How to Set Up Salesforce Email Relay: A Simple Step-by-Step Guide

Sai Rakesh Puli

sairakesh2004@gmail.com
Independent Researcher, Texas, USA

Abstract

Email deliverability is a critical factor for effective marketing and communication. Many organizations face challenges when emails sent through Salesforce are flagged as spam or fail to land in recipients' inboxes, leading to decreased engagement and increased unsubscribe rates. Salesforce Email Relay provides an effective solution by allowing organizations to route their emails through their own SMTP servers instead of Salesforce's default servers. This guide outlines a step-by-step approach to configuring Salesforce Email Relay with Gmail and other email services, ensuring secure, reliable email delivery and improved brand consistency. Key considerations include SMTP server setup, domain verification, security protocols, and testing procedures, along with best practices for maintaining deliverability and preventing authentication failures.

Keywords: Salesforce Email Relay, Email Deliverability, SMTP Server, Email Configuration, Gmail Integration, DMARC, DKIM, TLS Encryption, Email Security, Salesforce Setup, Deliverability Testing, Email Authentication, SPF Records

Introduction

Poor email deliverability can seriously damage marketing efforts. Your own SMTP server can handle email sending through email relay, which gives you more control over deliverability and branding. On top of that, it keeps your messages from landing in spam folders since they come from your domain instead of Salesforce's shared IPs. The system lets you send up to 5,000 emails daily per organization. This powerful tool works with Professional, Enterprise, Unlimited, and Performance editions.

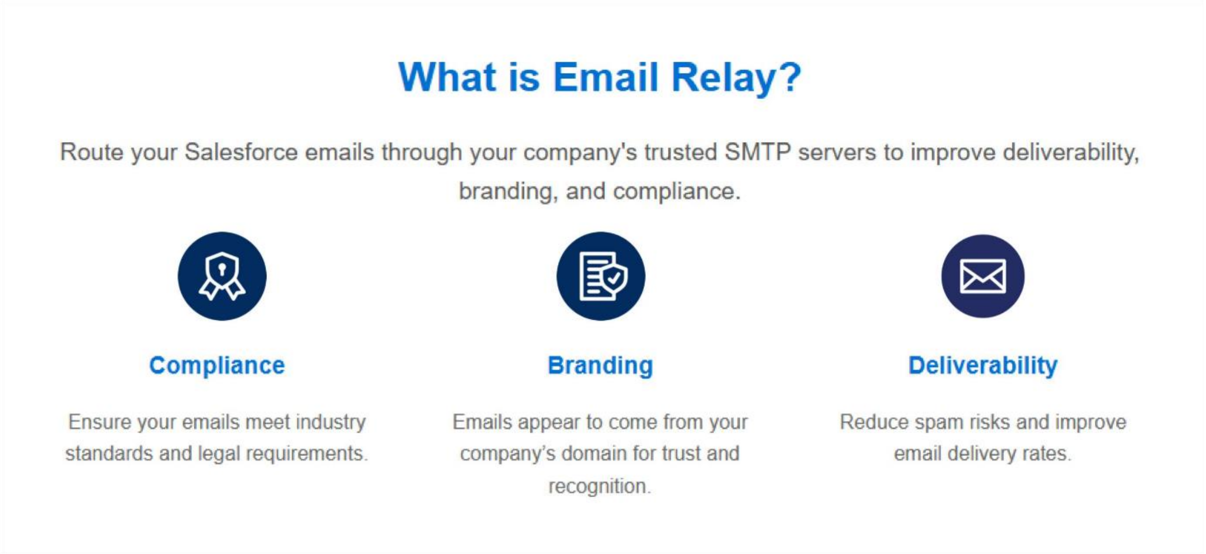
In this article, we'll show you how to set up Salesforce Email Relay step by step. You'll learn the ideal configuration for your system, whether you use Gmail or other email services. This setup ensures your organization's emails reach their intended recipients effectively.

What is Salesforce Email Relay and How Does it Work

Salesforce email relay, can be thought of as a bridge connecting your Salesforce organization to your preferred email server.

Understanding email relay fundamentals

The email relay process moves emails between servers. This feature lets you route all Salesforce-generated emails through your company's SMTP server instead of Salesforce's default servers. Your emails from Salesforce will appear to come straight from your organization's domain.



What is Email Relay?

Route your Salesforce emails through your company's trusted SMTP servers to improve deliverability, branding, and compliance.

Compliance

Ensure your emails meet industry standards and legal requirements.

Branding

Emails appear to come from your company's domain for trust and recognition.

Deliverability

Reduce spam risks and improve email delivery rates.

