User Guide for Cisco Domain Protection

June 22, 2018

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2018 Cisco Systems, Inc. All rights reserved.
Overview 1-1

Introduction 1-1
The DIY approach with As-Needed Help 1-1

History: The Need for DMARC 1-1

The Basics: What is DMARC? 1-2
What is a DMARC Enforcement Policy? 1-2
Who Endorses DMARC? 1-3

The Benefits of DMARC: Why You Should Care 1-4
Inbound Benefits 1-5
What is BEC? 1-5
DMARC and Inbound Threats: A Partial Solution 1-5

The Standards - A Closer Look 1-6
SPF - Sender Policy Framework 1-6
DKIM - DomainKeys Identified Mail 1-6
DMARC - Domain-based Message Authentication, Reporting, & Conformance 1-6

The Mechanics: How DMARC Works 1-7
What DMARC and Cisco Domain Protection Add 1-8

The Benefits - Before and After DMARC 1-9

General Process - Putting DMARC Into Practice 1-10
Why Implementing DMARC is Challenging 1-11
Specifying “Authentic” Email 1-11

What You’ll Be Doing 1-12
Moving toward a DMARC policy of “p=reject” 1-12

Before You Start 1-12

References 1-13

The Process of Implementing Cisco Domain Protection 2-1

The Overall Process 2-1

Step 1: Obtain Access to Portal 2-2
Advanced Topics 2-3

Step 2: Publish DMARC record(s) at Monitor 2-3
2a: Use the DMARC Builder to Create a Record 2-3
2b: Publish the Record in DNS 2-6

Step 3: Add Domains to the Portal 2-7
Step 3a: Organize your Domains into Groups  2-9

Monitoring  3-1
   Step 4: Monitor Traffic for a Period of Time  3-1
      Get Started with Monitoring  3-1
   Step 5: Identify a Target Domain or Set of Domains  3-5
   Step 6: Identify and Classify Senders  3-5
      The Senders Page  3-5
      What is the point of the Senders page?  3-7

Sender Policy Framework  4-1
   Sender Policy Framework (SPF)  4-1
      SPF Record Syntax  4-1
         Specifying IP Addresses  4-2
      SPF Alignment  4-3
   Step 7. Building and Proposing a New SPF Record  4-4
      Example: SPF for a Well-known Sender  4-4
      Example: SPF for a Custom Sender  4-8
   Using the “SPF Problems” Report  4-9
      Sharing or Subscribing to the Report  4-12
   Using the EasySPF™ Analyzer for an SPF Record  4-12
   Hosted SPF  4-18
      Stopping Hosting at Cisco  4-20
   Step 8 and 9: Publish SPF records and Identify Business Owners  4-21
      What if my Sender doesn’t support SPF?  4-21
   References  4-21

DomainKeys Identified Mail  5-1
   DomainKeys Identified Mail (DKIM)  5-1
      Overview: DKIM Involves Cryptography  5-1
      DMARC Requires DKIM Identifier Alignment  5-2
   Steps 10-11: Enabling DKIM on your Gateway  5-2
   Steps 12-14 - Enabling DKIM for 3rd Party Senders  5-3
      Request DKIM signing from Third-Party owners  5-3
      Implement DKIM keys for Third-Party Senders  5-4
      Verify DKIM for all Third-Party Senders  5-5
   DKIM Results Cisco Domain Protection  5-6
      Using the “DKIM Problems” Report to Find Issues  5-7
      Sharing or Subscribing to the Report  5-11
References 5-11

Moving to Reject 6-1
- Using DMARC for Enforcement 6-1
- Monitoring with Reports 6-1
- Report Interactivity 6-3
- Sharing and Scheduling 6-4
- Organizing Domains 6-5
- Steps 15 and 16: Enforce 6-8
- Congratulations! 6-9

Monitoring for Changes 7-1
- Monitoring past Reject 7-1
- Alerts 7-1
- What’s Next... 7-3

User Accounts 8-1
- Adding Users 8-1
- Activate New Users 8-2
- User Roles 8-2
- Administrator roles 8-2
- Read-only roles 8-2
- Domain-specific access 8-3
- Role Usage Examples 8-3
Overview

Introduction

This guide introduces you to **DMARC** — Domain-based Message Authentication, Reporting & Conformance — and how to use Cisco Domain Protection™ to guide you through the process of implementing DMARC for your organization.

Cisco Domain Protection is designed to help you protect your customers from phishers, spammers, and other email abusers who attempt to send inauthentic email purporting to be from you by helping you establish DMARC policies for your domains.

DMARC is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author (“From:”) domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of your domain from fraudulent email.

**Audience**

This guide is intended for use by email administrators who are starting to manage DMARC for their organizations.

The DIY approach with As-Needed Help

You can use Cisco Domain Protection and this guide to help you through the process of setting up, managing, and maintaining DMARC policies for your domains.

Cisco Domain Protection gives you visibility into data about email bearing your brand, tools to analyze that data in meaningful ways, tools to generate various files for implementing DMARC, and helpful tips for accomplishing tasks that cannot be enabled from a user interface.

History: The Need for DMARC

Email – despite its importance, ubiquity, and staying power – has never been secure.

Prior attempts at security have failed to solve email’s fundamental flaw – anyone can send email using someone else’s identity. This flaw has put the power of the world’s most admired brands in criminal hands: through email, criminals can use almost any brand to send spam, phishing emails, and malware installs, inflicting direct losses to customers and eroding the brand equity companies have spent years building up.
Many of the most respected brands in the world, including Facebook, Apple, JPMorgan Chase and PayPal, have adopted the DMARC standard to protect their customers and their brand.

Using DMARC, companies gain unprecedented visibility into legitimate and fraudulent mail sent using their domain names. The magic of DMARC is the ability to understand all the different mail streams being sent claiming to be from you - third parties, business units, threat actors. The overall impact to companies that have adopted DMARC is preservation of brand equity, elimination of customer support costs related to email fraud, and renewed trust and engagement in the company’s email channel.

DMARC – an open standard enabled on 70% of the world’s inboxes and also by the most security-forward brands – is the only solution that enables Internet-scale email protection and prevents fraudulent use of legitimate brands for email cyberattacks.

The Basics: What is DMARC?

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an open email standard published in 2012 by the industry consortium DMARC.org to protect the email channel. DMARC extends previously established authentication standards for email and is the only way for email senders to tell email receivers that emails they are sending are truly from them.

DMARC allows companies that send email to:

- **Authenticate all legitimate email** messages and sources for their email-sending domains, including messages sent from your own infrastructure as well as those sent by 3rd parties.

- **Publish an explicit policy** that instructs mailbox providers what to do with email messages that are provably authentic. These messages can either be sent to a junk folder or rejected outright, protecting unsuspecting recipients from exposure to attacks.

- **Gain intelligence on their email streams** by letting them know who is sending mail from their domains. This data helps companies to not only identify threats against their customers, but also discover legitimate senders that they may not even be aware of.

What is a DMARC Enforcement Policy?

When you set a DMARC policy for your organization, you as an email sender are indicating that your messages are protected. The policy tells a receiver what to do if one of the authentication methods in DMARC passes or fails.
Who Endorses DMARC?

DMARC is endorsed by the world’s largest senders, receivers, and industry consortia. More than 2.5 Billion Mailboxes Worldwide are DMARC-enabled.

Some of the world’s largest email *Senders* supporting the DMARC standard include the following organizations:

Some of the world’s largest email *Receivers* supporting DMARC include the following:
The Benefits of DMARC: Why You Should Care

**Brand Protection**
It is only a matter of time before a criminal will use your domain for his own benefit. Whether the criminal activity is phishing, malware distribution, or nuisance spam, it harms your brand to be associated with these attacks.

**Increased Email Deliverability**
Even legitimate messages may wind up in the spam folder if the receiver can’t tell the good from the bad.

In addition, the DMARC standard is endorsed by the following government agencies and industry trade organizations:

**Government Agencies**
- NIST - the National Institute of Standards and Technology  
  https://www.nist.gov/
- FTC - the Federal Trade Commission  
  https://www.ftc.gov/
- GOV.UK - https://www.gov.uk/

**Industry Associations**
- OTA - Online Trust Alliance  
  https://otalliance.org/
- M3AAWG - Messaging Malware Mobile Anti-Abuse Working Group  
  https://www.m3aawg.org/
- DMARC.org - https://dmarc.org/
- FS-ISAC - Financial Services Information Sharing and Analysis Center  
  https://www.fsisac.com/
- NH-ISAC - National Health Information Sharing and Analysis  
  https://nhisac.org/
By deploying DMARC, you can improve deliverability of your legitimate messages while eliminating the fraudulent.

**Service Calls**
Customers don’t call or send email to ask about phishing messages if they never receive those messages in the first place! One Cisco customer was able to redeploy 60 staff members after publishing a reject policy on a highly phished domain.

**Visibility Into Cyberattack Risk**
Do you know every 3rd party company sending email on behalf of your company? While 3rd party senders are needed, each time you provide customer, employee, or partner details to a 3rd party, you increase the risk of cyberattacks. DMARC enables you to see every 3rd party sending on your behalf to ensure they comply with email best practices.

**Inbound Benefits**
Implementing DMARC can also prevent some inbound email threats like BEC.

**What is BEC?**
Business Email Compromise (BEC) is an inbound threat where attackers impersonate company officials and send deceptive emails requesting wire transfers to alternate, fraudulent accounts. Often results in successful intrusion and access to victims’ credentials.

**Characteristics**
- Driven by social engineering and digital deception
- Contains no malicious links, malware or malicious content
- Easily evades the leading secure email gateways

**DMARC and Inbound Threats: A Partial Solution**
When configured correctly, DMARC stops phishing attacks where the attacker sends an email with a ‘From’ address that appears to originate from a protected domain. This makes it ideal for outbound phishing prevention, but is not an acceptable solution for inbound traffic.

<table>
<thead>
<tr>
<th>Inbound Deception Technique</th>
<th>Addressed by DMARC?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct / Same Domain Spoofing</td>
<td>Yes</td>
</tr>
<tr>
<td>Display Name Spoofing</td>
<td>No</td>
</tr>
<tr>
<td>Look-alike Domain Spoofing</td>
<td>No</td>
</tr>
</tbody>
</table>

While DMARC partially addresses BEC and sophisticated inbound threats, you need to augment your gateway protections with a comprehensive layer that identifies all forms for sender identity deception.
The Standards - A Closer Look

- SPF - Sender Policy Framework
- DKIM - DomainKeys Identified Mail
- DMARC - Domain-based Message Authentication, Reporting, & Conformance

SPF - Sender Policy Framework

SPF (Sender Policy Framework; IETF publication RFC 7208 dated April 2014) is an authentication standard that allows domain owners to specify which servers are authorized to send email with their domain in the Mail From: email address. SPF allows receivers to query DNS to retrieve the list of authorized servers for a given domain. If an email message arrives via an authorized server, the receiver can consider the email authentic.

Figure 1-4 Example DNS Record for SPF

e.example.net. IN TXT "v=spf1 a mx -all"

Weakness - SPF is not ideal for all email use cases and can fail if a message is forwarded. The Mail From: domain authenticated by SPF is not easily visible by an email recipient.

DKIM - DomainKeys Identified Mail

DKIM (Domain Keys Identified Mail; RFC 8301 dated January 2018) is an authentication standard that cryptographically associates a domain name with an email message. Senders insert cryptographic signatures into email messages which receivers can verify by using DNS-hosted public keys. When verification is successful, DKIM provides a reliable domain-level identifier that survive forwarding (unlike SPF).

