



User Guide for Cisco Domain Protection

First Published: 03-03-2020

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.

Cisco, Inc.

170 West Tasman Dr.

San Jose, CA, 95134, USA

www.cisco.com

Updated: Tuesday, March 3, 2020

Copyright 2020, Cisco, Inc.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

ALL DATA IS PROVIDED “AS IS” AND CISCO, INC MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF ACCURACY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE, AND CISCO, INC WILL HAVE NO LIABILITY FOR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, LOST PROFITS, DATA OR BUSINESS, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES.

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.

Domain Protection™ is a trademark of Cisco, Inc.

All trademarks mentioned in this document or website are the property of their respective owners.

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.



Table of Contents

Preface	10
Terms of Service	10
Whats New in Domain Protection	11
About Domain Protection	13
Audience	14
The DIY Approach With As-Needed Help	14
About DMARC	14
History: The Need for DMARC	14
Who Endorses DMARC?	15
Government Agencies	16
Industry Associations	16
What is DMARC Enforcement?	17
DMARC Benefits	17
Inbound Benefits	17
What is BEC?	18
DMARC and Inbound Threats: A Partial Solution	18
DMARC Benefits: Before and After	18
How DMARC Works	19
What DMARC and Cisco Domain Protection Add	20
Hosted DNS Records	21
Putting DMARC Into Practice	21
Why Implementing DMARC is Challenging	22
Poor Visibility	22
Discovering & Authorizing 3rd Party Senders	22
The cost of “doing it wrong”	23

Specifying “Authentic” Email	23
What You’ll Be Doing	23
Moving toward a DMARC policy of “p=reject”	23
Before You Start	24
Ensure you have access to Domain Protection.	24
Gather a list of domains	24
Obtain the ability to make DNS changes	25
Compile a list of Stakeholders	25
References	25
Email Authentication Standards	26
SPF - Sender Policy Framework	26
SPF Record Syntax	27
Specifying IP Addresses	27
Authorization Types	27
What’s the difference between ~all and -all?	27
SPF Record Length	28
Additional Notes	28
Examples	28
SPF Alignment	29
SPF for a Well-Known Sender Examples	30
Google	30
SPF for a Custom Sender Example	32
To create a new custom sender	32
Don’t Forget about Alignment	33
Build and Propose a New SPF Record	33
References	34
Publish SPF Records and Identify Business Owners	35
What if my Sender doesn’t support SPF?	35
Identify SPF Problems	35
Hosted SPF	39
Host Your SPF Records at Cisco	39
Stop Hosting Your SPF Records at Cisco	42

Using the EasySPF™ Analyzer for an SPF Record	43
Review the Existing SPF Record	44
Analyze the Sender Data	44
Publish the Updated Record	47
DKIM - DomainKeys Identified Mail	48
Implement DKIM	49
DomainKeys Identified Mail	49
Overview: DKIM Involves Cryptography	49
DMARC Requires DKIM Identifier Alignment	49
Understanding Identifier Alignment	50
DKIM References	50
Request DKIM Signing From Third-Party Owners	51
Implement DKIM Keys for Third-Party Senders	52
Verify DKIM for All Third-Party Senders	53
Enable DKIM on Your Gateway	54
Step #1: Determine Domains	55
Step #2: Create Key Pairs	55
Step #3: Publish DNS Records with DKIM information	55
Step #4: Enable DKIM Signing on the Gateway	55
Host Your DKIM Records at Cisco	55
Verify That DKIM is Working	56
Find DKIM Problems	57
DKIM Problems Example	58
Sharing or Subscribing to the Report	60
EasyDKIM Analyzer	60
View DKIM Keys for a Domain in EasyDKIM Analyzer	60
Add a Domain DKIM Record for Domain Protection to Monitor	62
DMARC - Domain-based Message Authentication, Reporting, & Conformance ...	62
Publish DMARC record(s) at Monitor	63
Create a DMARC Record With DMARC Builder	63
DMARC example	64
Publish the DMARC Record in DNS	66

Congratulations!	66
Host Your DMARC Records at Cisco	66
Add Organization Domains for DMARC Policy Publication	68
What's an Unverified Domain?	68
Additional Options regarding DNS and Verification	69
DMARC Builder Settings	69
Implementing DMARC	72
The Overall Process	72
Get Credentials and Training	73
Contacting Support	74
Advanced Topics	74
Monitor Traffic and Senders	74
Monitor Your Traffic	75
Get Started with Monitoring	75
Next Steps	75
Identify a Target Domain or Set of Domains	76
Identify and Classify Senders	76
Senders	77
How the Senders Page Works	79
What is the point of the Senders page?	79
Approve a Sender for a Domain	79
Add a Sender to a Domain	80
Ignore a Sender for a Domain	81
Add an IP Address to a Custom Sender	81
Add an Unapproved IP Address to a Custom Sender	84
Ignore an Unapproved IP Address	84
Senders Filters	85
Nominate a Custom Sender to be a Well-Known Sender	85
Convert a Custom Sender to a Well-Known Sender	86
IP Address Overlap	87
Track All Senders	87