Fig I.What is Email Relay [1]

Key components of the Salesforce email relay

1.Company-Owned Domain for Sending Emails

One of the most crucial elements in setting up Salesforce Email Relay is the use of a company-owned domain. This ensures that all emails sent from Salesforce appear as though they originate from the organization’s domain, reinforcing brand consistency and trustworthiness. Instead of emails being sent from a generic Salesforce address, recipients will see the organization's official domain in the sender's field. This boosts the likelihood of emails reaching the inbox and improves user engagement. Furthermore, using a company-owned domain helps ensure that the organization maintains full control over its email communications.

2. SMTP Server Configured to Salesforce's Security Requirements

The second key component of the Salesforce Email Relay is the SMTP server configuration. This server must be configured to meet Salesforce’s security requirements, such as supporting standard email encryption protocols and allowing SMTP authentication. Salesforce requires that the relay host (the company’s SMTP server) be able to handle email traffic securely and within Salesforce's sending limits. The server must be able to process up to 5,000 emails daily per organization, depending on the Salesforce edition, and should also support encryption for secure transmission of emails.

3. Authentication Protocols and TLS Encryption

To further improve security, Salesforce Email Relay relies heavily on authentication protocols such as TLS (Transport Layer Security) encryption. TLS ensures that email communication between Salesforce and the SMTP server is secure and encrypted, preventing unauthorized access to sensitive information. In addition, Salesforce requires the use of SMTP authentication, which ensures that only authorized users can send emails through the relay. This prevents abuse and enhances security by ensuring that email traffic is verified and protected.

4. DMARC Policy to Prevent Spoofing and Phishing

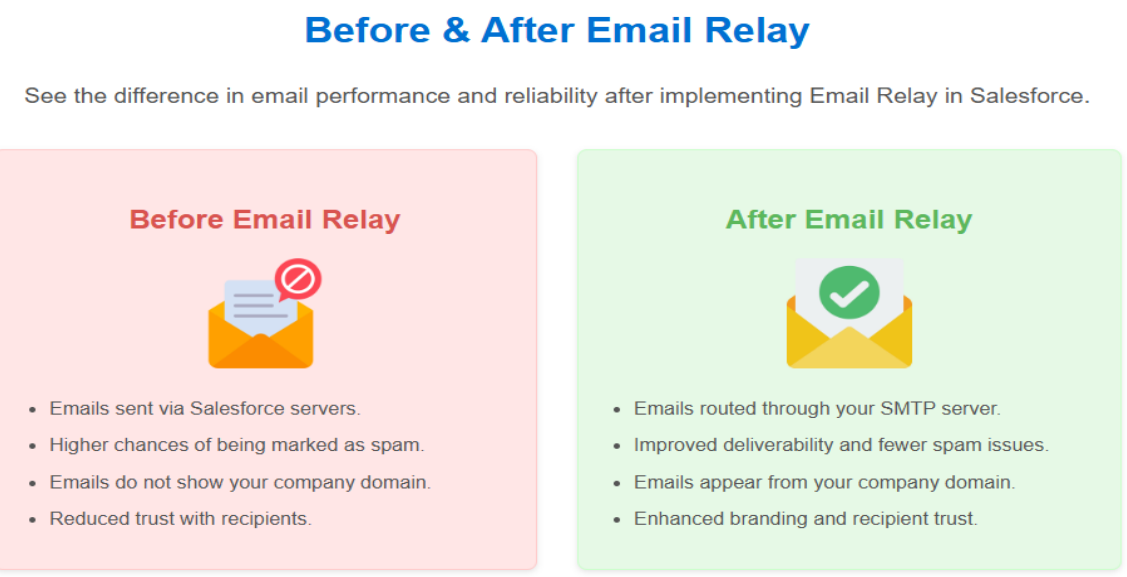
Another critical component of the email relay setup is the implementation of a DMARC (Domain-based Message Authentication, Reporting, and Conformance) policy. DMARC is essential for preventing email spoofing and phishing attacks. By establishing a DMARC policy, organizations can tell email receivers how to handle messages that fail to pass authentication checks. A properly configured DMARC policy, such as setting it to "reject," ensures that unauthorized emails are not delivered, further improving the organization’s email security and deliverability rates.

5. DKIM Signing to Boost Deliverability

Finally, DKIM (DomainKeys Identified Mail) signing is an important feature for improving email deliverability and security. DKIM allows the organization to attach a digital signature to outgoing emails, confirming that the emails originated from an authorized source and have not been tampered with during transmission. This signature helps email recipients' servers validate the authenticity of the email, reducing the likelihood of the email being marked as spam. DKIM signing, in combination with DMARC and SPF (Sender Policy Framework) records, enhances the organization's email reputation and ensures higher deliverability.

