Ensuring Email Delivery with DMARC Alignment in Puzzel Case Management using Puzzel Servers

Introduction

As email security standards become stricter, it's crucial for your organisation to ensure that your email communications comply with these standards to maintain high deliverability rates. This guide provides a step-by-step approach to align DMARC when using Puzzel Case Management/Puzzel Customer Insight with Amazon Simple Email Service (SES), ensuring your emails successfully reach your recipients without being flagged or rejected due to security policies. If you would prefer to use your own email service for sending email, please follow our SMTP setup guide instead.

Initial Email Channel Setup in Puzzel Case Management

To start sending emails through Puzzel Case Management, follow these initial setup steps:

1. **Create an Email Channel**: Set up an email channel within Puzzel Case Management, specifying the customer's own email address as the sender.
2. **Verify Email Ownership**: A verification email will be sent to the specified address (upon request by raising a support ticket), containing a unique link to confirm ownership. This step is crucial for proving that you have the right to use the email address.
3. **Once verified, our customer support team will configure the channel to Send via Amazon SES** Once verified, the email channel needs to be configured to send emails through the Amazon SES gateway, ensuring that emails are sent securely and reliably.

Authorising Puzzel Case Management via DNS Records

To authorise Puzzel Case Management to send emails on behalf of your domain, you'll need to add specific DNS records:

SPF Record

The Sender Policy Framework (SPF) record helps prevent email spoofing by specifying which mail servers are allowed to send emails on behalf of your domain.

- **For new SPF records**: Add `"v=spf1 include:spf.cm.puzzel.com ~all"` as a TXT record in your DNS settings.
- **If you already have an SPF record**: Append `include:spf.cm.puzzel.com` to your existing SPF record, followed by `~all`.

DKIM Record

DomainKeys Identified Mail (DKIM) adds a digital signature to emails, allowing the recipient to verify that the email was indeed sent from your domain and hasn't been tampered with.

- Add a CNAME record with:
    - **Hostname**: `lw._domainkey.yourdomain.com`
    - **Record**: `lw.domainkey.cm.puzzel.com`

Aligning DMARC to Avoid Email Rejection

Domain-based Message Authentication, Reporting, and Conformance (DMARC) ensures that legitimate emails are properly

Copyright ©2022 Puzzel Ltd. All rights reserved.

authenticated against established DKIM and SPF standards. To align DMARC and avoid email rejections due to security policies, follow these additional steps:

> Note
>
> This step represents a new addition to our standard onboarding process, reflecting the latest in best practices. Should you choose to implement these records for your existing sending domains, we kindly request that you submit a support ticket to notify our team once the updates are complete. This will enable us to activate the changes on our side promptly, ensuring a smooth continuation of service.

Setting up for DMARC Alignment

Create additional DNS records on a subdomain of your sending domain (e.g. puzzel.yourcompany.com) to ensure DMARC alignment:

MX Record

- **Priority**: 10
- **Record Value**: feedback-smtp.eu-west-1.amazonses.com

TXT Record for SPF

- **Value**: "v=spf1 include:domainkey.cm.puzzel.com ~all"

This configuration uses your subdomain for the MAIL FROM and return-path addresses, aligning with the domain for SPF lookups and ensuring compliance with DMARC policies.

Conclusion

Adhering to email security standards is vital for ensuring your communications reach their intended audience. By setting up SPF, DKIM, and ensuring DMARC alignment as outlined in this guide, you can significantly reduce the risk of email delivery issues when using Puzzel Case Management with Amazon SES. Always ensure that your DNS records are correctly configured and regularly review them to comply with evolving security practices, safeguarding your email communications against rejection or flagging by recipient email servers.

Copyright ©2022 Puzzel Ltd. All rights reserved.