Figure 1-5 Example DNS Record for DKIM

selector._domainkey.example.net IN TXT "v=DKIM1; k=rsa; p=public key data"

Weakness - DKIM is generally more complex to set up than SPF, requiring a cryptographic signature on each message sent. DKIM will fail when content is modified in transit, like messages sent through a mailing list.

DMARC - Domain-based Message Authentication, Reporting, & Conformance

DMARC (Domain-based Message Authentication, Reporting & Conformance; RFC 7489 dated March 2015) is an email authentication standard that works in conjunction with SPF & DKIM, bringing long-missing features to email – enabling senders to gain visibility into how their email domains are used and abused, describing how to combine existing authentication technologies to create secure email channels, and providing receivers with clear directives on how to safely dispose of unauthorized email – all at Internet scale.
The Mechanics: How DMARC Works

The DMARC model uses DNS as the mechanism for policy publication. DMARC records are hosted as TXT DNS records in a DMARC specific namespace. The DMARC namespace is created by prepending “_dmarc.” to the email domain that is to become DMARC compliant. For example, if the email domain “example.com” publishes a DMARC record, issuing a DNS query for the TXT record at “_dmarc.example.com” will retrieve the DMARC record.

The DMARC specification allows senders to publish policy records containing parameters that receivers use to inform the processing of emails that purport to come from the sender’s email domain. The features that DMARC enables are:

- **Flexible policies.** The DMARC model allows email senders to specify one of three policies to be applied against email that fails underlying authentication checks:
The Mechanics: How DMARC Works

Table 1-2 DMARC Policy Options

<table>
<thead>
<tr>
<th>DMARC Policy Setting</th>
<th>Syntax</th>
<th>Action Taken by Receivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (&quot;Monitor&quot;)</td>
<td>&quot;p=none&quot;</td>
<td>&quot;p=none&quot; policy means no policy should be applied; that is, the Domain Owner is not asking the Receiver to take action if a DMARC check fails. This policy is also often referred to as &quot;monitor&quot; policy. This option is used when senders simply want to collect feedback from receivers. This policy allows the domain owner to receive reports about messages using their domain even if they haven’t deployed SPF/DKIM, so that they could for example determine if their domain is being abused. There would be no change in how their messages are treated; however domain owners would now gain some visibility into what mail is being sent under the domain’s name. If you have not yet deployed SPF or DKIM, start by publishing a DMARC policy first because of its reporting capabilities.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Quarantine</td>
<td>In a quarantine policy, email that fails authentication checks should be treated with suspicion. Quarantine instructs receivers to “set messages failing DMARC aside for additional processing.” Most receiving mail systems will deliver these messages to an end user’s spam-folder. It could mean increased anti-spam scrutiny or tagging as “suspicious” to end-users in some other way.</td>
</tr>
<tr>
<td>Reject</td>
<td>Reject</td>
<td>Do not accept messages that fail the DMARC checks.</td>
</tr>
</tbody>
</table>

- **Sub-domain-specific policies.** DMARC records can specify different policies for top-level domains vs. sub-domains (using the “p=” and “sp=” tags).
- **Phased rollout of policy.** DMARC records can include a “percentage” tag (“pct=” ) to specifies how much of an email stream should be affected by DMARC policy. Using this feature, senders can experiment with progressively stronger policies until enough operational experience is gained to move to “100% coverage.”
- **Identifier Alignment flexibility.** The DMARC specification allows domain owners to control the semantics of Identifier Alignment. For both SPF and DKIM generated authenticated domain identifiers, domain owners can specify if strict domain matching is required or if parent and/or sub-domains can be considered to match.
- **Feedback controls.** DMARC records include parameters that specify where, how-often, and in which format feedback should be sent to the email domain owner.

What DMARC and Cisco Domain Protection Add

So DMARC adds important functionality to that available through SPF and DKIM:

- Flexible policy options for acting upon SPF and DKIM authentication failures — this is the “missing piece” in the SPF and DKIM specifications that is necessary for elimination of malicious emails.
- The ability to gather data on all email senders using your domain name. DMARC sends data in XML format to the address of your choosing.

The XML data that DMARC generates can be difficult to handle, in part because the email data is usually extremely voluminous. In handling and analyzing the data, keep in mind the following needs:

- Data needs to be analyzed in aggregate to visualize trends.
• Individual emails must be available to analyze sender details.
• Historical data should be housed for the insights it can provide on both threats and legitimate senders.

Cisco’s data analysis gives you the benefit of its experience working with the world’s highest volume email senders to help you interpret and understand the data that comes in from DMARC. In addition, for all related tasks that must be performed outside of any user interface, Cisco assists you in creating the properly formatted files.

Cisco Domain Protection fills in the missing pieces between the protocols:
• reports interpretation based on industry understanding of email ecosystems
• visibility of actual sample email messages
• guidance through key steps in implementation

The Benefits - Before and After DMARC

Without DMARC, brands have limited visibility into how domains are being used to send email:

Figure 1-8    Before Implementing DMARC

DMARC provides visibility into all email traffic and then instructs receivers how to handle unauthenticated emails, all outside of the mail flow:
General Process - Putting DMARC Into Practice

The detailed process for implementing DMARC using Cisco Domain Protection is the remainder of this guide; however, the high-level process is as follows: domain owners who wish to become DMARC-compliant need to perform 3 activities, repeating as necessary for each domain they plan to protect:

Step 1  **Publish a DMARC record.** To begin collecting feedback from receivers, publish a DMARC record as a TXT record with a domain name of “_dmarc.<your-domain.com>”:

```
_a TXT record with a domain name of “_dmarc.<your-domain.com>”:
```

Doing so will cause DMARC-compliant receivers to generate and send aggregate feedback to “dmarc-feedback@<your-domain.com>”. The “p=none” tag lets receivers know that the domain owner is only interested in collecting feedback.

Step 2  **Deploy email authentication: SPF and DKIM.**

- Deployment of SPF involves creating and publishing an SPF record that describes all of the servers authorized to send on behalf of an email domain. Small organizations usually have simple SPF records, where complex organizations often maintain SPF records that authorize a variety of data-centers, partners, and 3rd-party senders. DMARC-supplied aggregate feedback can help identify legitimate servers while bootstrapping an SPF record.

- Deployment of DKIM requires domain owners to configure email servers to insert DKIM-Signatures into email and to publish public keys in the DNS. DKIM is widely available and supported by all major email vendors. DMARC-supplied aggregate feedback can help identify servers that emit email without DKIM signatures.

Step 3  **Ensure that Identifier Alignment is met.** DMARC-supplied aggregate feedback can be used to identify where underlying authentication technologies are generating authenticated domain identifiers that do not align with the Email Domain. Correction can be rapidly made once misalignment is identified.
Why Implementing DMARC is Challenging

**Poor Visibility**
Most companies don’t realize how complex their email ecosystem is until they begin getting aggregate data from DMARC reporting. Standard reporting comes in the form of individual XML files that specify domain names, IP addresses and authentication details. While many tools can parse and visualize this XML data, making sense of the stream and understanding what subsequent actions to take to improve the authentication status of domains is very difficult and error prone, requiring a deep understanding of email flows.

**Discovering & Authorizing 3rd Party Senders**
The most challenging step of the DMARC journey is understanding all of your 3rd party senders and ensuring that legitimate senders are authenticating properly. On average, customers have 64% of legitimate emails sent through 3rd parties like as Salesforce.com, Marketo, or MailChimp.

**Figure 1-10 Prevalence of 3rd-party Senders**

The Cost of “Doing it Wrong”
Despite the emergence of new messaging platforms, email continues to be the most critical vehicle for communication and digital engagement for organizations. Incorrectly configuring authentication can lead to false positives, deliverability issues, and brand damage. Taking the final step to a Reject policy can be a daunting prospect if the business impact of undeliverable email is unknown or cannot be predicted.

**Specifying “Authentic” Email**
Cisco Domain Protection and the DMARC specification allow you to identify and authorize legitimate (approved) senders who send mail “from” your domain differently from illegitimate senders who may be abusing your brand.
What You’ll Be Doing

While DMARC implementation involves a level of technical understanding of the specifications and how to use them, it also involves administration, management, and communication. Over time, you are likely to gain an intimate understanding of email senders, both internal and external to your organization.

Moving toward a DMARC policy of “p=reject”

DMARC is initially implemented by adding TXT record in the DNS record for your domain. The file contains properties and values that you edit to specify how DMARC applies policies for the domains that you control.

Your goal in the process of implementing DMARC is to move, ultimately toward a policy (labeled ‘p’) of ‘p=reject’. A reject policy tells email receivers that all non-compliant emails should be discarded. However, the DMARC specification contains a variety of policies to afford a gradual implementation, without impacting your mail flow. Allowing for incremental deployment and strengthening of DMARC policies was a primary design goal for the specification. See Table 1-2, ‘DMARC Policy Options,’ on page 8.

You should start with a simple “monitoring-mode” record for a sub-domain or domain, that requests that DMARC receivers send you statistics about messages they see using your (sub-)domain. You can do this even before you’ve implemented SPF or DKIM in your messaging infrastructure (though until they are in place you won’t be able to move beyond this step).

As you introduce SPF (Chapter 4, ‘Sender Policy Framework,’ on page 1) and DKIM (Chapter 5, ‘DomainKeys Identified Mail,’ on page 1), the reports will provide the numbers and sources of messages that pass these checks, and those that don’t. You can easily see how much of your legitimate traffic is or is not covered by them, and troubleshoot any problems. You’ll also begin to see how many fraudulent messages are being sent, and where from.

When you believe that all or most of your legitimate traffic is protected by SPF and DKIM, you can implement a “quarantine” policy — you’re now asking DMARC receivers to put messages using your domain that fail both of these checks into the local equivalent of a spam folder. You can even request that only a percentage of your email traffic have this policy applied – you’ll still get the statistical reports that allow you to see what’s happening to your messages.

Eventually as any implementation problems are addressed, you can increase that percentage to 100% at whatever pace you’re comfortable with. In the end, all messages that fail the DMARC checks should be going to the spam folder instead of your customers’ inboxes.

Before You Start

Before you start with your DMARC implementation using Cisco Domain Protection, you will need to perform the following tasks:

Step 1  Ensure you have access to the Cisco Domain Protection portal  
Your Cisco representative should have provided access for at least one user account to Cisco Domain Protection portal located at 

Contact Cisco support https://www.cisco.com/support/, or submit a support case to support@cisco.com. 
For urgent matters, please call Cisco support at 855-682-1708
Chapter 1      Overview

The one user account is an administrative account; additional user accounts (with varying roles and permissions for delegated administrative or read-only rights) can be created from this original account. For details, see Chapter 8, `User Accounts,' on page 1.

Step 2  Gather a list of domains
You will need a list of domains — and sub-domains — which you plan to protect for your organization. This list should include the primary domain for your organization — that is, the one most associated with your organization and the one most used for sending email (for example: your organization) — as well as any defensive or test domains that your organization owns and maintains (for example: domains that you, domains that your organization, domains that your test, etc.). Keep in mind any history of mergers and acquisitions, along with specific instances where domains were created and used to distinguish products and processes.

Step 3  Obtain the ability to make DNS changes
You will need the ability to make changes to the Domain Name System (DNS) records for the domains you plan to protect. The DMARC authentication protocol (as well as the SPF and DKIM protocols) relies on DNS services in order to perform authentication. You'll need to make changes to DNS throughout the process of securing your domains — from getting initial data to flow into Cisco Domain Protection, to modifying your DMARC policies from monitor to reject.

