|  |
| --- |
| SPF and DKIM |

SPF and DKIM Implementation Guide

Table of Contents

[**SPF and DKIM Implementation Guide** 3](#_Toc192174007)

[Summary 3](#_Toc192174008)

[Importance of Configuring SPF and DKIM 3](#_Toc192174009)

[Configure SPF 4](#_Toc192174010)

[Configure DKIM 4](#_Toc192174011)

[Final Sage People Configuration 6](#_Toc192174012)

[Helpful Salesforce References 6](#_Toc192174013)

**SPF and DKIM Implementation Guide**

Summary

Sage People, built on the Salesforce platform, enables organizations to streamline HR processes, including sending emails to employees, clients, and stakeholders directly from the Salesforce org. However, for these emails to reach their intended recipients reliably—without being flagged as spam or rejected by email servers—proper email authentication is essential. Configuring Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) ensures that emails sent from Sage People are recognized as legitimate by recipient email servers. This article outlines why SPF and DKIM are critical for Sage People email functionality and provides instructions to configure them based on Salesforce recommendations.

Importance of Configuring SPF and DKIM

When clients use Sage People to send emails—such as notifications, updates, or HR-related communications—these emails are sent through Salesforce’s email infrastructure on behalf of the client’s domain (e.g., @clientdomain.com). Without proper authentication, recipient email servers may view these messages as suspicious or unauthorized, leading to deliverability issues. Here’s why configuring SPF and DKIM is vital:

Improved Email Deliverability:

SPF and DKIM verify that emails originate from an authorized source (Salesforce, in this case), reducing the likelihood of messages being marked as spam or blocked entirely. This ensures Sage People emails land in recipients’ inboxes, not their junk folders.

Protection Against Spoofing:

SPF specifies which servers are allowed to send emails for the client’s domain, while DKIM adds a cryptographic signature to prove the email’s authenticity and integrity. Together, they prevent malicious actors from impersonating the client’s domain, safeguarding their reputation.

**Compliance with Email Standards:**

Major email providers like Google and Yahoo increasingly require sender authentication (SPF, DKIM, and sometimes DMARC) to combat phishing and spam. Configuring these protocols ensures Sage People emails meet modern security standards, avoiding disruptions.

Seamless Sage People Functionality:

Sage People relies on email for critical workflows, such as employee onboarding or performance reviews. Misconfigured authentication can interrupt these processes, leading to delays and frustration for end users.

Client Trust and Brand Integrity:

Emails that fail authentication may display warnings (e.g., “via salesforce.com”) or be rejected, eroding trust in the client’s brand. Proper SPF and DKIM setup ensures a professional sender identity aligned with the client’s domain.

In short, SPF and DKIM are foundational to ensuring Sage People emails are delivered reliably, securely, and with the client’s branding intact.

Configure SPF

SPF authorizes Salesforce to send emails on behalf of the client’s domain by adding a specific entry to the their domain name system (DNS). The configuration of SPF happens entirely outside of Sage People/Salesforce. The client’s domain administrator will do this by including a Salesforce entry in their DNS. For example:

include:\_spf.salesforce.com ~all

**NOTE**: The client domain or IT administrator will often request a list of Salesforce IP addresses instead of the adding the above to their SPF. This is strongly discouraged because Salesforce constantly changes their IP addresses. As a result, it will be very difficult for IT administrators to maintain them and will cause email deliverability issues when IP addresses are added or removed by Salesforce. The above SPF entry is a macro that points to the current Salesforce mail server IP addresses and removes the need to maintain the IP addresses manually.

Configure DKIM

DKIM adds a digital signature to emails, allowing recipients to verify their authenticity and ensuring only the client’s specific Salesforce org can send signed emails. It also helps to ensure the email wasn’t tampered with after it was sent by Sage People/Salesforce.The configuration of DKIM happens in both the Sage People/Salesforce org and the client’s DNS. You will create the DKIM keys in Salesforce and the client’s domain administrator will add them to the client’s DNS.

1. **Create the DKIM Keys in Salesforce**
	1. Navigate to the DKIM Keys page in Salesforce (Setup 🡪 Email 🡪 DKIM Keys)
	2. Click the ‘Create New Key’ button
	3. Choose ‘2048-bit’ for the ‘Key Size’
	4. Enter a name for the ‘Selector.’ For example: Sage
	5. Enter a name for the ‘Alternate Selector.’ For example: SageAlt
	6. Enter the client’s email ‘Domain.’ For example: clientsdomain.com
	7. Enter the ‘Domain Match Pattern’. This is normally set to the client domain entered in the previous step. For example: clientsdomain.com
	8. Click the ‘Save’ button



* 1. After the DKIM geys are generated, copy the entire values after the fields ‘CNAME Record’ and ‘Alternate CNAME Record’ and send these values to the domain administrator:



1. **Activate the DKIM Keys**

Once the client’s domain administrator has successfully added the DKIM Keys to their DNS, activate the DKIM Keys in Salesforce

* 1. Navigate to the DKIM Keys page in Salesforce (Setup 🡪 Email 🡪 DKIM Keys)
	2. Click on the ‘Selector’ for the DKIM Keys you created. **NOTE**: Don’t click on the ‘Edit’ link to open the DKIM Keys, you must click on the ‘Selector’ link to open them.
	3. Click the ‘Activate’ button. **NOTE:** This button will only be available if the DKIM Keys have been properly updated to the client’s DNS by the domain administrator. If the button is still grayed out, let the domain administrator know corrections to the DNS entries are needed.

Final Sage People Configuration

Once SPF and DKIM have been properly configured, there are a few final configuration steps that need to be completed in Salesforce.

1. Navigate to the Salesforce ‘Deliverability’ page (Setup 🡪 Email 🡪 Deliverability)
2. Uncheck the following two settings found on the ‘Deliverability’ page:
	1. Activate counce management
	2. Enable compliance with standard email security mechanisms

**NOTE**: the above settings are not needed when SPF and DKIM are being utilized and can cause deliverability issues when they are enabled for clients wtih SPF and DKIM configured.

1. Check the following setting found on the ‘Deliverability’ page:
	1. Verify the ownership of email sending domains by DKIM keys

**NOTE**: When DKIM Keys are configured, active, and the above setting is checked it means the Salesforce email address verification status check will be bypassed when users send emails since the ownership of email sending domain can be verified by active DKIM Keys. However, any Organization-Wide Addresses will still need to be verified even with DKIM Keys are configured.

1. Click the ‘Save’ button

Helpful Salesforce References

Salesforce provides some excellent resources that provides more details about SPF and DKIM. The following are populate references:

* Ensure you can receive email from the Salesforce application:
<https://help.salesforce.com/s/articleView?id=000388992&type=1>
* Sender Policy Framework (SPF):
<https://help.salesforce.com/s/articleView?id=sales.emailadmin_spf_overview.htm&type=5>
* Sender Policy Framework and Salesforce SPF Records:
<https://help.salesforce.com/s/articleView?id=000382664&type=1>
* Create a DKIM Key:
<https://help.salesforce.com/s/articleView?id=sales.emailadmin_create_secure_dkim.htm&type=5>
* SPF and DKIM Alignment Fails:
<https://help.salesforce.com/s/articleView?id=000381292&type=1>



# sage.com

# 0191 479 5911