How email relay is different from standard email sending

The biggest difference shows up in email processing and delivery. Standard Salesforce email sending pushes messages directly through Salesforce's SMTP server. Email relay gives you complete control over delivery while you still use Salesforce's powerful features.



Before & After Email Relay

See the difference in email performance and reliability after implementing Email Relay in Salesforce.

Before Email Relay

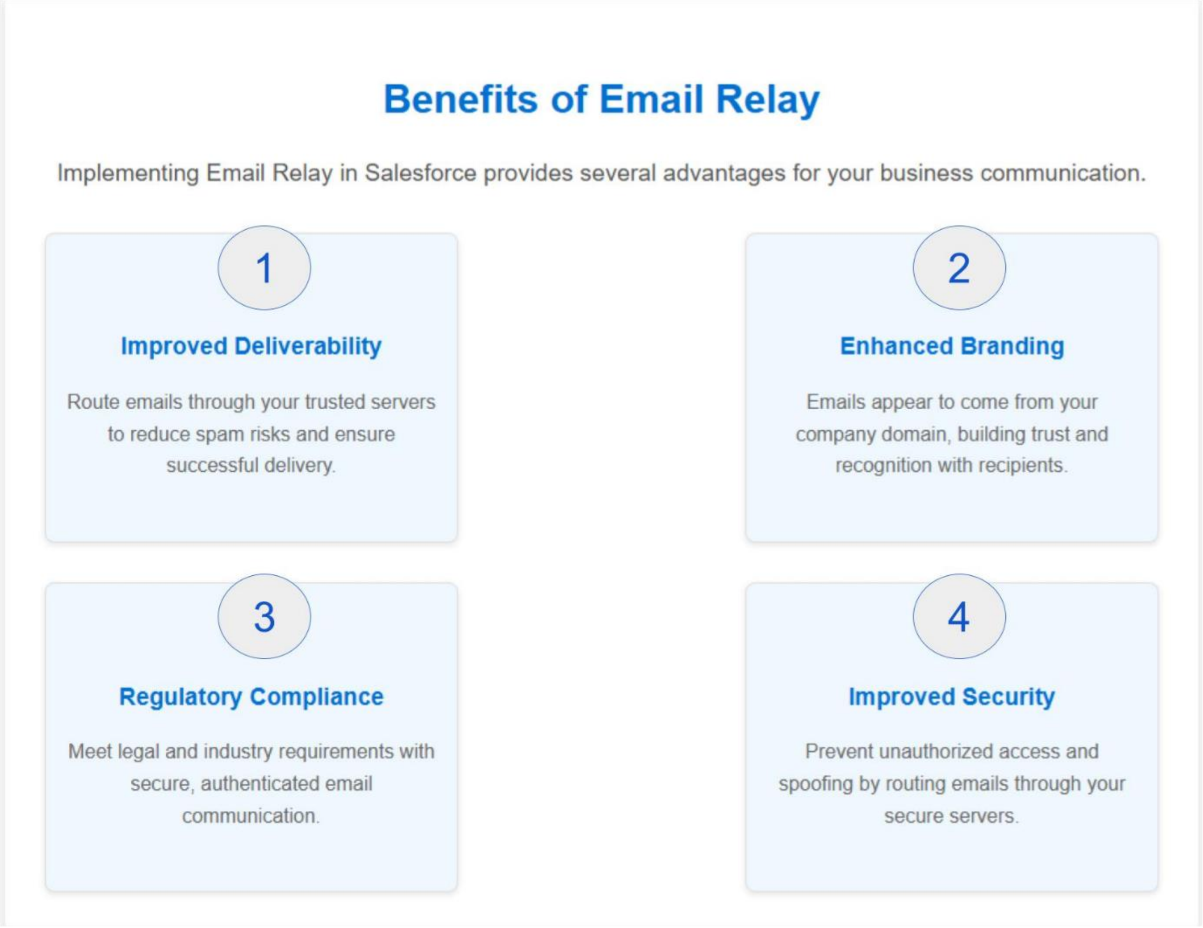
- Emails sent via Salesforce servers.
- Higher chances of being marked as spam.
- Emails do not show your company domain.
- Reduced trust with recipients.

After Email Relay

- Emails routed through your SMTP server.
- Improved deliverability and fewer spam issues.
- Emails appear from your company domain.
- Enhanced branding and recipient trust.

Fig II. Before and After Email Relay [2]

This setup brings unique benefits. Recipients see emails from their familiar domain instead of a generic Salesforce address. You also get better control of important metrics like opens, bounces, and spam complaints.



Benefits of Email Relay

Implementing Email Relay in Salesforce provides several advantages for your business communication.

1 Improved Deliverability

Route emails through your trusted servers to reduce spam risks and ensure successful delivery.