Step 4  Compile a list of Stakeholders
The process for authenticating all outbound email for your organization may involve a large number of groups, depending on the size of your organization. For example, you may have dedicated a outbound marketing that communicates with potential customers, a support team which communicates with existing customers, and a business continuity team tasked with sending order confirmations or receipts from back-end systems. All teams need to be aware of requirements for authentication the email they send on behalf of your organization — as well as the deliverability issues if they fail to authenticate properly as DMARC policies you enable become more stringent. Communicate early and often throughout this process!

References

Patrick Peterson. “DMARC Whiteboard Session”
https://www.youtube.com/watch?v=6ZyzR1xNV0E
The Process of Implementing Cisco Domain Protection

The Overall Process

Cisco Domain Protection is the leader in helping customers implement DMARC and email authentication.

At the highest level, the process involves these five *phases*:

<table>
<thead>
<tr>
<th>Table 2-1</th>
<th>The Overall Process for Implementing Cisco Domain Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase</td>
<td>Step</td>
</tr>
</tbody>
</table>
| Phase 1   | 1. Obtain access to portal and receive introductory training from Cisco.  
           | 2. Publish DMARC record(s) at Monitor  
           | 3. Add domains to portal |
| Phase 2   | 4. Monitor traffic  
           | 5. Identify Target Domains  
           | 6. Identity and classify all Senders (Well-known and Custom) |
| Phase 3   | 7. Propose new SPF Record  
           | 8. Publish new SPF Record  
           | 9. Identify internal business owners  
           | 10. Enable DKIM signing on email gateway  
           | 11. Verify DKIM working on email gateway  
           | 12. Request DKIM signing from third-party owners  
           | 13. Implement DKIM keys for all third-party senders  
           | 14. Verify DKIM working for all third-party senders |
| Phase 4   | 15. Obtain sign-off from all business owners  
           | 16. Move DMARC record(s) to Reject |
| Phase 5   | 17. Review Alerts and Reports |
Cisco’s best practices for authenticating email from all of your domains using Cisco Domain Protection will typically comprise the specific steps in the following table:

**Note**
You can think about steps 2 and steps 4-17 as a repeatable process for each of the domains in your organization you plan to protect.

Some domains can move through this process quickly — for example defensive or internal domains which you own but never plan to use to send any legitimate email.

Other domains — for example, your primary domain, or a domain with extremely high volume — will require you to move through each step in the process methodically and communicating changes to stakeholders as appropriate.

The following chapters provides assistance for understanding and completing each step, especially with supporting data available in Cisco Domain Protection.

**Step 1: Obtain Access to Portal**

As part of the typical initiation and on-boarding process, you should receive a brief overview of accessing the Cisco Domain Protection portal.

During this kick-off meeting, your Cisco representative will grant access to Cisco Domain Protection at https://dmp.cisco.com.

Cisco sends you an email with your access information; this account is the first administrative account for your organization, and this will be used to create additional user accounts for your organization.
Advanced Topics

Some items to consider at this stage:

- Cisco Domain Protection contains roles-based permissions and access control (RBAC) which grants differing levels of permissions to user accounts within the portal. You may want to think about creating a read-only user, an audit-only user, or a user who can only administrates reports within the portal, for example. To learn more about permissions, see Chapter 4, `Sender Policy Framework,' on page 1.
- Once you log into the portal, you will be redirected to a URL which is unique for your organization, for example: https://organization_name.dmp.cisco.com
- Cisco provides an API for accessing some portions of the product programmatically. To access the API documentation, you will need to create a user account and grant API access permissions to that user.
- Cisco also supports Single Sign-On (SSO), either initiated from a Service Provider (SP-initiated) or directly from an Identity Provider (IdP-initiated). To learn more setting up SSO for your organization, contact a Cisco representative.
- The administrator account (and any subsequent accounts with user creation permissions) can reset passwords for users you create.

Step 2: Publish DMARC record(s) at Monitor

Publishing a DMARC record at a Monitor policy is one of the very first steps you’ll take in protecting your domain; it is also the method to start having data flow into the Cisco Domain Protection portal, and, indirectly, a way for you to for you to show to Cisco that you are the owner of the domain. DMARC policies are published in the DNS as text (TXT) resource records (RR) and announce what an email receiver should do with non-aligned mail it receives for email from the given domain.

For each domain you plan to protect, you’ll publish a DMARC record with the “none” flag set for the policies; this requests that data reports be sent from receivers to Cisco. You can then use Cisco Domain Protection to analyze the data and modify your mail streams as appropriate.

Note
A DMARC record with “none” flag set for its policy does not impact mail flow or the deliverability of messages sent from that domain. A “none” flag is the simply first step in the process of authenticating email from your domains: it allows you to collect data for analysis. Over time, as you implement SPF and DKIM for a domain and authorize senders (in the following steps of this guide), you can modify your DMARC policy flags to a more stringent policy (like “quarantine” and ultimately, “reject.”)

2a: Use the DMARC Builder to Create a Record

Cisco’s DMARC Builder allows you to look up the DMARC policy record for any domain. You can then use the DMARC Builder to either modify or create the text of a valid DMARC record for the domain(s). Finally the DMARC Builder provides information about the DNS provider for the domain and how to get the DMARC record published.

Step 1
After logging into the Cisco Domain Protection portal, navigate to the Tools > DMARC page.
Step 2: Enter a domain name and click “Look up” to view the domain’s current DMARC record or create a new one.

If the domain has no DMARC policy, you will be presented with the option to create a new DMARC record or to host a new DMARC record at Cisco:

Click “Create new DMARC record” to create a new record.

(This guide assumes you’ll be editing your own DNS infrastructure. Contact Cisco Support if you are interested in hosting DMARC records at Cisco.)

For example:
In this example, the domain is “foo.com”, the policy is “Monitor,” and the email address at Cisco to send reporting data to is “pauls-mints-and-gum@rua.cisco.com” and “pauls-mints-and-gum@ruf.cisco.com.” Below are descriptions of the different DMARC policy record fields which you can edit in the DMARC Builder.

**Domain(s):** The domain name for which you are creating or modifying a DMARC record. This can be a single domain or a comma separated list of domain names.

**Policy:** The action that a domain owner requests email receivers to take on messages with their domain in the header From address which fail DMARC.

- **None:** This tells a receiver to take no special action on messages which fail DMARC, but send DMARC data to the specified reporting addresses in the domain’s DMARC record. **Note: This is the recommended policy to choose in this step.**
- **Quarantine:** This requests that receivers place messages which fail DMARC in the recipient’s spam folder or other quarantined area where the message may be reviewed with suspicion.
- **Reject:** This requests that receivers reject any messages which fail DMARC and report on the action in DMARC data. Rejected messages will never be available to the recipient.

**Send Aggregate Data to:** The email address where DMARC aggregate data will be sent. Cisco's DMARC Builder sets Cisco's reporting address by default. You can specify another reporting address in addition to Cisco's address and both will appear in the DMARC record. DMARC receivers should send reporting data to both addresses.

**Send Forensic Data to:** The email address where DMARC forensic data will be sent. Cisco's DMARC Builder sets Cisco's reporting address by default. You can specify another reporting address in addition to Cisco's address and both will appear in the DMARC record. DMARC receivers should send reporting data to both addresses.

---

**Warning**

Forensic data is a real time flow of messages failing DMARC. Data volumes can be very high and very sporadic. Adding your own reporting address here may cause problems with your local mail server.

**Advanced Settings**

The record elements under “Advanced Settings” are optional and will default to the recommended settings.

**Note**

Cisco recommends that you do not change these settings initially.

A note about the Subdomain Policy: By default, a domain's DMARC policy applies to all of its sub-domains. The DMARC specification allows you to apply a different policy to sub-domains if you wish. Whatever sub-domain policy you specify will apply to ALL sub-domains. If you want a different policy for specific sub-domains, you can publish a DMARC record specifically for that sub-domain.

**Step 3**

Click “Continue.”

A DMARC record will be displayed similar to the following:
Figure 2-5    DMARC Builder Step 3

This DMARC record, for the domain “bar.com” defines the following parameters:

- **DNS record location** — The DNS text record must be installed for _dmarc.bar.com
- **v=DMARC** — This is version 1 of the DMARC specification
- **p=none** — The policy (p=) for this record is None, or a monitor only policy
- **ri=3600** — The reporting interval (ri=) should be 3600 seconds, or once per hour
- **rua=organization_name@rua.cisco.com** — The reporting user email address for aggregate information (rua=) should be sent to. This address is unique for your organization and is the mechanism by which Cisco receives data.
- **ruf=organization_name@ruf.cisco.com** — The reporting user email address for forensic information (ruf=) should be sent to. This address is unique for your organization and is the mechanism by which Cisco receives data.

**Step 4**  Click “Create Instructions” to download a text file (.txt) to use in the next step.

**Note**  Repeat the steps in this section for each domain you plan to protect in Cisco Domain Protection.

---

**2b: Publish the Record in DNS**

Now that you have a properly formatted DMARC record for your domain, you will need to update your DNS record for the domain.

The exact steps to get your DMARC record published will vary based on how the DNS for your domain is managed. However you submit requests for DNS changes, you will need to request that this DMARC record be published as a TXT resource record. The record must be published at the sub-domain created by prepending `_dmarc` as indicated in the DNS Record Location section listed in the previous step. Be sure to include the full DMARC record, including everything within the quotes (but not the quotes themselves). There should be no line-wraps, newlines, or whitespace other than the spaces explicitly shown within the record below.

**Note:**
**Step 3: Add Domains to the Portal**

If you published DMARC records with a `p=None` policy for all of the domains you are planning to protect with Cisco Domain Protection, you can skip this step! Those domains will be automatically added and verified by Cisco. If you have additional domains for which you haven’t published a `p=None` policy read on:

You must add domains to the portal; in Cisco Domain Protection, most activities are centered around the domain. Your organization may have a very large list of domains, or you may have a more manageable number of domains.

In either case, your activity in this step will be to let Cisco Domain Protection know which domains are associated with your organization.

Once you’ve gained access to the portal, the first page you see after authenticating is the Status > Protection page:

**Figure 2-6 The “Add Domains” Button on the Status > Protection Page**

**Step 1** Click the **Add Domains** button.
Step 2  In the dialog page, select an option for entering domains:

- **Basic:** Text Field: Enter a single domain or several domains (separated by commas) in the provided text field.
- **CSV upload:** Browse to a local text or comma-separated values file containing the list of domains.

**Advanced Topic: Domain Groups**

The Advanced section of this dialog allows you to specify a domain group and an Cisco distinction for each newly upload domains. See the following section for a discussion of Domain Groups.

Step 3  Click “Add your domains.” A dialog similar to the following will appear:

**What’s an Unverified Domain?**

You can specify policy and see data only for verified domains.

A Cisco representative takes an action to ensure that any domain uploaded into the system domain is ready to be managed, this “verifying” the domain. Cisco will periodically check all unverified domains to see if changes have occurred which allow them to be verified. You can resubmit a domain for verification to have it rechecked sooner.

The quickest method to have a domain verified is to publish a DMARC record for the domain, as described in the previous section. Cisco strongly recommends this method.

Publishing a DMARC record for a domain requires that you modify the DNS entry for the domain, which is another way of showing that you have you have authority over the domain. (By verifying every domain entered into the system, Cisco can ensure that no domains are mistakenly or inadvertently entered.)
Additional Options regarding DNS and Verification

Update the DNS name server record (NS record) for your domain so that it is something that Cisco can correlate to your organization. If the DNS for your domain is managed by an external DNS provider this may not be possible.