Move to Reject	88
Congratulations!	89
Review Your Email Traffic	89
Review Domain Status	89
Monitoring DMARC	93
What's Next...	94
Brand Indicators for Message Identification	95
BIMI Record Syntax	95
BIMI Implementation	97
Create a BIMI Record	97
Edit a BIMI Record	98
Preview Your Brand Mark Identifier	98
Host Your BIMI Records at Cisco	99
Stop Hosting Your BIMI Records at Cisco	99
Monitor Your Outgoing Messages	101
Email Traffic Reports	101
Available Reports	101
What Does My DMARC Trend Look Like?	102
What's happening to messages failing DMARC?	103
Which messages pass DMARC with SPF & DKIM?	103
Which ISPs do I send email to?	103
How much email using my domains is legitimate?	103
What are my SPF problems?, What are my DKIM problems?	104
Are any legitimate messages being rejected?	104
What Legitimate Subdomains Don't I Know About?	104
How much spoofed email am I blocking?	104
What subdomains are being used to spoof me?	105
Configure Email Traffic Reports	105
Share an Email Traffic Report	105
Schedule an Email Traffic Report	106
Email Traffic Report Settings	106

Threat Feed	108
Configure the Threat Feed	109
Whitelist a URL	109
View a Failure Sample	109
Share a Failure Sample	110
Threat Feed Settings	111
Alerts	113
Alert Types	113
View Alerts	114
Filter the Alerts List	114
Subscribe to Alerts	115
Unsubscribe to Alerts	115
Configure Alerts	116
Alert Configuration Options	116
Exception List	116
Threshold	116
Manage Organization Alert Subscriptions	117
Domain Groups	117
System Domain Groups	118
Custom Domain Groups	119
Add a Domain Group	119
Delete a Domain Group	119
Administration	120
Organization Settings	120
Audit Trail	123
View Organization Activity	123
Search Organization Activity	124
Query Keys	124
How Search Works	126
User Accounts	127
Create a User Account	127

Edit a User Account	127
Delete a User Account	127
View User Activity	128
User Account Settings	128
User Information	128
Roles	128
Domain Access	130
Role Examples	130
Create a Read Only user who can receive emailed reports and alerts	130
Create a User Admin with Read Only access and who can create other Read Only users	131
Create a User Admin who can only create other users	131
Create a user who can change domain settings, but can not create or edit users ..	131
Single Sign-On (SSO)	131
Enable Single Sign-On for Your Organization	132
Application Programming Interface	133
Generate API Credential	133
View API Documentation	133



Preface

Terms of Service

A Cisco Terms of Service (TOS) must be reviewed and accepted before anyone at your organization can use Domain Protection. The TOS is presented in one of two ways:

- For most organizations, the first person to log in to Domain Protection will be presented the TOS on first login. The TOS must be accepted during that first login.
- For organizations with a master sales agreement, the TOS is managed and accepted outside of the Domain Protection application by the Cisco sales team.



CHAPTER

1

Whats New in Domain Protection

Cisco is always working to improve the Domain Protection product, from fixing issues to improving existing features to adding new features. This section highlights the feature changes in Domain Protection, as well as documentation updates not necessarily related to product features.

Release	Date	Update Details
2020.02	February 2020	<p>This update includes the following improvements to the Domain Protection documentation:</p> <ul style="list-style-type: none"> • Corrections were made to the roles that can be assigned to users. One role was renamed, and a new role was added and documented. See "User Account Settings" on page 128. • The Domain Protection Threat Feed functionality is now documented. See. "Threat Feed" on page 108. • How you can search the Domain Protection audit trail is now documented. See "Search Organization Activity" on page 124.
2019.12	December 2019	<p>Product style sheets (CSS) incorporated some fixes as a part of an infrastructure upgrade, so dialog box title text now contrasts with the background and is easier to read. Screen shots in this document have been updated.</p>
2019.11	November 2019	<p>This November documentation release focuses on improving its content, including:</p> <ul style="list-style-type: none"> • Reorganized this guide. High-level sections now include subjects such as: <ul style="list-style-type: none"> • Email standards • Getting to reject (DMARC) • Monitoring your outgoing email ecosystem once your get to reject • Added a section on understanding identifier alignment. See "Understanding Identifier Alignment" on page 50. • Added a section on how to whitelist alerts. See Whitelist Alerts. • Added a section on SPF record length. See "SPF Record Length" on page 28. • Added information about the Threat Feed. See "Threat Feed" on page 108.
2019.10	October 2019	<ul style="list-style-type: none"> • Corrected the URL for Domain Protection.