2 Enhanced Branding

Emails appear to come from your company domain, building trust and recognition with recipients.

3 Regulatory Compliance

Meet legal and industry requirements with secure, authenticated email communication.

4 Improved Security

Prevent unauthorized access and spoofing by routing emails through your secure servers.

Fig III. Benefits of Email Relay [3]

Email relay is a great way to stay compliant with industry regulations. Messages that route through your server can be archived centrally based on your organization's retention policies. Your existing content scan filters can also check outgoing messages that align with your organization's best practices.

Salesforce makes email relay accessible in Professional, Enterprise, Unlimited, Developer, and Performance editions. You'll still need to follow Salesforce's standard rules, including daily sending limits for users and organizations.

Prerequisites for Setting Up Email Relay

You should first verify our Salesforce edition and required permissions.

Email server requirements

To ensure smooth integration with Salesforce Email Relay, the SMTP server must meet specific security standards. One of the most critical requirements is support for Transport Layer Security (TLS) encryption, which ensures that email transmissions are secure and protected from unauthorized access during transit. In addition to TLS encryption, the server must support SMTP authentication, enabling Salesforce to securely authenticate the connection between its servers and the organization's relay host.

This authentication prevents unauthorized access and ensures that only legitimate email requests are processed. The server must also be capable of handling the expected email volume, which may vary based on the organization's Salesforce edition. For instance, Salesforce allows up to 5,000 emails per day per organization. Furthermore, the email server must comply with regional availability requirements, as Salesforce Email Relay is available across various regions, including Japan, Asia Pacific, Europe, and the Americas. Adhering to these server requirements ensures the email relay operates securely, efficiently, and within Salesforce's operational limits.

Domain verification checklist

Before setting up Salesforce Email Relay, it is essential to complete several domain-related tasks to ensure proper functionality and security. The sender email address used in the relay must belong to the organization's domain, meaning the organization needs full ownership of the email addresses it plans to use for sending emails. This ownership is vital for maintaining control over email communications and ensuring that the messages are recognized as legitimate by recipients. Once ownership is established, a few important steps must be taken to ensure secure and effective email delivery.

Establish a DMARC Policy

The first step in securing the domain is to establish a DMARC (Domain-based Message Authentication, Reporting, and Conformance) policy for the organization’s domain. DMARC helps prevent email spoofing by defining how emails that fail authentication should be handled. A DMARC policy helps ensure that only authorized email senders can send emails on behalf of the domain, enhancing email security and improving deliverability by reducing the likelihood of the emails being marked as spam.

Configure DKIM Signing for Outgoing Emails

Next, it is crucial to configure DKIM (DomainKeys Identified Mail) signing for all outgoing emails. DKIM adds a digital signature to each email, verifying that the email was sent by an authorized sender and ensuring its integrity. This digital signature helps recipients' email servers authenticate the email, making it less likely to be flagged as spam or rejected. DKIM signing is a key part of improving email deliverability and protecting against fraudulent email activities.

Verify the Hostname on Salesforce's Certificate

To further secure the email relay, it is important to verify the hostname on Salesforce's SSL/TLS certificate. This ensures that the email server being used for the relay matches the certificate provided by Salesforce, providing an extra layer of trust and verification. Proper verification helps ensure that the communication between Salesforce and the organization's email server remains secure and prevents man-in-the-middle attacks or other forms of unauthorized interception.

