted sending IP addresses for their domain in order to lower the chance that a spammer spoofs their domain in a spam campaign. In DNS, a TXT record is used to define the SPF record.

If you do not have an SPF record, you are not required to create an SPF record to use Sendio Email Continuity. However, if you have an SPF record, but are not routing outbound email through Sendio, your SPF record might need to be updated for you to send outbound emails cleanly from Sendio when Email Continuity is enabled. We recommend updating the SPF record immediately after purchasing Sendio Email Continuity.

The following are fictitious examples of SPF records called foo.com and goo.com:

```
foo.com.      3600  IN    TXT    "v=spf1 mx ip4:23.34.44.21 -all"
goo.com.      3600  IN    TXT    "v=spf1 ip4:23.34.44.21 -all"
```

In the examples above:

- The “mx” string in the foo.com SPF record means that any IP address in the domain’s MX record is permitted to send outbound email. Usually if you have that string in place, you are already covered for Sendio Email Continuity since the MX record should already point to your Sendio box.
- The “ip4” string delineates a specific IP address or IP address range. If you want to be certain that your SPF record is correct, type ip4: in your SPF record explicitly.

Additional Details Regarding Sendio Email Continuity

Integrity Services and Sendio Email Continuity

In the Sendio interface, the **Continuity Inbox** option is a sub-option of the **Integrity Services** option. If Integrity Services is disabled for the system, domain, or account, the Continuity Inbox is no longer available for associated accounts in the system or domain, or for specific accounts that are configured as disabled. In addition, emails to accounts that have Integrity Services Disabled are not held for a full 28 days, as is done for a standard Continuity Inbox.

After the **Retry Duration** value is reached (maximum value is 7 days), these messages bounce back to the sender. In practice, Integrity Services seldom is disabled. When it is disabled, however, it usually is for one or two accounts that want to use antivirus checking only, with no other security checks. For more information about Integrity Services, refer to the standard Sendio Administration Manual.

Sendio Email Continuity when Unknown Recipient Address is Set to Allow

In the Administrator web interface, **System > Inbound Control** has an **Unknown Recipient Address** parameter whose default setting is **Reject**. If you change this setting to **Allow**, the following behavior results when you enable Continuity Inbox for the system or a specific domain.

For 28 days, Sendio holds inbound messages associated with “Unknown Recipients” (just as it does for other inbound messages) and displays the messages in **Global Views > Inbound Messages**. However, since there is no associated “account” in Sendio for these “passthrough” emails, there is no associated Continuity Inbox; as a result, users and administrators cannot reply or forward these messages. To get maximum use of Sendio Email Continuity, it is highly recommended to have all accounts in Sendio.

Number of Email Recipients

If a user sends an email from the Continuity Inbox to an email address in an external domain (that is, the same domain or an email address in another domain resident on the same Sendio instance) the setting **System > Outbound Control > Maximum Destination Count** is applied to the message.

If a user sends an email from the Continuity Inbox to an internal email address (that is, the same domain or an email address in another domain resident on the same Sendio instance) the following two settings are applied to the message:

- System > Outbound Control > Maximum Destination Count
- System > Inbound Control > Maximum Recipient Count

Internal Messages and Contacts

To facilitate seamless email delivery when Email Continuity is enabled for a system, domain, or account, any internal emails (that is, the same domain or an email address in another domain resident on the same Sendio instance) sent from the Continuity Inbox are not subject to Contact checking. For example, if **user1@foo.com** sends an email from his Continuity Inbox to **user2@foo.com**, the email is forward to the Continuity Inbox of **user2@foo.com**, even if no contact exists in the user2@foo.com Sendio queue for user2@foo.com.

Failed Outbound Deliveries during Email Continuity

If a user sends an outbound email from his Continuity Inbox to recipients in one more external domains and the email is rejected by a recipient mail server, no “UNDELIVERABLE” bounce will be present in the users Continuity Inbox. For definitive proof that an outbound message was successfully sent to all recipients of the message, a user or administrator should consult the **Messages > Outbound Messages** tab in their Sendio user Interface and not the **Sent Items** in their Continuity Inbox.

Failed deliveries are indicated with a red x through a green box. For details about the failed delivery, click the message, and then click its **History** button.

Sent Emails Appear in Inbox After Service is Restored

When Email Continuity is enabled, each time a user sends an email via the Continuity Inbox email editor, the user’s own email address is silently blind-copied (BCCd) on the message. If you disable Email Continuity, the BCCd emails are forwarded to the user’s Inbox on the mail server. The user can move the BCCd emails to the Sent Items folder on the mail server if desired.

Email Aging and Email Continuity

After an administrator enables Email Continuity, new inbound emails from internal and external senders will be available in each user’s Continuity Inbox for up to 28 days, and then get automatically deleted at the start of the 29th day.

In addition, all previously delivered emails that have not aged-out via the Pending Queue Lifetime setting in System > Options are automatically present in a user’s Continuity Inbox for replying and forwarding. However, these previously delivered emails may age-out sooner than 28 days, depending on the Pending Queue Lifetime setting.

For example, assume that a previously delivered email to the customer mail server gets pushed to the Continuity Inbox when Email Continuity is enabled. That email’s 28-day expiration date in the Continuity Inbox is based on when the message first arrived to the Sendio instance and the Pending Queue Lifetime setting. If Sendio processed and delivered the email to your mail server on July 1, the Pending Queue Lifetime setting was 3 weeks (21 days), and Email Continuity was enabled on July 15, the message would remain in the Continuity Inbox until July 22, and then get deleted automatically.