Release	Date	Update Details
		<ul style="list-style-type: none"> Clarified that Cisco employees cannot make changes to Domain Protection user accounts. See "User Accounts" on page 127.
2019.04	April 2019	<ul style="list-style-type: none"> DKIM Management and Hosting <p>Cisco added the capability to host DKIM records. Domain Protection can now manage DKIM records hosted by Cisco. The DKIM management in Domain Protection can discover existing DKIM keys used for domains. Cisco can now host all DNS records relating to DMARC, SPF, and DKIM. Read more at "Host Your DKIM Records at Cisco" on page 55.</p>



CHAPTER 2

About Domain Protection

Cisco Domain Protection™ helps you protect the ownership of your brand by protecting your customers from phishers, spammers, and other email abusers who attempt to send inauthentic email claiming to be you. Domain Protection does this by helping you easily and thoroughly obtain outgoing email authentication. This authentication is for all your domains and for all who send messages from those domains, and it is authentication established by DMARC policies.

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) protocols to improve and monitor protection of domains from fraudulent email by:

- Adding linkage to the author ("From:") domain name
- Publishing policies for recipient handling of authentication failures
- Reporting from receivers to senders

This guide introduces you to DMARC and explains how to use Cisco Domain Protection to guide you through the process of implementing DMARC for your organization and to keep your DMARC status up-to-date. The topics covered here include:

- SPF, and building SPF DNS records for your domains. See "SPF - Sender Policy Framework" on page 26.
- DKIM, and building DKIM DNS records for your domains. See "DomainKeys Identified Mail" on page 49.
- DMARC, and building DMARC DNS records for your domains. See "Implementing DMARC" on page 72.
- Moving DMARC from monitor to reject. See "Move to Reject" on page 88.
- Hosting DNS records at Cisco.
- Ongoing monitoring of your domains, including changes in domains, senders, and IP addresses.
- Email traffic reporting. See "Email Traffic Reports" on page 101.
- Alerts, including alert subscriptions. See "Alerts" on page 113.
- Domain Protection administration, including user accounts and user roles.

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

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.

About 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. Policies can instruct that messages that are provably authentic to be directed to an inbox folder. Messages that are provably inauthentic 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.

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.

Who Endorses DMARC?

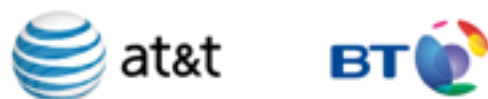
DMARC is endorsed by the world's largest senders, receivers, and industry consortia. More than 2.5 Billion Mailboxes Worldwide are DMARC-enabled.

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



Senders supporting DMARC

Some of the world's largest email Receivers supporting DMARC include the following:



Receivers supporting DMARC

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/>

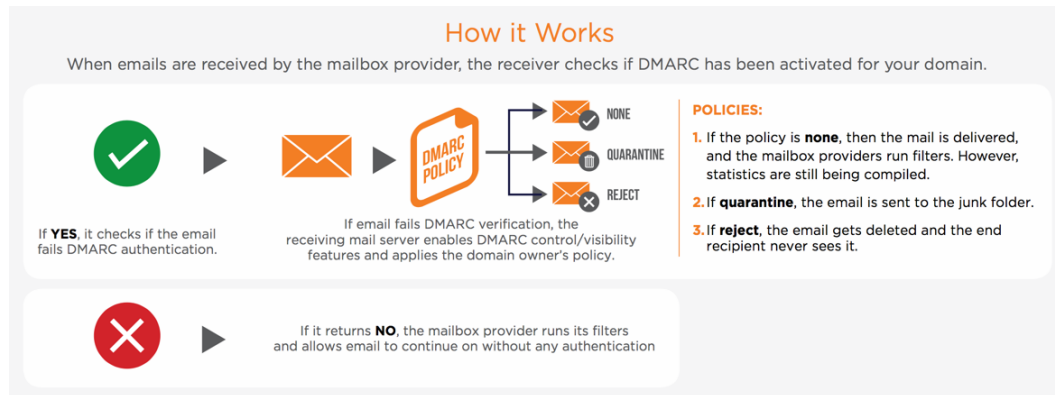
DMARC.org - <https://dmarc.org/>

FS-ISAC - Financial Services Information Sharing and Analysis Center
<https://www.fsisac.com/>

NH-ISAC - National Health Information Sharing and Analysis
<https://nhisac.org/>

What is DMARC Enforcement?

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.



How DMARC Works

DMARC Benefits

- 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.