**Example:** You are trying to register `cat.com` in the Cisco system. If `dog.com` has already been approved by Cisco for your organization and the NS record for `cat.com` is `ns1.dog.com`, then Cisco can trust that you have authority over `cat.com` (because DNS for `cat.com` is controlled by a domain that we know is yours).

Update the DNS mail exchanger record (MX record) for your domain so that it is something that Cisco can correlate to your organization. This is not always possible; it depends on how email is hosted for your domain.

**Example:** You are trying to register `cat.com` in the Cisco system. If `dog.com` has already been approved by Cisco for your organization and the MX record for `cat.com` is `mail1.dog.com`, then Cisco will trust that you have authority over `cat.com` (because all mail sent to `cat.com` is directed to a domain that we know is yours).

**Step 3a: Organize your Domains into Groups**

Cisco Domain Protection allows you to group domains in an arbitrary fashion, and you can use those domain groups throughout the product. For example, you may have a set of domains which are owned by one organizational unit which should be considered together. Grouping domains by name allow users to find their grouped domains to work from more easily than having to work from one large list of domains. Domain groups are a powerful classification tool which can be useful as you gain proficiency with Cisco Domain Protection.

Manage your domains and domain groups through the Manage > Domains page:

**Figure 2-7 An Example Domain Groups Page**
On this page, you can review all of your active and defensive domains, create custom domain groups for categorization of your domains, and manage access to your users.

**System Domain Groups**
System domain groups are predefined common domain categories to provide quick access to help you better manage your domains. System domain groups are also dynamically populated. By default, eight (8) system level domain groups exist, and you can add additional custom groups. For example, the “Reject Policy” group will contain all domains in your organization with a DMARC reject policy. When Cisco discovers a DMARC reject policy for one of your domains, that domain will automatically become a part of the “Reject Policy” group. You do not need to do anything to add or remove domains from this group.

---

**Note**
A domain can belong to more than one unique group.

“**Active**” vs. “**Defensive**” domains: A domain will be considered “Active” unless “Mark as Defensive” is selected. A defensive domain is domain which does not have any mail flow associated with it.

**Third Party**: Domains administered by non-corporate entities such as partners or agents

**Custom Domain Groups**
Custom domain groups allow you to create groups of domains to better organize your workflow. For instance, in the example above, you may have one team who works on “Cards” domains and the other “Checking/Savings:” domains. Grouping domains allows the users to find their grouped domains more easily than having to work from one large list of domains. You can also restrict users from viewing other domains by when creating user accounts.

**To create a new Custom Domain Group:**
1. Click “Add New Domain Groups” from your Custom Domain Groups list.
2. Enter the name of your new domain group. Type “Return” to save the name.
3. Once created, select domains to add from an existing group.
4. Use the “Add to Domain Group” button to add selected domains to your new Custom Domain Group.

**Deleting a Custom Domain Group**
1. Hover over the Custom Domain Group that you no longer want to use.
2. Click on the trash can icon to remove the group.
3. Confirm that you wish for that group to be removed from Cisco.

Please note: once a Custom Domain Group is deleted, it cannot be recovered.
Monitoring

Steps in this chapter include:

- Monitor Traffic
- Identify Target Domains
- Identity and classify all Senders (Well-known and Custom)

Once you have successfully created and published a DMARC record for a domain, data will begin appearing within the Cisco Domain Protection portal.

You can now begin the process of monitoring email traffic, identifying domains to secure, and identifying and classifying all Senders.

Step 4: Monitor Traffic for a Period of Time

As DMARC reporting data (aggregate and forensic) begins to be sent into Cisco Domain Protection, you can begin the process of monitoring your traffic.

In most cases, Cisco recommends at least two weeks of data collection to obtain a meaningful data set.

With DMARC reporting data, you’ll be able to see which Senders are sending email on behalf of your domain, from which sending inventory (IP addresses), and whether those emails pass SPF and DKIM authentication checks.

But the first step is to monitor traffic for a period of time. The period of time varies with the size and complexity of your organization. For example, your organization may send receipts or order confirmation emails every single day, but it may also employ a third-party Sender to send a marketing campaign less often — while another department may a newsletter from a different third-party Sender sporadically. You should consider that some legitimate third party email newsletters, campaigns, or other types of events can occur on a monthly, quarterly, or even annual basis, and for that reason might not be captured within an initial two week window. Most companies don’t realize how complex their email ecosystem is until they begin getting aggregate data from DMARC reporting.

The point is: you want to monitor data for a period of time so that you are confident that you have collected all third-party senders on your behalf so that you can set up authentication for all potential Senders for a domain.

Get Started with Monitoring

Navigate to the Analyze > Email Traffic menu to familiarize yourself with the available reports in Cisco Domain Protection.
The Analyze Email Traffic pages provide a list of common questions to provide you with helpful views into your email ecosystem. Each view is a detailed report about your email ecosystem:

**Figure 3-1 Email Traffic Analyzer Reports**

You can adjust the filter options for every report to help you get to the information you need. This will allow you to find and fix problems quickly and get your email authentication configured properly.

- Click the “Modify Settings” button to see the available filter options for any report. For example, you can:
  - Filter each report for a single domain or domain group.
  - Increase or decrease the data range from the default value of 2 weeks. Cisco recommends increasing the date range — for example, 90 days — to see trends patterns in your sending. (For example, a newsletter sent quarterly.)
  - Change the granularity of message grouping (daily, weekly, or monthly)
  - Modify the Message Origin of certain reports; for example, in some views, it may make sense to include or exclude certain categories of messages.

**What’s My DMARC Trend Look Like?**

A great place to start monitoring data is with the default view: the “What’s My DMARC Trend Look Like?” report.

At this point, you may only have a few domains generating data into Cisco Domain Protection, and those domains may have no authentication whatsoever.

- Drill into to specific data by clicking any of the links in the DMARC Pass or DMARC Fail columns.
Clicking the link for a specific domain in this view yields a report or all IP addresses sending on behalf of that specific domain in the selected time-frame.

You can drill down even further by clicking the “DMARC Pass” link for any IP address listed in this table.

**Figure 3-2** The “What’s my DMARC Trend Look Like?” view for the ‘Active Domains’ Group

**What Legitimate Subdomains Don’t I Know About?**

Another useful view in the initial stages of monitoring is the “What legitimate subdomains don’t I know about?” view.

- In the “Things I Can Fix” section, click the link for “What Legitimate Subdomains don’t I know about?”

The results of this view may shed light on subdomains of your primary domain that may be being used to send email.
Figure 3-3 The “What Legitimate Subdomains Don’t I know about?” View

Legitimate subdomains in this report are only reported for approved domains.

Sharing or Subscribing to the Report
You can send the “What legitimate subdomains don’t I know about?” report to others or receive an emailed version of the report at a regular interval.

Click the “Share” or “Subscribe” buttons at the top of the view to share or subscribe to the report. (Keep in mind that all scheduled reports maintain their scope as defined in the “Modify Settings” button.) Cisco recommends subscribing to a weekly version of this report as you begin your monitoring.

Take some time to explore all views and drill-down capabilities in the Analyze > Email Traffic section.

Next Steps
Do not be overwhelmed by the extensive reporting capabilities and rich granularity of the data! At this point in the process, you are merely collecting information to inform your strategy for the next phases of the project:

- Identifying a target set of domains to begin with
- Identify sender messaging authentication requirements (SPF, DKIM) for the target set of domains
- Work with your messaging team to set authentication on your own mail infrastructure for the target set of domains
- Work with 3rd party senders and business units to set authentication for the target set of domains
- Modify DNS SPF and/or DKIM records for the target set of domains
- Observe and confirm settings
Step 5: Identify a Target Domain or Set of Domains

After spending a period of time monitoring the data in Cisco Domain Protection, you should begin to think about identifying a target set of domains to begin securing.

For example, some strategies could be:

- **Start with your primary domain, or your highest volume domains**
  Perhaps your primary domain — and not specific subdomains — is used for all email communications from your company; for example, and email with the address joe@foo.com is as likely to be used for daily corporate communication as it is to be used for receipts or order confirmations, newsletters, marketing campaigns, or messaging from your CRM system.
  If this is the case, tackling your primary domain first may be the most prudent.

- **Start with defensive domains, and then move to active domains**
  By definition, defensive domains should be sending no email, and so they are easier to lock down with stringent policies. (An unprotected defensive domain which isn’t locked down is exposed to potential abuse from spammers.) Using data in Cisco Domain Protection, you can catalog defensive domains and move quickly to a DMARC reject policy.
  After shoring up the policies for defensive domains, you can concentrate on those domains which are intended to send legitimate mail for your organization.

- **Start with business-critical or back-end system automation domains with consistent or uniform sending profiles**
  If, for example, your organization sends customer support mail from a single subdomain (e.g. If, for example) from a single third-party sender (e.g. Zendesk), it may be easier to implement authentication for this domain first.

- **Or, start with non-business-critical first**
  Conversely, if you do not want to disrupt the deliverability of business critical email, consider starting with domains that send marketing mail first, as it may be easier to identify a “cut-over” for sending authenticated email from these scheduled mailers.

Regardless of which strategy you choose, you should group domains using the Configure > Manage Domains view as described in Step 3a [HREF TBD].

Step 6: Identify and Classify Senders

Now that you have defined a strategy for implementing email authentication for a given set of domains, you can begin to identify and classify Senders for those domains (and for your organization as a whole).

The Senders Page

**Step 1**

Navigate to the Diagnostics > Senders page.

By default, Cisco Domain Protection will recognize well-known third party senders by their sending infrastructure.
Figure 3-4 The Diagnostics > Senders page (Well-known Senders)

For example, in this view, the organization has identified and approved Marketo, Acxiom, Taleo, and Epsilon as legitimate third-party senders.

If you navigate to this page and see no approved and unapproved senders, do not be alarmed — you may just not have had the appropriate authentication information published in DNS yet.

**How the Senders Page Works**

Cisco Domain Protection looks at DNS records for all of your organization’s registered domains to determine the IP addresses that are likely to send legitimate messages on behalf of your organization. On this page you can view the Well-known Senders that Cisco considers to be legitimate for your organization. You can also see the domains used to discover those IP addresses and specific DNS record source that we used to discover them.

If you do not see data in the Approved tab, click the Unapproved tab to see:

- Unapproved Well-known Senders
- Unapproved IP addresses

**Selecting a Specific Domain**

From the drop-down, select an individual domain to see the approve and unapproved Well-known Senders and IP addresses.
What is the point of the Senders page?

As data begins flowing to it, Cisco Domain Protection is aggregating information for your entire organization as well as on a per-domain basis. You can use the Senders page to help organize and track the Well-known and Customer senders for every domain in the system.

- Move legitimate third-party Well-known Senders from the Unapproved tab to the Approved tab by clicking “approve.” (Conversely, if you know your organization is not using a Well-known Sender, you can click ignore to move that Well-known Sender to a list of ignored Senders.)

- Group legitimate IP addressed into Custom Senders. It is impossible for Cisco to classify IP addresses used to send email which may be part of your organizations sending infrastructure. (For example, many larger organizations have dedicated mail exchange servers they own and manage to send outbound email.) If you recognize IP addressed in the Unapproved IP addresses section for a given domain, you can classify these IP addresses by adding them the to a Custom Sender, or choose not to work on them by adding them to the Ignored list.