Set Up Proper SPF Records

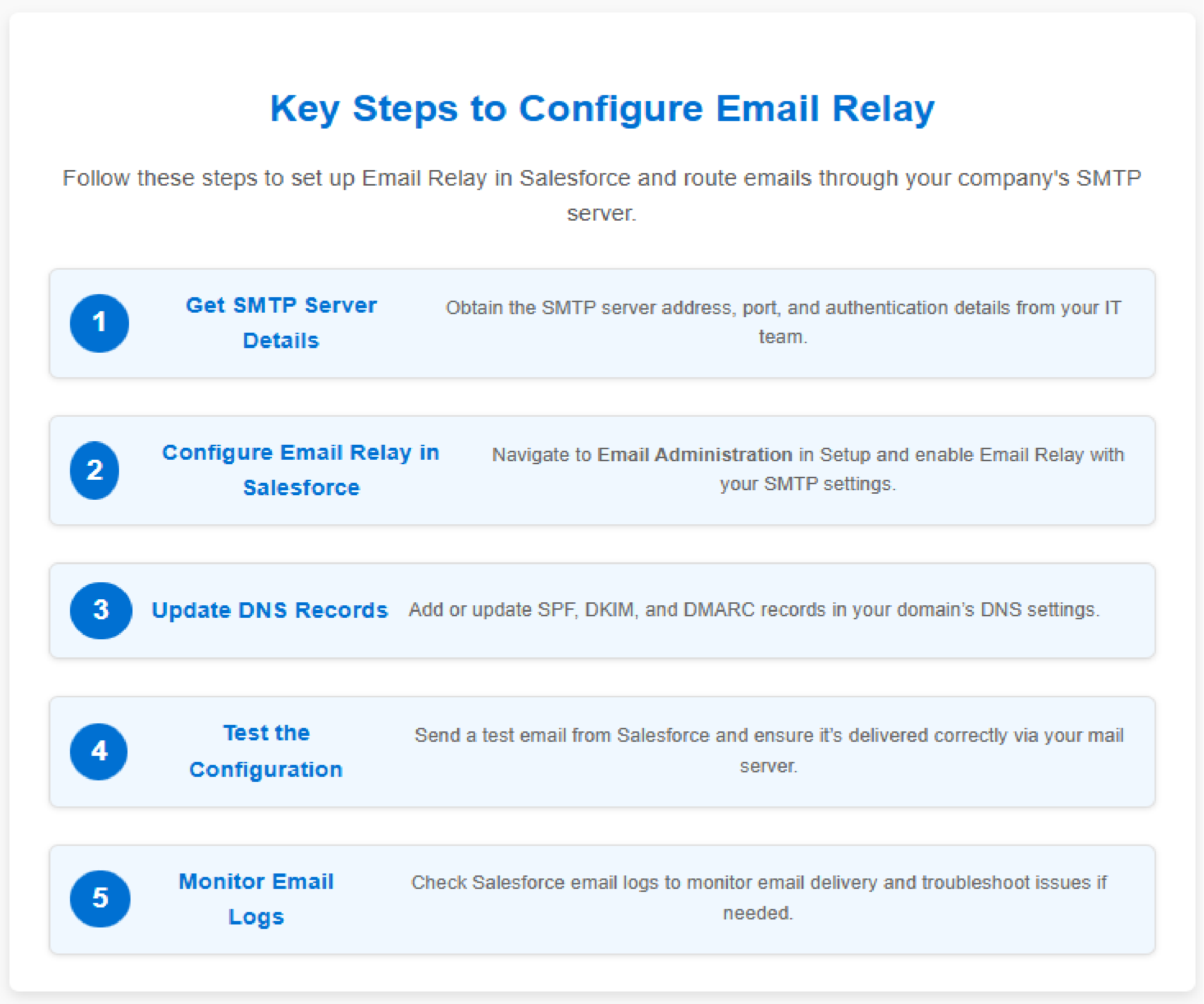
Lastly, setting up correct SPF (Sender Policy Framework) records is essential for preventing email authentication failures. SPF records specify which mail servers are authorized to send emails on behalf of the organization’s domain. This helps prevent unauthorized senders from impersonating the domain and ensures that the organization’s emails are authenticated by recipient mail servers. Proper SPF configuration reduces the risk of emails being marked as spam or rejected, thus ensuring higher email deliverability.

Testing these configurations in a sandbox environment is significant before implementing them in our production org. This approach helps us identify and fix any potential issues without affecting our live environment.

Organizations using Office 365 must complete domain authorization with Microsoft before relay setup. This step will give a proper integration between our email infrastructure and Salesforce's systems.

Configuring Email Relay with Gmail

Setting up email relay with Gmail needs attention to detail, but we've broken it down into simple steps. Let's get started by configuring our Google Workspace settings.



Key Steps to Configure Email Relay

Follow these steps to set up Email Relay in Salesforce and route emails through your company's SMTP server.

1 Get SMTP Server Details — Obtain the SMTP server address, port, and authentication details from your IT team.

2 Configure Email Relay in Salesforce — Navigate to **Email Administration** in Setup and enable Email Relay with your SMTP settings.

3 Update DNS Records — Add or update SPF, DKIM, and DMARC records in your domain's DNS settings.

4 Test the Configuration — Send a test email from Salesforce and ensure it's delivered correctly via your mail server.

5 Monitor Email Logs — Check Salesforce email logs to monitor email delivery and troubleshoot issues if needed.

Fig IV Key Steps[4]

Setting up SMTP relay in Google Workspace

To set up SMTP relay in Google Workspace, you first need to access the Google Workspace admin dashboard. This requires super admin access to the account. Once logged in, navigate to the “Apps” section in the dashboard, and select “G Suite,” then “Gmail.” From there, scroll down to the “Advanced Settings” section where you will find the “SMTP relay service” option. Click the “Configure” button to begin the setup process. This will allow you to configure the necessary settings to ensure secure and reliable email relay between Google Workspace and Salesforce, enabling emails to be sent through your organization’s domain instead of a generic Google address.