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.

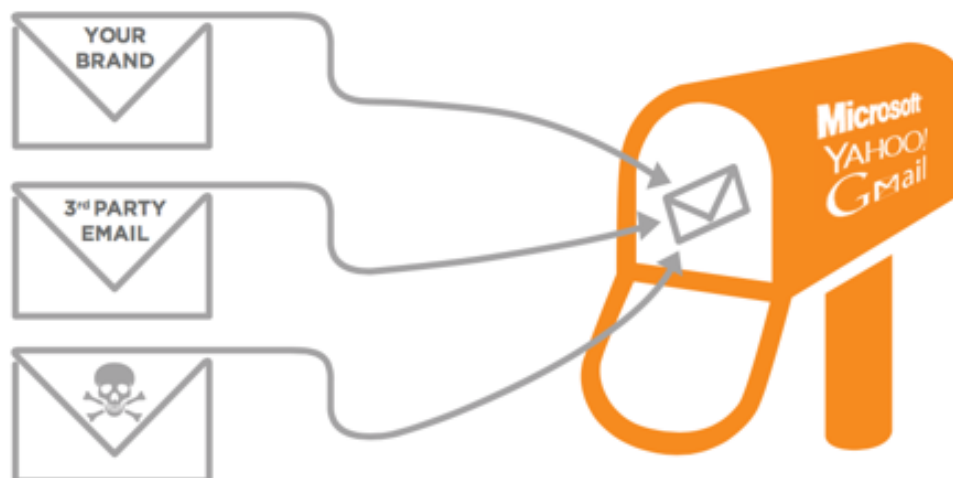
Inbound Threats Stopped by DMARC policies

Inbound Deception Technique Addressed by DMARC?	
Direct / Same Domain Spoofing	Yes
Display Name Spoofing	No
Look-alike Domain Spoofing	No

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.

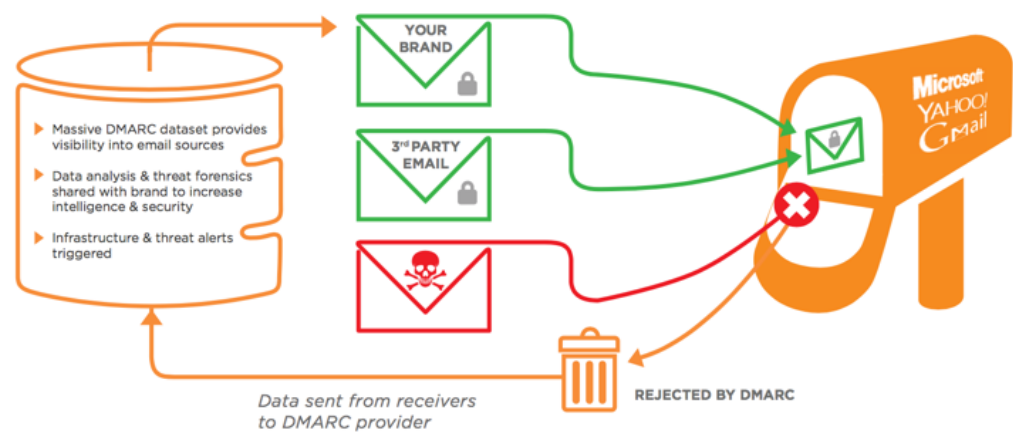
DMARC Benefits: Before and After

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



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:



After implementing DMARC

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 pre-pending “_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:

DMARC Policy Options

DMARC Policy Setting	Syntax	Action taken by Receivers
None (“Monitor”)	p=none	“p=none” 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 “monitor” 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,

DMARC Policy Setting	Syntax	Action taken by Receivers
		start by publishing a DMARC policy first because of its reporting capabilities.
Quarantine	p=quarantine	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.
Reject	p=reject	Do not accept messages that fail the DMARC checks.

- 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

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.

Domain Protection fills in the missing pieces between the protocols by

- Reporting its interpretation based on industry understanding of email ecosystems
- Providing visibility of actual sample email messages
- Guiding you through key steps in implementation

Hosted DNS Records

Cisco can host your DMARC, SPF, and DKIM records. Cisco-hosted DMARC, SPF, and DKIM records mean that changes that you make in Domain Protection get updated in DNS quickly, securely, and automatically.

Normally, when anything changes in your DMARC, SPF, and DKIM, you would have to update your own host records manually, one-by-one for each domain that has its records changed. This can be a lot of make-work, especially if you have a lot of domains. For example, with DMARC, the goal is to start with `p=none` (monitor), then move to quarantine, and finally get to reject. Imagine if you have a thousand domains that you manage (which you can do in Domain Protection; you are limited to 5 domains in Business Fraud Protection) and you have to change a thousand DNS records for each DMARC move.