Note

This act of authorizing senders within Cisco Domain Protection — moving them from Unapproved to Approve — will be the basis of (and reflected in) the SPF and DKIM policies you manage for your domains in the next chapter! You will work to authenticate all email from approved Senders for your domains, and your DMARC policies will instruct receivers on what to do with message which fail authentication.
Sender Policy Framework

Steps in this chapter include:

- Propose New SPF Record
- Publish New SPF Record
- Identify Internal Business Owners

The monitoring tools you learned about in Chapter 3, `Monitoring,' on page 1 will directly inform your work in this chapter; that is, you’ll use the monitoring results to identify third party senders for a domain and work to enable authentication methods (SPF and/or DKIM authentication) for those Senders.

Using Cisco Domain Protection, the insight into your mail flow helps you to enable SPF.

Sender Policy Framework (SPF)

The Sender Policy Framework, also known as SPF is published as RFC 7208: (See https://tools.ietf.org/html/rfc7208.)

The framework defines an authentication process that ties the “5321.from” address (also known as the Mail From, Envelope From or Return Path) to authorized sending IP addresses. This authorization is published in a TXT record in DNS.

Receivers can check SPF at the beginning of a SMTP transaction and compare the 5321.from domain to the connecting IP address to determine if the connecting IP is authorized to transmit mail for that domain.

By publishing an SPF record for a domain, you are asserting that email should only originate from IP addresses in the published record.

SPF Record Syntax

At its simplest, the SPF TXT record contains a version indicator, the allowed IP addresses for the domain, and an authorization type.

For example, in this simple SPF record:

```
For example, in this simple SPF record:
```

- v=spf1 is the version indicator,
- 198.51.1.137 is the allowed sending IP address (an IPv4 address), and
• **-all** is an authorization type that asserts that only the IP address 198.51.1.137 is authorized to send mail for the domain.

### Specifying IP Addresses

There are a few ways to define authorized IP addresses within an SPF record.

- You can specify a single IPv4 or IPv6 address by prepending qualifiers such as `ip4:191.51.1.137` or `ip6:7939:a348:460d:966f:a986:d0ba:1e9a:c67e`
- You can specify a range of IP addresses in CIDR format, for example `ip4:191.51.1.137/29`
- You can specify any IP that is also an A or MX record for the sending domain. For example “v=spf1 mx -all” authorizes any IP that is also a MX for the sending domain.
- Other SPF records can be included using the `include:` command; for instance, `include:_spf.google.com` includes Google’s SPF record.

**Note**

Some mechanisms and modifiers cause DNS queries at the time of evaluation, and some do not. The “include”, “a”, “mx”, “ptr”, and “exists” mechanisms and the “redirect” modifier require DNS queries. A single SPF record MUST limit the total number of lookups to **10 lookups** during SPF evaluation, to avoid unreasonable load on the DNS.

### Authorization Types

The end syntax of the SPF record allows you to publish different types of authorization methods.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Result</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pass</code></td>
<td>Mean</td>
<td>Allow all mail.</td>
</tr>
<tr>
<td><code>fail</code></td>
<td>All</td>
<td>Only allow mail that matches one of the parameters (for example, IPv4, IPv6, MX) in the record.</td>
</tr>
<tr>
<td><code>softfail</code></td>
<td>exam</td>
<td>Allow mail whether or not it matches the parameters in the record.</td>
</tr>
<tr>
<td><code>neutral</code></td>
<td>reco</td>
<td>No policy statement.</td>
</tr>
</tbody>
</table>

**What’s the difference between What and and?**

Before the DMARC standard existed and the SPF standard existed on its own, the softfail (‘softfail’) authorization was made available as a means to allow organizations to become comfortable with the idea of asserting their outbound IP space in the environment where receivers interpreted and acted on the authorization differently.

In practice with DMARC and Cisco Domain Protection, you can start with a neutral authorization (“neutral”) and move rather quickly to a softfail authorization (“softfail”) and ultimately to a fail authorization (“-all”) as you monitor data.

You can use the “What are my SPF Problems?” report to continuously monitor data as you modify SPF records for your domains.
SPF Alignment

In addition to simply asserting in an SPF record the list of IP addresses allowed to send on behalf of your domain, you’ll need to work with Senders to ensure that SPF is aligning properly.

Understanding alignment requires understanding the SMTP protocol to a small degree. For SPF, a domain is considered aligned when the domain portion of the RFC5321.MailFrom (also known as the MAIL FROM, Envelope From or Return Path) matches the From: address (also known as the Friendly From: address) displayed in the body (or DATA portion) of the email message.

Most of the time, the ‘Return-Path’ header is used to show the RFC5321.MailFrom domain and is typically not visible in most email clients.

An example SMTP conversation is shown below:

An example SMTP conversation is shown below:

An example SMTP conversation is shown below:

An example SMTP conversation is shown below:

An example SMTP conversation is shown below:

An example SMTP conversation is shown below:

An example SMTP conversation is shown below:

An example SMTP conversation is shown below:

An example SMTP conversation is shown below:

In the example above, line 4 is the RFC5321.MailFrom address, and line 12 is the Friendly From address (which is usually visible in the mail client). In this example, the domains portions are considered aligned for SPF purposes.
Step 7. Building and Proposing a New SPF Record

The process for proposing a new SPF record should be the same for all domains that you plan to protect.

---

**Step 1**
Use the Senders page in Cisco Domain Protection to identify Senders for a given domain.

**Step 2**
Find SPF instructions for that Sender and Publish an SPF record:

- Use the “Sender Profile” links for Well-known Senders in Cisco Domain Protection to learn if the vendor supports SPF.
- Use the data for Custom Senders to enumerate IP Addresses which you control.

**Step 3**
Work with the Senders (Well-known or Custom Senders) to ensure that SPF alignment is achieved.

- Monitor progress via the Senders page and the Analyze > Email Traffic pages.

**Step 4**
Update/modify your SPF record for the domain to account for all potential Senders.

---

**Note**
See also Using the EasySPF™ Analyzer for an SPF Record, page 4-12.

**Step 5**
When you are confident that you have accounted for all Senders for a domain in its SPF record, update the SPF record to use a **the SP policy**.

You will repeat each of the above steps for each domain you plan to protect.

---

Example: SPF for a Well-known Sender

**Step 1**
Navigate to the Diagnostics > Senders page and select one of your domains from the “Single domain:” menu to view the Senders for that domain.

If you use Google as your email provider (for example, you are a G Suite environment), you will find Google listed in the Senders:

![Google Sender Profile](image)

Note that the “SPF record” column indicates that no SPF record was found for the selected domain.
Step 2  Click the Sender Profile link for Google to view Cisco’s information about the Sender:

The Sender Profile page contains information on whether the Sender support aligned SPF and instructions for achieving it. (You can also see your SPF pass rate and whether other Cisco customers have been successful achieving SPF authentication with this Sender.)

Following the links in the Sender Profile page, you will learn that you are adding the following to your SPF record for the selected domain:

record for the selected

...will authorize Google’s IP addresses for that domain.

Your new SPF record can take up to 48 hours to go into effect, but it usually happens more quickly. Afterwards, you will notice the “SPF Record” indicator changes to show that you have included the Sender in the SPF record for your selected domain:
The “SPF Pass” column will show the messages from that Sender which pass SPF alignment for the domain.

(In the case of G Suite, you use G Suite’s Postmaster tools to add and verify the domain in order to achieve SPF alignment. See https://support.google.com/mail/answer/6227174 for more details.)

Step 3  Repeating the process, you may notice on the Senders page that your organization uses Zendesk for the selected domain:

Step 4  Click the Sender Profile link for Zendesk to view Cisco’s information about the Sender: Following the links in the Sender Profile page, you will learn that you adding the following to your SPF record for the selected domain:
Step 7. Building and Proposing a New SPF Record

...will authorize Zendesk’s IP addresses for that domain.

At this point, you proposed SPF record would include authorization for both Senders, Google and Zendesk:

Note: You add approved Senders to a single SPF record for a domain in order to authorize them. Do not create a separate SPF record for each Sender. Instead, increase the SPF record (but be aware of the 10 DNS mechanism lookup described above.)
Example: SPF for a Custom Sender

A Custom Sender appears in the lower half of the Senders page.

What are Custom Senders?

Custom Senders can be used to organize senders or servers that aren’t part of Cisco’s Well-known Senders. Perhaps your organization has an old mail gateway on-premises that sends outbound email for a legacy system. Cisco Domain Protection groups IP addresses which it cannot otherwise associate with a Well-known Sender into the “Unassigned” Custom Sender group, by default.

You can use Custom Senders as filters in various views and reports. For example, you could classify servers you own within your infrastructure as Custom sender.

To create a new custom sender:

Step 1  Navigate to the Configure > Manage Custom Senders page.
Step 2  Click “Add New Sender” on the left side under “Custom Senders”:
Step 3  Enter the name of your new Custom Sender and save. Once created, select IP addresses/Ranges to add from the “Unassigned” group.

For example, assume that you have grouped internal IP addresses in your infrastructure into a Customer Sender named “My Internal Senders:”

As with the Well-known Senders in above, the Custom Senders section of the page confirms that email traffic is being seen from this Custom Sender, and the SPF Record indicator notes that the Sender(s) are not yet represented in the SPF record for the domain.

Navigating to the Configure > Manage Custom Senders page, you can see the list of IP addresses defined for that custom sender.

To add the IP address to the SPF record, modify the SPF record to include the IPv4 or IPv6 address. For example:

e xample:he IP ad

(An RFC 1918 address is used here as an example.)

Your SPF record for the selected domain would now be modified to include Google, Zendesk, and the specific IP address from the “My Internal Senders” Custom Sender group:

s pecific IP address from the "My Internal Senders" Custom Sender group:e Goo

Note

It is possible to specify ranges of IP addresses in CIDR format.
There are other mechanisms for specifying addresses in an SPF record (for example “a”, “mx”, “exists”), but they are more advanced and beyond the scope of this document. (The “ptr” mechanism, for example, is discouraged from being used in the SPF RFC specification.) For more information on these mechanisms, refer to http://www.openspf.org/RFC_4408#mechanisms.

Don’t Forget about Alignment

Again, adding the IP addresses from Custom Senders doesn’t guarantee alignment will be achieved. You must work with the systems sending mail from that infrastructure to ensure that the RFC5321.MailFrom (also known as the MAIL FROM, Envelope From or Return Path) matches the From: address (also known as the Friendly From: address) displayed in the body (or DATA portion) of the email message.

**Using the “SPF Problems” Report**

Using this report, you can often identify domains and categories of issues to be addressed as you work through authentication and creating comprehensive SPF records for each Sender in a given domain.

**Step 1**

Navigate to the Analysis > Email Traffic > What are my SPF Problems to view the initial report.

**Figure 4-1 The Top Level of the SPF Problems Report**

Often, identifier misalignment is the largest issue.
Note that you can use the Modify Settings button in the upper left to narrow the scope or filter this report (for example, show only the SPF problems for a single domain for the last 2 weeks).

**Figure 4-2  The Modify Settings Window**

For example, you may want to increase the scope to look for messages “From All Sources.” Senders outside your Sender Inventory will appear on the “Unapproved” tab on the Diagnostics > Senders page. Examine the list of Senders in the lower portion of this report to understand issues. For example, you may notice that you have “Identifier Misalignment” issues with mail being sent from the Sender MailChimp for a selected domain:

**Figure 4-3  Identifier Misalignment Issues with MailChimp**

**Step 2**  Click the link for the messages sent from Sender MailChimp to drill into the details for that Sender:
The view shows that Messages sent from MailChimp are failing alignment (assuming you have added the IP addresses for the Sender MailChimp to your SPF record for the domain).