Configuring Gmail authentication settings

To ensure a secure and functional setup for Salesforce email relay with Gmail, you need to configure the authentication settings properly. Begin by setting the host to smtp-relay.gmail.com and the port to 587 (recommended over port 25 to avoid common blocks). For TLS settings, choose "Preferred" to ensure that all communications are encrypted. Under the authentication section, select “Only accept mail from specified IP addresses,” and add the appropriate IP addresses or ranges used by Salesforce for sending emails.

Next, navigate to the Google Workspace admin console and click on "Apps" in the left menu, then select "Gmail." Scroll to the "Routing" section and locate the SMTP relay service. Here, click on the "Edit Action" and configure the relay for Salesforce. Make sure to select “Only addresses in my domains” under "Allowed Senders" to restrict the relay to only authorized senders within your organization. Once you’ve entered the necessary IP ranges used by Salesforce, save the configuration.

Return to the Salesforce email relay setup and input the credentials for Google. You should now be able to run a deliverability test to verify that your relay is set up correctly. This process will help ensure that emails sent through Salesforce are securely relayed through your organization's domain, providing better deliverability and control over the messaging system.

Testing Gmail relay connection

After completing the Salesforce email relay configuration with Gmail, it’s crucial to verify that everything is functioning as expected. To do this, follow these steps:

Access Salesforce Setup: Log in to your Salesforce account and go to the Setup page.

Search for "Test Deliverability": Use the search bar to find the "Test Deliverability" option.

Enter a Test Email Address: Input a test email address, preferably a Gmail address, to receive the test message.

Send a Test Message: Click to send the test email.

Once the test email is sent, check the email headers in the received message. For Gmail users, open the email and click on “Show original” to view the detailed header information. Ensure that both SPF and DKIM entries show as “PASS,” indicating that the email has been authenticated correctly.

All emails sent through Salesforce will appear in your Gmail "Sent Mail" folder. To enable this feature, make sure you’ve turned on the "detailed mail storage" option in your Google Workspace settings.

After the setup, monitor the delivery of emails. If any issues arise, you can revisit your configuration settings or check the detailed logs available in both Salesforce and Google Workspace admin panels to troubleshoot and resolve any problems

Email Relay Security Configuration

Security is the lifeblood of any working email relay setup. Let's explore ways to strengthen our Salesforce email relay with reliable security measures.

Implementing TLS encryption

Transport Layer Security (TLS) encryption serves as the first line of defense in securing email communications. To ensure secure communication between Salesforce and the email server, TLS settings must be properly configured for the email relay. Key security components include:

Turn on TLS encryption for all outgoing messages to protect the data in transit.

Secure SMTP authentication to ensure that only authorized servers can send emails through the relay.

Certificate validation to authenticate the email server and prevent man-in-the-middle attacks.

Encrypted communication channels to safeguard sensitive information and prevent eavesdropping during transmission.

Setting up DMARC and SPF records

Without a doubt, proper domain authentication is critical to preventing email spoofing and enhancing email deliverability. To ensure secure and authentic email communications, we need to add the following records to our domain provider:

A. SPF Record

The Sender Policy Framework (SPF) record verifies that Salesforce is authorized to send emails on behalf of our domain.

We need to create an SPF record with the following value:

v=spf1 include:_spf.salesforce.com ~all

B. DMARC Policy Setup

The Domain-based Message Authentication, Reporting, and Conformance (DMARC) policy helps manage email authentication and reject unauthorized senders. Set up the DMARC policy options as follows:

- p=none (original testing phase)
- p=quarantine (intermediate security)
- p=reject (strictest protection)

After adding these records to our DNS configuration, it may take up to 24 hours for authentication to be completed. If authentication hasn't been successful within this time, it's essential to review the DNS configuration for any errors that may be preventing proper validation

Managing Authentication Protocols for Email Security

Our authentication strategy should incorporate multiple layers of protection, striking a balance between security and functionality. One of the key components of this strategy is implementing DKIM (DomainKeys Identified Mail). DKIM provides two modes of operation to control email authentication:

Strict Mode (adkim=s): This mode rejects emails that don't have the proper DKIM setup, offering a higher level of security by preventing unauthorized email senders from impersonating the domain.

Relaxed Mode (adkim=r): This mode provides more flexibility, allowing emails that may have minor DKIM discrepancies to be accepted, reducing the likelihood of legitimate emails being rejected.