Now imagine Cisco hosting your DMARC (and SPF and DKIM) records. You have that same thousand domains and you want to move them all from monitor to quarantine. In Domain Protection, you can make that change to the DMARC records of all those domains at once. And if Cisco is hosting your DMARC records, the change will be made to all thousand domains automatically (and quickly and securely).

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:

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>"`:

`"v=DMARC1; p=none; rua=mailto:dmarc-feedback@<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.

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.

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.

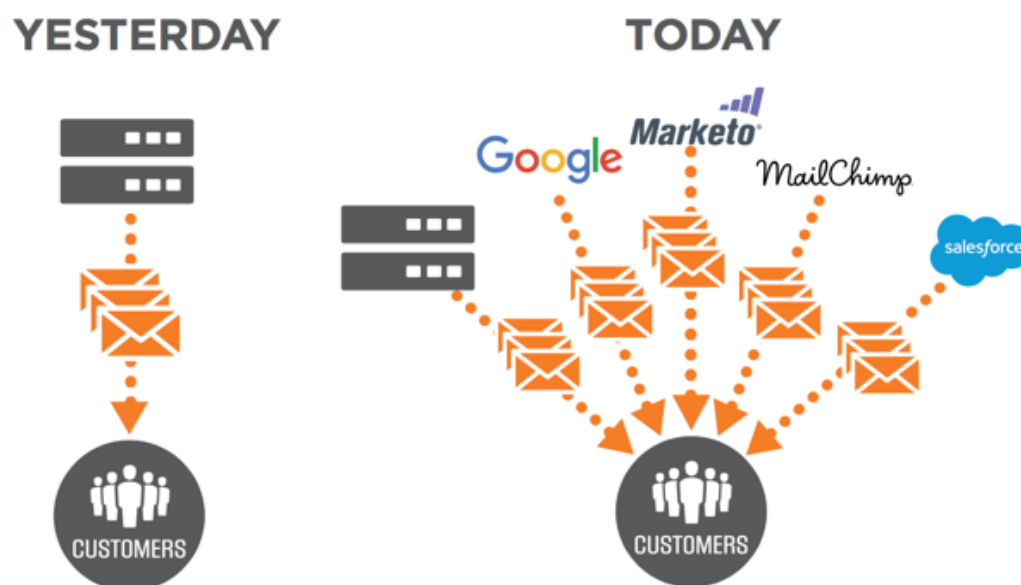
Why Implementing DMARC is Challenging

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.



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 "How DMARC Works" on page 19.

You start with a simple "monitoring-mode" record for a sub-domain or domain that requests DMARC receivers to 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 ("Build and Propose a New SPF Record" on page 33) and DKIM ("DomainKeys Identified Mail" on page 49), 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 Domain Protection, you will need to perform the following tasks:

Ensure you have access to Domain Protection.

Your Cisco representative should have provided access for at least one user account to Domain Protection, located at <https://dp.cisco.com>.

Contact Cisco support <https://www.cisco.com/c/en/us/support/all-products.html>.

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 "User Accounts" on page 127.

Gather a list of domains

You will need a list of domains and sub-domains that 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: coltrane.net), as well as any defensive or test domains that your organization owns and maintains (for example: blue.coltrane.net, col-

trane-soprano.net, coltrane-tenor.net, a-love-supreme.net, 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.

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 Domain Protection, to modifying your DMARC policies from monitor to reject.

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:

- A marketing team that sends email blasts to potential customers by using third-party software
- A support team that communicates with existing customers both directly and through support software
- A business continuity team tasked with sending order confirmations or receipts automatically 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

Here is a video reference that can help you understand the fundamental concepts in DMARC: Patrick Peterson, "DMARC Whiteboard Session"

<https://www.brighttalk.com/webcast/10593/104965/dmarc-whiteboard-session-for-engineers>



CHAPTER 3

Email Authentication Standards

Email authentications standards include SPF, DKIM, and DMARC.

- "SPF - Sender Policy Framework" below
- "DKIM - DomainKeys Identified Mail" on page 48
- "DMARC - Domain-based Message Authentication, Reporting, & Conformance" on page 62

SPF - Sender Policy Framework

SPF (Sender Policy Framework; IETF publication RFC 7208 dated April 2014, see <https://tools.ietf.org/html/rfc7208>) 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.

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

Example DNS Record for SPF

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.

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.

Details about SPF include:

- SPF record syntax
- SPF record length
- SPF alignment

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:

```
"v=spf1 ip4:198.51.1.137 -all"
```

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.

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.