The Sender Profile page for MailChimp has specific notes about enabling authentication with SPF for both MailChimp and Mandrill, which is a MailChimp product that uses the same IP addresses but has a different configuration for SPF:
In this fashion, you can narrow categories of issues:

- by domain
- by Well-known Sender
- by Custom Sender

For each domain, you can use the Senders page and the “What are my SPF problems?” reporting view to arrive at a comprehensive list of Senders and their corresponding entries in an SPF record for each of your domains.

### Sharing or Subscribing to the Report

You can send the “What are my SPF Problems?” report to others or receive an emailed version of the report at a regular interval.

Click the “Share” or “Subscribe” buttons at the top of the view to share or subscribe to the report.

Keep in mind that all scheduled reports maintain their scope as defined in the “Modify Settings” button. For example, you may want to routinely send a narrowed version of the report (a single Sender for a single domain) to a business owner, while you received a wider scoped version of the report (all Senders for all domains) as you track your journey toward building comprehensive SPF records for your domains.

### Using the EasySPF™ Analyzer for an SPF Record

You can also use the recently-introduced EasySPF Analyzer to analyze and existing or create a brand new SPF record based on your approved Senders.

#### Step 1

Navigate to the Diagnostics > Senders page, and select a single domain to view the approved Senders for that domain.
Step 2  Select Modify SPF Record > EasySPF Analyzer to enter the EasySPF Analyzer view.

In the first step of the EasySPF Analyzer, review the existing SPF record. Take note of: the Senders identified within SPF Record, the number of IP addresses authorized, the number of DNS querying mechanisms, and any syntax errors in the existing record.

You can hover the SPF Record components to show more information and learn about the connection between mechanism components and the relationship with the Approved Senders for the domain you selected.

Step 3  Select Analyze with Data to modify the current SPF Record
Step 2 of the EasySPF Analyzer Options

In this view, you can:

- Click the Supporting Data link to review the messages sent for the domain from that Sender.
  Perhaps you have purchased a dedicated IP address from a third-party sender. You may want to narrow the definition for the Sender in your SPF record (in this case) to a smaller set of IP Addresses. You can review the number of IP addresses used to send messages from that sender in the supporting data view (and even drill down further).
  For each of the Well-known and Custom Senders for a domain, the Supporting Data link shows:
    - IP Address: Origin IP address of messages
Chapter 4: Sender Policy Framework

Using the EasySPF™ Analyzer for an SPF Record

- IP Addresses referenced by any include mechanism for a Sender
- PTR Name (Pointer Record): Host name of IP Address
- Sender Based Reputation Score (SBRS)
- Country: Geographic Location of IP address
- SPF Pass Rate %
- DMARC Pass Rate %
- DMARC Pass Volume
- Total Email Volume

- Click Include, Include Subset, or Exclude to modify the definition for each Sender represented in the domain’s SPF record.

As you made changes, additions and deletion are updated in the modified SPF record shown at the top of the page:

Figure 4-8 Changes to the SPF Record

v=spf1 -all include:bf1.com include:bigfootinteractive.com
ip4:172.22.125.10/32 ip4:67.228.245.98

The DNS Query mechanisms are also updated as you change from an include mechanism to an explicit IP address or range.

You can reset to the existing SPF Record (as currently found in DNS) at any time to remove any changes you’ve made.

Editing a specific subset of a Well-known Sender definition will “flatten” an include statement to a series of IP addresses.
• Select “Save” to remain on Step 2 and continue to modify the SPF Record, or elect “Save and Publish” to move onto Step 3 “Publish Updated Record.”

Note: If you save a modified record in progress, you can return to the modified view by clicking the link in the Analyze > Domains > Domain Detail page:

If you click the “Publish” button, Step 3 of the EasySPF Analyzer will present the modified SPF record to you.

You may need to review an “Unaligned Sender Warning” if you have included a mechanism for a Sender whom Cisco knows not to send aligned SPF email. In this case, you should visit the Sender Profile page for that Sender to determine if additional actions are needed to fully authenticate message from that Sender.
The lower portion of the page will contain the new SPF record and instructions for creating the SPF record in DNS. Click the “Print Instructions” button to create a printer-friendly version of the instructions.
Hosted SPF

You may want Cisco to host SPF records on your behalf. When you choose to host your SPF records at Cisco, you can speed up your authentication efforts by quickly and accurately publishing SPF records while you approve Senders without incurring manual DNS changes delays at your organization. Using Hosted SPF, you can confidently leverage Cisco Domain Protection’s Email Cloud Identity to authenticate email for a domain in just a few clicks.

To get started using Hosted SPF for a domain, start by:

**Step 1** Navigating to the Diagnostics > Senders page and selecting a single domain to view the approved Senders for that domain.

**Step 2** Select Modify SPF Record > Hosted SPF Record @ Cisco.

![Figure 4-13 The Host SPF Record @ Cisco Option](image)

A reminder informs you that Cisco will include all Approved Senders for the selected domain:

![Figure 4-14 Hosted SPF Record Reminder](image)

**Step 3** Click Continue to begin hosting the SPF Record for the domain.
You must take action for the SPF record to be used. You need to update your DNS to “point” to Cisco (redirect) for SPF evaluation.

After you select to host an SPF record with Cisco, the status is reflected in the Diagnostics > Domains pages:
Stopping Hosting at Cisco

To stop hosting an SPF Record which is hosted, simply select “Stop Hosting” from the Analyze > Senders page for the selected domain:

A warning will remind you of the steps you need to take to begin hosting the SPF record within your own DNS infrastructure:
Step 8 and 9: Publish SPF records and Identify Business Owners

Steps 9 and 10 in this process are iterative: you will likely publish and update SPF records for your domains as you work with the business owners in your organization and you gain confidence in the comprehensiveness of your domain records.

Similarly, as you gain more confidence, you will update your SPF records as you start with a neutral authorization (“auth”) and move to a softfail authorization (“* a”) to a fail authorization (“-all”) as you continue to monitor data.

What if my Sender doesn’t support SPF?

Some Senders may only support aligned SPF from a dedicated IP address. (For example, the Sender Marketo.)

In this case, to pass DMARC without the dedicated IP option you must use DKIM to sign your messages using an aligned DKIM signing domain.

Remember that the DMARC specification states that if one or both the SPF and DKIM checks succeed while still being aligned with the policy set by DMARC, then the check is considered successful; otherwise the DMARC check is set as failed.

See the next chapter for setting up aligned DKIM.

References

Here are a few additional references that can help you understand the process of enabling SPF authentication for your domains.

Google G Suite Administrator Help, “Authorize Senders with SPF:”
https://support.google.com/a/answer/33786
Microsoft Office365 Help, “Set up SPF in Office 365 to help prevent spoofing:”

OpenSPF:
http://www.openspf.org/

Wikipedia entry for SPF:

RFC 7208, “Sender Policy Framework:”

Word to the Wise blog, “Authenticating with SPF: -all or ~all”
https://wordtootherwise.com/2014/06/authenticating-spf/

Global Cyber Alliance, “Introduction to the Sender Policy Framework (SPF): A Closer Look”
https://www.youtube.com/watch?v=oEpU-iqBerI
DomainKeys Identified Mail

Steps in this chapter include:

- Enable DKIM Signing on Email Gateway
- Verify DKIM Working on Email Gateway
- Request DKIM Signing from Third-Party Owners
- Implement DKIM Keys for all Third-Party Senders
- Verify DKIM Working for all Third-Party Senders

The monitoring tools you learned about in Chapter 3, "Monitoring," on page 1 will directly inform your work in this chapter; that is, you'll use the monitoring results to identify third party senders for a domain and work to enable authentication methods (SPF and/or DKIM authentication) for those Senders.

Using Cisco Domain Protection, the insight into your mail flow helps you to enable DKIM.

DomainKeys Identified Mail (DKIM)

DomainKeys Identified Mail, also known as DKIM, is published as RFC 6376: (See https://tools.ietf.org/html/rfc6376.)

DKIM defines a standardized way for those who send email to digitally sign. This allows recipients to confirm with a high degree of assurance who the sender of the email really is, and whether or not the message was altered during transit. DKIM complements SPF by providing email senders with a way to digitally sign all outgoing email from their domain. DKIM is broadly supported by the world’s major email box providers, and is one of the two underlying authentication methods incorporated into DMARC.

DomainKeys Identified Mail (DKIM) permits a person, role, or organization that owns the signing domain to claim some responsibility for a message by associating the domain with the message. DKIM separates the question of the identity of the Signer of the message from the purported author of the message. Assertion of responsibility is validated through a cryptographic signature and by querying the Signer’s domain directly (in DNS) to retrieve the appropriate public key.

Overview: DKIM Involves Cryptography

Signing messages with DKIM involves creating a public key/private key pair.

- After you create the key pair, you publish the public key in DNS, and you use the private key to create a hash (or “sign”) portions of the message.
When receivers receive your DKIM signed message, they check they signature against your public key. If there is a match, the message is considered to PASS DKIM signing.

**DMARC Requires DKIM Identifier Alignment**

The DMARC specification extends the notion of DKIM PASS.

To pass DMARC-DKIM, the message:
- the message must be signed with a valid DKIM signature
  AND
- the signed content of the message must not have changed
  AND
- the DKIM signing domain must match the From domain as required by DMARC.

*Identifier Misalignment* is defined as messages passing DKIM checks for the DKIM signing domain, but the DKIM signing domain does not match the From domain as required by DMARC. This mismatch in domains causes a DMARC-DKIM failure.

**Steps 10-11: Enabling DKIM on your Gateway**

You'll need to repeat the following process for enabling DKIM for each of the email gateways you use for a given domain.

Email gateways in your own infrastructure often appear as Custom Senders on the Diagnostics > Senders page.

If you are hosting your own email gateways sending outbound mail, you will need to take these 4 steps to implement DKIM:

---

**Step 1: Determine Domains**

Determine all the domains that are allowed to send outbound mail from the email gateway. The Diagnostics > Domains page (and custom domain groups) can help you identify a comprehensive set of domains.

**Step 2: Create Key Pairs**

Next you'll use an tool to create the DKIM public / private key pairing and the policy record. The ‘public’ key is a key that you will placed in your public-facing DNS record along with the DKIM a ‘policy record’.

The ‘private’ key is a long key that is installed on the email gateway (MTA/Email sending systems). When you send an outgoing email, the outgoing email gateway adds the DKIM signature.

Several online tools are available to help you create the key pairs. Some of the available online tools for creating key pairs include:

- [https://port25.com/dkim-wizard/](https://port25.com/dkim-wizard/)
- [https://www.dnswatch.info/dkim/create-dns-record](https://www.dnswatch.info/dkim/create-dns-record)

Searching for “DKIM key generator” or “DKIM key wizard” will yield additional results.

**Step 3: Publish DNS Records with DKIM information**
Create DNS text records that include DKIM information for every domain that is used to send e-mail. These records will be inserted in your public facing DNS record for each sending domain. Note that you will be create

**Step 4** Enable DKIM Signing on the Gateway

The instructions for enabling DKIM signing will vary depending on your gateway. Here are some pointers to documentation for popular gateway models:

- Cisco Email Security Gateway

- Symantec

- Postfix
  https://petermolnar.net/howto-spf-dkim-dmarc-postfix/

---

**Steps 12-14 - Enabling DKIM for 3rd Party Senders**

- Request DKIM signing from Third-Party owners, page 5-3
- Implement DKIM keys for Third-Party Senders, page 5-4
- Verify DKIM for all Third-Party Senders, page 5-5

**Request DKIM signing from Third-Party owners**

You'll need to repeat the following process for enabling DKIM for each of the 3rd party senders you use for a given domain.