To monitor the effectiveness of our security protocols, we should implement **aggregate reporting** (rua) and **forensic reporting** (ruf). These reports provide critical information about:

- Email traffic patterns
- Authentication failures

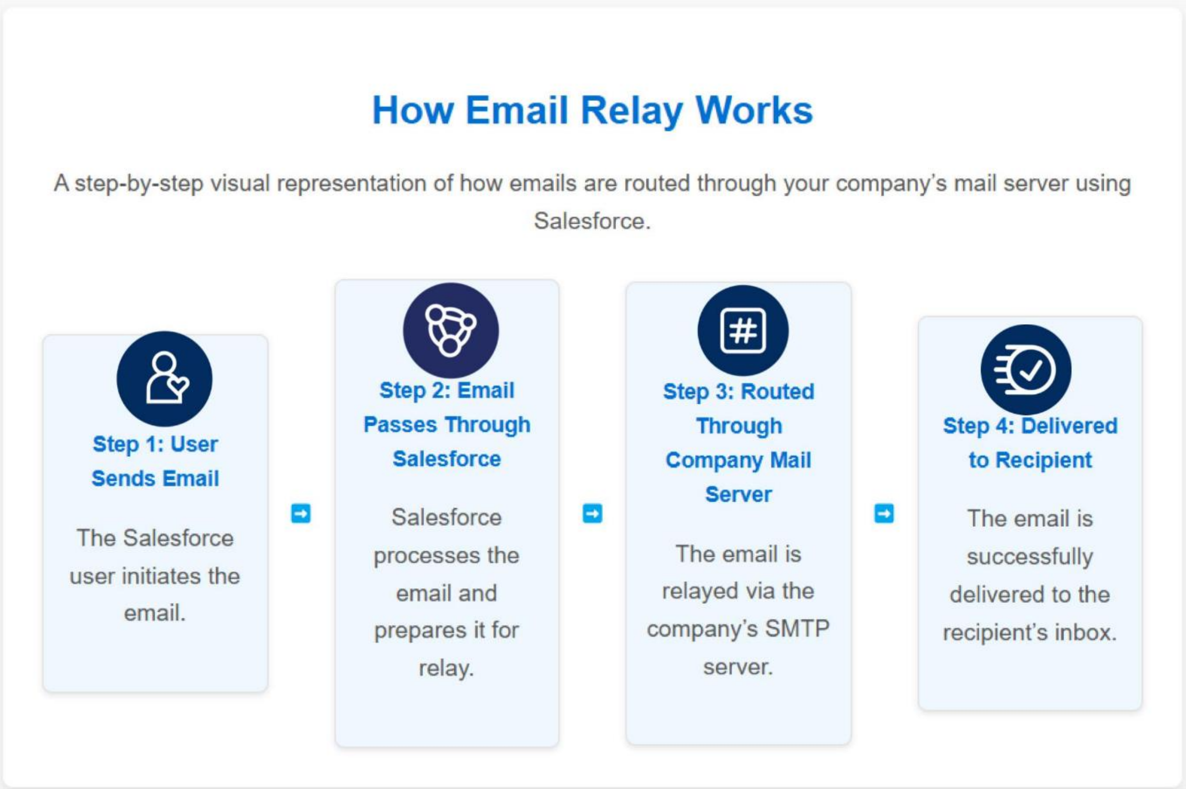
- Delivery success rates
- Potential security threats

The **"fo=1"** setting should be enabled to provide optimal protection. This setting generates reports when either SPF or DKIM authentication fails, allowing us to quickly identify and address any security issues. By reviewing these reports, we can stay on top of any potential vulnerabilities and resolve them before they escalate.

Before making any changes to DNS settings, it's essential to back up all existing configurations. A single incorrect modification could disrupt the functioning of your entire domain’s services. Additionally, it’s a best practice to have a colleague review your security configurations. Typos or errors in the configuration could result in costly issues, so an extra set of eyes can help ensure everything is set up correctly.

Testing and Validating Email Relay Setup

The email relay setup needs confirmation to ensure everything works correctly. Let's go through the key testing steps that ensure proper functionality.



How Email Relay Works

A step-by-step visual representation of how emails are routed through your company’s mail server using Salesforce.

Step 1: User Sends Email
The Salesforce user initiates the email.

Step 2: Email Passes Through Salesforce
Salesforce processes the email and prepares it for relay.

Step 3: Routed Through Company Mail Server
The email is relayed via the company’s SMTP server.

Step 4: Delivered to Recipient
The email is successfully delivered to the recipient’s inbox.

Fig V How Email Relay Works[5]

Running deliverability tests

We need to confirm our email relay configuration through Salesforce's built-in testing tools. Here's our testing process:

To confirm that the email relay configuration is correctly set up, we need to run a deliverability test using Salesforce's built-in tools. Start by navigating to Setup in Salesforce and entering "Deliverability" in the Quick Find box. From there, select "Test Deliverability." Next, enter a test email address, preferably one you control, such as a Gmail address, and click "Send Test."