SPF record authorization types

Statement	Result	Meaning
+all	pass	Allow all mail
-all	fail	Only allow mail that matches one of the parameters (for example, IPv4, IPv6, MX) in the record
~all	softfail	Allow mail whether or not it matches the parameters in the record
?all	neutral	No policy statement

What’s the difference between ~all and -all?

Before the DMARC standard existed and the SPF standard existed on its own, the 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 Domain Protection, you can start with a neutral authorization (“?all”) and move rather quickly to a softfail authorization (“~all”) 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 Record Length

SPF (Sender Policy Framework) is a DNS (Domain Name System) record, and the DNS specification limits DNS record strings to 255 characters. However, some environments are too complicated to fit into a 255 character string. You can create SPF records larger than 255 characters because the specification that defines SPF also states that DNS records can have multiple strings. See [RFC 4408](#) for the technical details.

Specifically:

As defined in [[RFC 1035](#)] sections [3.3.14](#) and [3.3](#), a single text DNS record (either TXT or SPF RR types) can be composed of more than one string. If a published record contains multiple strings, then the record **MUST** be treated as if those strings are concatenated together without adding spaces. For example:

IN TXT "v=spf1 first" "second string..."

MUST be treated as equivalent to

IN TXT "v=spf1 firstsecond string..."

If you attempt to create an SPF or TXT record with a single string greater than 255 characters, BIND, the DNS software, will generate an error, such as "Invalid rdata format: ran out of space."

Additional Notes

- Any DNS response that exceeds 512 bytes is slightly undesirable, because in the absence of EDNS0 (which the vast majority of—but not all—implementations honor these days), responses that exceed 512 bytes, the limit of a UDP packet, will signal truncation and prompt a retry via TCP. It is optimal to stay within a total of 512 bytes if possible.
- The RDATA itself, which is comprised of both the length-bytes and payloads of all strings contained therein, may not exceed 65535 bytes in total. That 64K limit is a general restriction on DNS records of all types, not specific to TXT records.

Examples

Here is an example of a single SPF record with 2 separate text strings:

```
"v=spf1 ip4:156.77.0.0/16 ip4:63.88.61.0/24 ip4:216.30.177.0/24 ip4:74.86.131.74
ip4:63.76.9.0/24 ip4:63.251.90.0/24 ip4:69.25.31.0/24 ip4:216.74.162.0/24 ip4:216.197.69.0/24
ip4:66.35.231.0/24 ip4:204.3.170.225/32 ip4:64.94.179.244/30 ip4:64.94.179.217
ip4:212.118.254.242/31 ip4:208.86.144.242 ip4:204.90.130.118 ip4:204.90.130.121" "
ip4:192.33.34.0/24 ip4:205.211.178.40/30 ip4:149.235.225.40/30 ip4:67.231.144.228
ip4:67.231.152.222 ip4:216.119.217.33 ip4:216.119.209.33 include:thirdparty.net -all"
```

Here is an example of a separate record for some of your traffic, useful for when your domain does not have many DNS lookups:

```
_spf.mydomain.com TXT v=spf1 ip4:156.77.0.0/16 ip4:63.88.61.0/24 ip4:216.30.177.0/24
ip4:74.86.131.74 ip4:63.76.9.0/24 ip4:63.251.90.0/24 ip4:69.25.31.0/24 ip4:216.74.162.0/24
ip4:216.197.69.0/24 ip4:66.35.231.0/24 ip4:204.3.170.225/32 ip4:64.94.179.244/30
ip4:64.94.179.217 -all
```

```
mydomain.com TXT v=spf1 ip4:212.118.254.242/31 ip4:208.86.144.242 ip4:204.90.130.118
ip4:204.90.130.121 ip4:192.33.34.0/24 ip4:205.211.178.40/30 ip4:149.235.225.40/30
ip4:67.231.144.228 ip4:67.231.152.222 ip4:216.119.217.33 ip4:216.119.209.33 include:third-
party.net -all
```

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:

```
1 S: 220 smtp.example.com ESMTP Postfix
2 C: HELO relay.example.com
3 S: 250 smtp.example.com, I am glad to meet you
4 C: MAIL FROM:<bob@example.com>
5 S: 250 Ok
6 C: RCPT TO:<alice@example.com>
7 S: 250 Ok
8 C: RCPT TO:<theboss@example.com>
9 S: 250 Ok
10 C: DATA
11 S: 354 End data with <CR><LF>.<CR><LF>
12 C: From: "Bob Example" <bob@example.com>
13 C: To: Alice Example <alice@example.com>
14 C: Cc: theboss@example.com
15 C: Date: Tue, 15 January 2008 16:02:43 -0500
16 C: Subject: Test message
```

17 C:
18 C: Hello Alice.
19 C: This is a test message with 5 header fields and 4 lines in the message body.
20 C: Your friend,
21 C: Bob
22 C: .
23 S: 250 Ok: queued as 12345
24 C: QUIT
25 S: 221 Bye

{The server closes the connection}

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.