**Step 1** Go to the Diagnostics > Senders page.

Click the Sender Profile link of a sender in the Well-known Senders list to learn about that sender’s DKIM capabilities:
Steps 12-14 - Enabling DKIM for 3rd Party Senders

Figure 5-1  The Link to DKIM Instructions on a Sender Profile Page

Clicking the link for the DKIM Instructions redirects you to the instructions for enabling DKIM signing for messages Salesforce sends on behalf of your domain located at: https://help.salesforce.com/articleView?id=emailadmin_create_dkim_key.htm

Implement DKIM keys for Third-Party Senders

Reading the documentation for each Sender (as in the Salesforce example above), the process often involves:

- Generating a key pair
- Choosing a selector for a domain
- Publishing the public key in DNS

For DKIM keys, the specification defines that:

- The name of the TXT file is formed from the selector, followed by “_.”, then the domain key, followed by “.”, and then the domain name. For example:
  selector._domainkey.domain.com.

- The value in the TXT file is in the format v=DKIM1; k=rsa; p=MHww..., where the value after p= is the contents of the public key.

You’re now ready to move on to the next Approved, Well-known Sender for your selected domain. Repeat the above steps for the next Approved, Well-known Sender, updating your DNS TXT records accordingly.

Note

Many 3rd-party Senders enable DKIM signing by default. For example, Microsoft Office365 and Google G Suite enable DKIM signing for outgoing messages automatically.
Verify DKIM for all Third-Party Senders

You can verify that a DKIM record is published correctly in DNS by using Cisco Domain Protection (or even a publicly available tool, such as MX toolbox: https://mxtoolbox.com/dkim.aspx).

In Cisco Domain Protection, navigate to the Tools > DKIM menu and enter a domain name and selector. For example:

**Figure 5-2 Checking for a DKIM Record**

You can verify that a 3rd party is signing correctly by examining the headers of a received message. For example, in the Gmail client, choosing “Show Original” on a message will show the authentication results for SPF, DKIM, and DMARC.

This example message was sent from Salesforce.com from their sending infrastructure. Note that the Gmail client shows the authentication results of DKIM PASS:

**Original Message**

<table>
<thead>
<tr>
<th>Message ID</th>
<th><a href="mailto:6B86EFC2-0C5A-4A25-B5A6-72D23026912E@cisco.com">6B86EFC2-0C5A-4A25-B5A6-72D23026912E@cisco.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Created at</td>
<td>Tue, Jun 19, 2018 at 2:46 AM (Delivered after 6 seconds)</td>
</tr>
<tr>
<td>From:</td>
<td></td>
</tr>
<tr>
<td>To:</td>
<td></td>
</tr>
<tr>
<td>Subject:</td>
<td></td>
</tr>
<tr>
<td>SPF:</td>
<td>PASS with IP 173.37.142.88 Learn more</td>
</tr>
<tr>
<td>DKIM:</td>
<td>‘PASS’ with domain cisco.com Learn more</td>
</tr>
<tr>
<td>DMARC:</td>
<td>‘PASS’ Learn more</td>
</tr>
</tbody>
</table>
Examining the headers for the message, you can see that Salesforce inserted the proper DKIM headers:

```
DKIM-Signature: v=1; a=rws-sha256; c=relaxed/simple;
d=cisco.com; i=@cisco.com; l=5289592; q=dns;txt;
s=ip; t=1529401619; x=1530611219;
h=to:subject:domain:ids:in-reply-to:;
mime-version;
bh=wnGqr24eIbPG97Fe3sW9PspP7oMJuL1JpjdA0DKqzUx=
; b=Cr5VTd6UKVC84l3Qu4G/FwA3g0WTTezZNM4YYUpD/06uxRmllepYH9XF
 exxCsKmcntaV3H7CUXFblZ6sTwGnuntrzWh1U3p0UZFX8l2e8V0HleI
 bDnRq9C+gaVvtr723RmpnaJZCnna0BjYUC/Usb5Go+vZE+tAaYXX/0
```

d=cisco.com - The domain is cisco.com
s=s1024 - The selector is ‘s1024’
h=... - The headers used to determine the hash.
bh=... - The body hash of the message.
b=... - The actual digital signature of the contents of the message.


## DKIM Results Cisco Domain Protection

When DKIM signing has been enabled for a domain, you will see the results in the Senders page. In this example, the DKIM Pass column is updated to show the DKIM PASS results for the domains for messages sent from the Custom Sender A:

<table>
<thead>
<tr>
<th>Sender Name</th>
<th>Domains</th>
<th>Volume</th>
<th>SPF Pass</th>
<th>SPF Record</th>
<th>DKIM Pass</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>9 (total)</td>
<td>126,949</td>
<td>99%</td>
<td>–</td>
<td>99%</td>
</tr>
<tr>
<td></td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>113,995</td>
<td>99%</td>
<td>–</td>
<td>99%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10,576</td>
<td>99%</td>
<td>–</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1,162</td>
<td>100%</td>
<td>–</td>
<td>100%</td>
</tr>
</tbody>
</table>

Results are also shown for Well-known Senders; this example is showing the DKIM PASS results for email sent from the Sender Salesforce Marketing Cloud:
Clicking the link for any of the results of the DKIM Pass column will display the results of the “What are my DKIM Problems?” report, described in the following section.

**Using the “DKIM Problems” Report to Find Issues**

Using this report, you can often identify domains and categories of issues to be addressed as you work through authentication and creating achieving DKIM signing for each Sender in a given domain.

**Step 1**

Navigate to the Analysis > Email Traffic > What are my SPF Problems? to view the initial report.
Often, identifier misalignment is the largest issue after “No DKIM Signatures” (that is: messages were not DKIM signed at all). Note that you can use the Modify Settings button in the upper left to narrow the scope or filter this report (for example, show only the DKIM problems for a single domain for the last 2 weeks).
For example, you may want to increase the scope to look for messages “From All Sources.” Senders outside your Sender Inventory will appear on the “Unapproved” tab on the Diagnostics > Senders page. Examine the list of Senders in the lower portion of this report to understand issues. For example, you may notice that you have “Identifier Misalignment” and “No DKIM Signature” issues with mail being sent from the Sender Google for a selected domain:

**Figure 5-5  Identifier Misalignment Issues with Google**

<table>
<thead>
<tr>
<th>Sender</th>
<th>DKIM Issues</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>All Issues</strong></td>
<td>107,991</td>
</tr>
<tr>
<td>Google</td>
<td>Identifier Misalignment</td>
<td>106,858</td>
</tr>
<tr>
<td></td>
<td>No DKIM Signature</td>
<td>1,057</td>
</tr>
<tr>
<td></td>
<td>DKIM Fail</td>
<td>66</td>
</tr>
</tbody>
</table>

**Step 2** Click the links for the messages sent from Sender Google to drill into the details for that Sender:
Using the “DKIM Problems” Report to Find Issues

Chapter 5  Domain Keys Identified Mail

Figure 5-6  Google Misalignment Detail View

The view shows that Messages sent from Google are failing alignment. In fact, the majority of alignment failures are coming from a single IP address: 209.85.220.69, mail-sor-f69.google.com.

Step 3  Click the link for that IP address to drill into a deeper level of detail.

In this example, the majority of the failures (more than 50,000) are from a single domain which is misaligned with the DKIM key:
In this fashion, you can narrow categories of issues:

- No DKIM Signature (meaning: you need to implement DKIM signing for the Sender for the specific domain)
- Identifier Misalignment (meaning: you need to align the From: domain with the signing key which is being used for the specific domain).

For each domain, you can use the Senders page and the “What are my DKIM problems?” reporting view to methodically approach DKIM signing for all of Senders for each of your domains.

**Sharing or Subscribing to the Report**

You can send the “What are my DKIM Problems?” report to others or receive an emailed version of the report at a regular interval.

Click the “Share” or “Subscribe” buttons at the top of the view to share or subscribe to the report.

Keep in mind that all scheduled reports maintain their scope as defined in the “Modify Settings” button. For example, you may want to routinely send a narrowed version of the report (a single Sender for a single domain) to a business owner, while you received a wider scoped version of the report (all senders for all domains) as you track your journey toward building comprehensive SPF records for your domains.

**References**

Here are a few additional references that can help you understand the process of enabling DKIM signing for your domains.

Google G Suite Administrator Help, “About DKIM:”
https://support.google.com/a/answer/174124?hl=en

Microsoft Office365 Help, “Use DKIM to validate outbound email sent from your custom domain in Office365:”
OpenDKIM:
http://opendkim.org/

Wikipedia entry for DKIM:

RFC 6376, “DomainKeys Identified Mail (DKIM) Signatures”

Word to Wise blog, “A DKIM Primer Resurrected:”
https://wordtothewise.com/2016/04/a-dkim-primer-resurrected/

F-Zero, “How To Setup DKIM in 3 Steps - Set Up DNS & EMail:”
https://www.youtube.com/watch?v=q4SNXHhIIJw
Moving to Reject

Steps in this chapter include:

- Obtain sign-off from all business owners
- Move DMARC record(s) to Reject

Using DMARC for Enforcement

In the previous chapters, you learned the steps needed to authenticate email from your domains. As you iterate through each of the steps for each of your domains, you can use the tools and reports in Cisco Domain Protection to organize and track your progress.

Monitoring with Reports

You learned about some of the reports in the previous chapters. As you iterate through the steps, take some time to review all of the remaining reports available to you in the Analyze > Email Traffic views.
Each of these reports provides valuable insight from DMARC aggregate and forensic data, and they represent the power of the Cisco Domain Protection solution. Keep in mind that, for any report, you can edit the parameters in multiple ways using the “Modify Settings” button:
Figure 6-2  Modify Report Settings for all Email Traffic Analyzer Reports

Most reports have multiple, “drill-down” views that allow you to hone in on specific mail flows and areas to address.

**Report Interactivity**

**Note**

Many of the reports in the view have interactive chart options; that is, you can click on a section of bar graph for a time period to narrow results.

Most of the table columns in the report views are sort-able; click on a column header to sort the table by that column, or click again to inverse sort.

Similarly, you can filter the view by enabling and disabling portions of the graphs to show (i.e. click on the key at the top of a bar chart to enable or disable showing that section.)
Sharing and Scheduling

Finally, all report views are able to be shared or scheduled. Click the buttons at the top of the report view to share and/or schedule a report with the parameters you’ve selected in the “Modify Settings” button.

The reports are as follows:

THE BIG PICTURE

- What does my DMARC trend look like?
  This report shows the general trend for DMARC pass and fail for messages. As you increase authentication from all of your Senders for all of your domains, you can determine when you have a sufficient amount of email passing DMARC checks so that you can move to a Reject policy with confidence.

- What's happening to messages failing DMARC?
  Message which fail DMARC checks can have different actions taken on them, depending on a) your policy and b) the actions of the receiver. Use this view to examine failing messages and see how various large receivers (Google, Yahoo, AOL, Microsoft, etc.) are processing them. Drill into details to examine failing messages on a domain-by-domain basis.

- Which messages pass DMARC with SPF & DKIM?
Conversely, this view shows you the passing messages — passing DMARC, passing SPF, or passing both — on a domain-by-domain basis. You can use this view to drill into details and see how each domain doing with respect to authentication checks.

- Which ISPs do I send email to?

This pivoted view show the ISP breakdown of failure permutations: passed both DKIM and SPF, failed both, or passed one or the other.

- How much email using my domains is legitimate?