Once the test is sent, you should receive a confirmation message indicating successful delivery. Keep in mind that DNS changes might take up to 48 hours to fully propagate through the system, so if the test doesn't go through immediately, give it some time for the DNS changes to take effect before testing again.

Verifying email headers

After receiving the test email, it's crucial to verify the email headers for a thorough check. Look for the presence of the **X-SFDC-LK header**, which should include your organization's unique ID, confirming that Salesforce is handling the email correctly. It's also important to ensure that the email is routed through the email server you configured for the relay. This confirms that Salesforce is utilizing the correct SMTP server for sending emails. Additionally, you should check the authentication results in the headers, especially for SPF and DKIM. Both should show a "PASS" status, indicating that the email has been successfully authenticated and complies with your domain's security policies. These steps will ensure that your email relay setup is functioning as expected.

Gmail users can check headers using the "Show Original" option. The header should show a chain of servers that has both Salesforce and our email relay server. To name just one example, a properly configured relay will show:

Received: from smtp02-ph2-sp1.mta.salesforce.com by smtp-relay.gmail.com

Case study

A mid-sized software company faced significant email delivery challenges that impacted their customer communication. Their issues were threefold: poor email delivery rates, inconsistent brand messaging in automated emails, and emails frequently ending up in spam folders. These problems had a direct effect on the business, as customer service emails reached only 82% of inboxes, and marketing emails had even lower success rates.

To address these problems, the company followed a structured approach. First, they conducted an original assessment where they documented their existing email setup, outlined their technical requirements, and created a timeline for implementation. The next phase focused on the technical setup, which included configuring SMTP settings, implementing authentication protocols, and adding essential security measures. They also moved into a testing phase where they ran a pilot program, closely monitored delivery rates, and made adjustments to improve their configuration.

During the setup, the team encountered a significant challenge when trying to integrate Office 365 with Salesforce. However, with the support of Salesforce, they created a custom solution that worked for their specific needs. Despite these hurdles, security remained a priority throughout the process. They added better TLS encryption, enforced stricter authentication rules, implemented detailed monitoring systems, and conducted regular security checks to ensure the integrity of their email delivery process.

The results were impressive. Within three months, email delivery rates reached 98%, spam delivery was reduced by 75%, and customer response rates increased by 40%. Long-term benefits included consistent brand messaging, fewer IT tickets related to email issues, and improved tracking and reporting capabilities. The project taught the company valuable lessons: thorough preparation, careful testing, and continuous monitoring were essential for success. The implementation team kept detailed documentation that helped train new staff and address ongoing challenges, ensuring that email performance continued to improve while maintaining security protocols.

Conclusion

Salesforce email relay helps businesses boost their email deliverability and keep their brand consistent. Email relay setup needs attention to detail when you're using Gmail or Office 365. You need to follow security protocols, set up proper authentication, and keep an eye on the system regularly. Companies that spend time on proper configuration see much better deliverability rates. Their emails also land in inboxes instead of spam folders more often.

The system comes with daily limits and technical requirements that might feel restrictive at first. But these boundaries keep performance optimal and protect against misuse. Your email relay system will deliver messages reliably to recipients if you monitor and maintain it regularly.

References

[1] Cirrus Insight, "Setting Email Relay in Salesforce with Google Apps," *Cirrus Insight Blog*, [Online]. Available: https://www.cirrusinsight.com/blog/setting-email-relay-salesforce-google-apps (accessed Apr. 25, 2021).

[2] Salesforce Stack Exchange, "How Can I Check If Email Relay is Working or Not," *Salesforce Stack Exchange*, [Online]. Available: https://salesforce.stackexchange.com/questions/231018/how-can-i-check-email-relay-is-working-or-not (accessed Apr. 28, 2021).

[3] Salesforce Official Documentation [Online]. Available: https://help.salesforce.com/s/articleView?id=release-notes.rn_sales_productivity_email_email_relay_enhancement.htm&release=224&type=5 (accessed Apr. 28, 2021).

[4] Salesforce Whiz, "Setting Up Salesforce Email Relay with G-Suite," *Salesforce Whiz Blog*, [Online]. Available: https://salesforcewhiz.wordpress.com/2020/07/17/setting-up-salesforce-email-relay-with-g-suite/ (accessed Apr. 30, 2021)

[5] Cloud on Purpose, "How to Configure Email Relay in Salesforce," *Cloud on Purpose Blog*, [Online]. Available: https://www.cloudonpurpose.com/blog/how-to-configure-email-relay-in-salesforce (accessed Apr 30, 2021).