SPF for a Well-Known Sender Examples

This example uses illustration from a system configured to demonstrate the concepts explained here. Your system may appear differently.

Google

- 1. Go to Diagnostics > Senders.
- 2. Select Single Domain, and then select one of your domains 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:

Well-known Senders

These Well-Known (to Cisco) Senders sent messages on your behalf. When there are multiple domains using a sender, you can view the per-domain breakdown by viewing details. Data shown are based on the top 100 IPs by volume; click the links for additional data where available.

Add Sender

Search:

Sender Name	Domains	Volume	SPF Pass	SPF Record	DKIM Pass	Source Type
<div>Google</div> <div><div>Sender Profile</div><div><div>SPF Alignment</div><div>DKIM Alignment</div></div></div>		2,270	0%		0%	Manual Remove

Note that the SPF Record column indicates that no SPF record was found for the selected domain.

- 3. Click the Sender Profile link for Marketo to view Cisco’s information about the sender:

Sender Profile: Marketo

Detailed information on specific well-known senders.



Definition

Use Cisco's definition ☐ Custom definition (advanced)

Web Site

<https://www.marketo.com>

Important Information

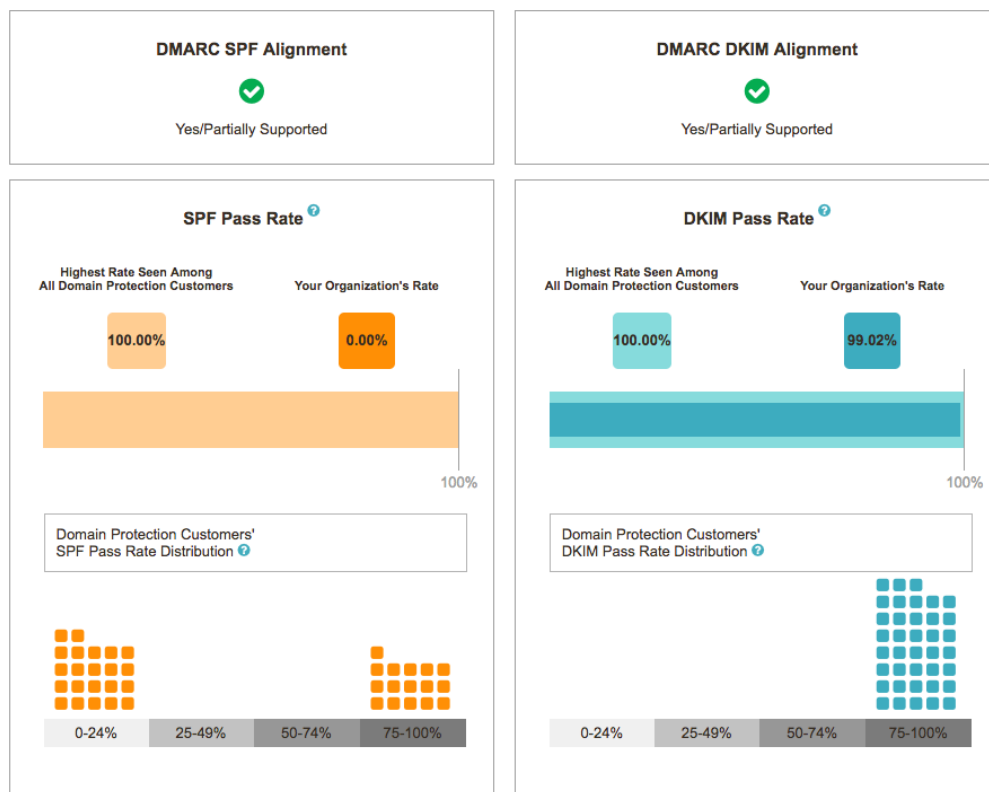
For SPF: Marketo supports aligned SPF provided that you use their dedicated IP option.

For DKIM: Marketo supports aligned DKIM for all customers regardless of whether you use a shared IP pool or their dedicated IP option. Our customer support would be happy to assist you with next steps.

NOTE: Marketo's SPF and DKIM support documentation is only available when logged in. Support tickets must be opened by named support contacts.

Contact Information

<https://login.marketo.com/homepage/community>




The Important Information section at the top of the Sender Profile page contains information on whether the sender supports aligned SPF, and if so, 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 when you add the following to your SPF record for the selected domain:

```
include:_spf.marketo.com
```

...it will authorize Marketo'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. Once it does, you will see the SPF Record indicator change to show that you have included the Sender in the SPF record for your selected domain:

SPF Pass	SPF Record
0%	

The SPF Pass column will show the percentage of messages from that sender the 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.)