In yet another pivoted view, you can the see the legitimate and threat messages, in aggregate volume and on a domain-by-domain basis.

*Legitimate messages* include any messages which originated from IP addresses within your Sender Inventory (i.e. your approved Senders list), whether they passed or failed DMARC authentication. Also included are messages from outside of your Sender Inventory which passed DMARC authentication, such as auto-forwarded messages which preserve the original DKIM signature.

*Threat Messages* are those which failed DMARC Authentication and originated from outside of your IP space.

**THINGS I CAN FIX**

- What are my SPF problems?

- What are my DKIM problems?

As discussed in the previous chapters, you can use these reports to drill into details about SPF and DKIM authentication progress and problems for any domain. See Using the “SPF Problems” Report, page 4-9 and Using the “DKIM Problems” Report to Find Issues, page 5-7 for more details.

- Are any legitimate messages being rejected?

Use this report to determine if any false positives are being rejected at receivers due to your DMARC policy.

- What legitimate subdomains don't I know about?

Use this report to discover subdomains being used to send messages for your organization. See What Legitimate Subdomains Don’t I Know About?, page 3-3.

**WHO IS SPOOFING ME**

- How much spoofed email am I blocking?

As you implement a reject policy, you can see the benefit of your enforcement policies in this report view.

- What subdomains are being used to spoof me?

Like the subdomain report above, you can use this view to discover subdomains are not currently authorized by you to send email. Register the subdomains as defensive domains in Cisco Domain Protection to work towards a DMARC reject policy.

**Organizing Domains**

The Analyze > Domains page has a detailed view for each domain. Click a domain to see its status:
Domain Details shows you a summary of data and characteristics of a domain registered to your organization. You can also edit some characteristics and store notes about the domain.

**Is Third Party**
Is this domain used by a third party sender to send email on your behalf? The domain could be used exclusively by a third party or have a mix of third party traffic. If Cisco has automatically detected a third party sender the box will already be checked.

**Is Defensive**
A defensive domain is a domain that is registered but is not used to send any legitimate email. Cisco recommends that defensive domains be protected by a DMARC reject policy to prevent abuse. If Cisco has automatically detected that a domain is defensive, the box will already be checked. Defensive domains are added to the Defensive Domains system group.

**Domain Groups**
A list of the domain groups that this domain belongs to.
Domain Protection Policy
The Cisco private channel policy published for this domain. If the domain has a published DMARC record the Domain Protection Policy is automatically synchronized to be the same. If no DMARC policy is published a Domain Protection Policy can be set here.

Name Server (NS)
The server that hosts DNS records for the domain.

Progress State
A domain's progress state will help you keep track of domains you are currently working on, domains you have completed work on, and domains that need attention. You may set a domain to 'I Am Working On', 'Configuration Completed', or 'Ready To Start' by clicking the star next to the domain name.

Note
Use the progress state to affect the state of the Domain Progress Meter of your overall progress on the Status > Protection page:

Figure 6-5 The Domain Progress Meter

- Configuration Completed
  When a domain is fully protected and Cisco has detected no remaining issues, it will automatically be marked as 'Configuration Completed' by Cisco Domain Protection. You can also mark a domain as 'Configuration Completed' when there is no further work planned to protect it. If you manually mark a domain as 'Configuration Completed', you are acknowledging that the domain has open issues which you have no need or intention to resolve.

- I Am Working On
  Mark a domain 'I Am Working On' if you are working on resolving the issues with this domain in order to get it into a fully protected state. For example, you have submitted a DNS change request to update the SPF record or to change the DMARC policy to reject, and you are waiting for the changes to take effect.

- Ready To Start
  Most domains will begin in this state. There are actions Cisco recommends you take in order to fully protect the domain. You can move a domain back to the 'Ready To Start' state from 'I Am Working On' or 'Configuration Completed' by manually changing its progress state.
Steps 15 and 16: Enforce

Using the monitoring views above, hopefully you can become confident enough with your authentication that you can enforce a stricter policy for your domains.

Feel free to schedule a review with Cisco Customer Support if you need help interpreting the data prior to moving to a Reject policy.

Cisco recommends that you:

- Obtain sign-off from all business owners.
  
  Prior to enabling an enforcement policy, ensure that you have communicated with all internal business owners for a domain. As the reports mentioned above can show, you should be able to anticipate any deliverability problems from a single domain, Sender, ISP receiver, etc.

- Move DMARC records for your selected domains to Reject.
  
  The process for updating and publishing a policy is the same as the one you used in Step 2: Publish DMARC record(s) at Monitor, page 2-3; however, now that you have gained visibility you can set the policy to be Reject:

The modified policy will contain the `p=Reject` notation:
Congratulations!

Using this guide, you have successfully managed the steps to implement an enforcement (p=Reject) policy for a domain or set of domains in your organization.

Using DMARC, you can be confident that you have protected your brand from spoofing and instilled trust in your customers.
Monitoring for Changes

Steps in this chapter include:

- Review Alerts and Reports

Monitoring past Reject

Once you have enabled one or more domains with a Reject policy, you should begin to see the benefits of your authentication efforts.

For example, the “What’s my DMARC trend look like” for this Cisco Domain Protection customer shows that, after moving a domain to Reject policy, the spammers simply moved on and stopped attempting to spoof the domain:

Figure 7-1 The Benefits of Moving to Reject

Alerts

Cisco Domain Protection has defined alert subscriptions to which you can subscribe. Consider subscribing to pertinent alerts as you monitor the authentication of all domains you plan to protect.

Step 1 Get started by navigating to Status > Alerts and clicking “Manage My Subscriptions.”
Step 2  Click the “Manage Organization Alert Settings” to manage thresholds and exceptions for the various alert types.

The most recent Alerts are also presented in the Status > Protection overview page:
What's Next...

This Getting Started guide only covers the basics of implementing a DMARC policy for your organization.

Contact Cisco Support to learn more about some of the advanced features of Cisco Domain Protection, including:

**Brand Spoofing Detection**
Become alerted whenever specific brand-identifying strings appear in failed DMARC messages.

**Cousin Domains**
Explore similar look-alike domains to your own that customers may be using to exploit your brand.

**Threat Feed**
Learn how to use Cisco's Threat Feed in conjunction with your take-down vendor to quickly respond to malicious spoofing.

**API Access**
Access information in Cisco Domain Protection from an application programming interface (API) to work in conjunction with your other security tools.

**SSO Access**
Enable logging into Cisco Domain Protection from a single sign-on (SSO) capability.

**Inbound Insight ("Reflect")**
You can install additional software to gain DMARC visibility for messages sent into your organization.
What's Next...
User Accounts

Adding Users

Cisco Domain Protection enables Roles Based Access Control (RBAC), which allows you to assign each user one or more roles for access to Cisco Domain Protection functionality.

Add new users to the system by navigating to the Manage > Users page and clicking “Create new user.”

On the left side of the page, enter values for:

- **Full Name**
  The user’s full name for display, as shown in the list of users, at the top of each page while the user is logged in, and in the audit logs of activity.

- **Email**
  The user’s email address, which is used for the user’s login credentials as well as the destination address for reports and alerts. Note that this email address used for the invitation email with the initial activation token.

- **Default Dashboard**
Select the Dashboard that displays to the user upon login.

**Activate New Users**

Cisco sends each newly created user an email with an invitation, valid for 30 days, to activate their new Cisco account. If you have assigned alerts and reports, the new user will receive reports and alerts during this 30 day window even if they don’t activate their account. If the user is not activated within the 30 day window, all reports and alerts are stopped.

**User Roles**

There are two types of user roles:

- **Administrator Roles**—can make changes to settings in your organization.
- **Read-only Roles**—for receiving alerts and/or viewing data/information

You can assign a role individually or in conjunction with another role (i.e. Organization Admin with Log Auditor user permissions). There is no hierarchical inheritance of role privileges. Use caution in choosing roles; roles below the highest level role you choose for a user are automatically selected. You can de-select roles, but de-selecting certain combinations may cause odd UI behavior. Some examples of setting up users with roles are provided below.

**Administrator roles**

The following are the administrator roles available:

- **Organization Admin**
  
  Manage organization level settings. This includes setting password rules for your organization, setting session expiration times, setting the data collection policy, and setting restrictions on IP-based access control lists for the users reaching the Cisco Domain Protection web portal.

- **Domain Policy Admin**

  Manage domain level settings. This includes adding, editing, or deleting domains or Custom Domain Groups from your organization and editing the Sender Inventory for your organization.

- **Threat Admin**

  Manage threat level settings. This includes configuring your organization’s Threat Feed and editing your organization’s URI Whitelists.

- **User Admin**

  Manage users, including adding, editing, or deleting users in your organization.

When you create a User Admin, you must assign the types of roles this Admin can give to users (see Role usage examples below).

**Read-only roles**

Following are read-only roles available:

- **Log Auditor**
View audit logs for your organization and users in your organization.

- **Read Only**
  View data and schedule reports in the web portal.

- **Report Recipient**
  Receive scheduled reports and alerts.

---

**Note**

This role, assigned by itself, cannot view data directly in the portal. It can only receive emailed reports which are scheduled by other users, receive emailed alerts when subscribed by other users, and view the list of reports subscribed to from the UI.

To create an account to use in sending reports and/or notifications to a mailing list rather than a person, create and invite a user as normal, then in the Users list, click on the user’s name to edit that user, add a strong password, click Update, and your fictitious user is now activated and available for receiving reports.

---

**Domain-specific access**

By default, new users will be assigned access to All Domains.

You can limit user access to specific domains by assigning the user access to a Custom Domain Group:

- Click on the arrow next to Domain Access above the Invite New User button.
- View the available domains groups, and select one or more Custom Domain Groups from the list.

  The user you create will only be able to see domains that are part of these groups, in the portal and in reports, and will only receive alerts for this set of domains.

Users with domain-specific access can only see data related to the domain(s) to which they have access, so their view(s) when accessing Email Traffic analysis of “What does my DMARC trend look like?” will differ from the view(s) available to users with access to all domains.

---

**Role Usage Examples**

- Create a Read Only user who can receive emailed reports and alerts
  When you select the Read Only role for a user, the Report Recipient role will also be selected by default. In order to create a read only user who can also receive emailed reports and alerts, simply accept these defaults. If you choose to de-select the Report Recipient role, your read only user will not show up in the list of available users to send a report to or in the list of users who can be subscribed to alerts.

- Create a User Admin with Read Only access and who can create other Read Only users
  Select User Admin as the highest access role for the user. Since you want this User Admin to only be able to create and manage users with Read Only access and below, you would de-select the “All privileges” option in the “Manage Users” box directly below the User Admin role. Then select the “Read Only” and “Report Recipient” options. Now this user will be able to create and manage users with Read Only and below permissions.

- Create a User Admin who can only create other users
Create a User Admin for the sole purpose of creating or editing other users. This role cannot use the product to view data or receive reports and alerts.

Create a new user, then select the User Admin role for the user you are creating, and then de-select all of the roles that were automatically selected beneath User Admin. The User Admin you create is allowed to create other users with “All Privileges” unless you change the setting in the Manage Users box below the User Admin role.

If you would like this new User Admin to be able to create all roles except for Organization Admin and User Admin, select the ‘x’ remove “All Privileges.” Then, use the “Select Role Types” input to select each of the roles except for Organization Admin and User Admin.

- Create a user who can change domain settings, but can not create or edit users

Select the Domain Policy Admin role for the user you are creating. All roles beneath Domain Policy Admin will be selected by default. If you do not want this user to be able to create or edit other users, de-select the User Admin role.