You add approved senders to a single SPF record for a domain 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.)

SPF for a Custom Sender Example

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. Domain Protection groups IP addresses that it cannot otherwise associate with a well-known sender into the Unassigned Custom Sender group, by default, which appears in the lower half of the Senders page.

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

1. Go to Configure > Manage Custom Senders.
2. Click Add New Sender.
3. Enter the name of your new custom sender.
4. Press Enter.

Once created, add IP addresses/Ranges to to the custom sender 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:

Custom Senders

These senders are either not known to Cisco or are infrastructure within your organization. You can group and label IP addresses in the Unassigned sender group in the [Manage Custom Senders](#) page.

Add IP Address

Search:

Sender Name	Domains	Volume	SPF Pass	SPF Record	DKIM Pass	Source Type
My Internal Senders		234,525	0%		0%	DNS

As with the Well-known Senders in "SPF for a Well-Known Sender Examples" on page 30, 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:

```
ip4:192.168.1.67
```

(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:

```
v=spf1 include:_spf.google.com include:mail.zendesk.com ip4:192.168.1.67 ~all
```

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 https://en.wikipedia.org/wiki/Sender_Policy_Framework#Mechanisms.

Don't Forget about Alignment

Adding the IP addresses from custom senders to a domain 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.

Build and Propose a New SPF Record

The process for proposing a new SPF record should be the same for all domains that you plan to protect. At a high level, the process is as follows:

1. Use the Senders page in Domain Protection to identify senders for a given domain
2. Find SPF instructions for that sender and publish an SPF record:
 - View the sender profiles for well-known senders in Domain Protection to learn if the vendor supports SPF.
 - Use the data for custom senders to enumerate IP Addresses which you control.
3. Work with the senders (well-known or custom) to ensure that SPF alignment is achieved.
 - Monitor progress via the Senders page and the Analyze > Email Traffic pages.
4. Update/modify your SPF record for the domain to account for all potential senders.
 - You can also use the "Using the EasySPF™ Analyzer for an SPF Record" on page 43.
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 "-all" policy.

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

Some examples to illustrate the process:

- "SPF for a Well-Known Sender Examples" on page 30
- "SPF for a Custom Sender Example" on page 32

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 Office 365 Help, "Set up SPF in Office 365 to help prevent spoofing:"

[https://technet.microsoft.com/en-us/library/dn789058\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dn789058(v=exchg.150).aspx)

Wikipedia entry for SPF:

https://en.wikipedia.org/wiki/Sender_Policy_Framework

RFC 7208, "Sender Policy Framework:"

<https://tools.ietf.org/html/rfc7208>

Word to the Wise blog, "Authenticating with SPF: -all or ~all"

<https://wordtothewise.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>

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 (“?all”) and move to a softfail authorization (“~all”) 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.

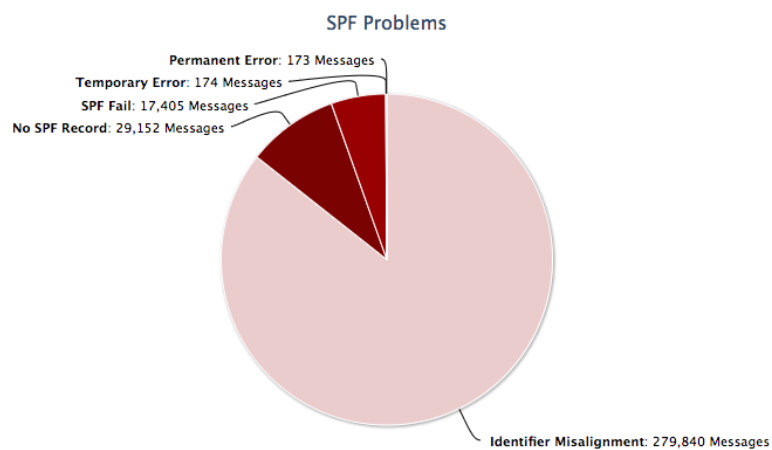
Remember that the DMARC specification states that if one or both the SPF and DKIM checks succeed while still being aligned with the policy set by DMARC, then the check is considered successful; otherwise the DMARC check is set as failed.

Identify SPF Problems

Using What are my SPF problems? report (go to Analyze > Email Traffic, then click What are my SPF problems?), 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.

What are my SPF problems?

Aetna Inc. **SPF Problems Report for Active Domains** using **Outbound Data** from March 12 to March 25, 2018

[Share](#)[Schedule](#)

Hover over a chart section for an explanation of the corresponding problem or click on a section to investigate further.

SPF Problems

Domains: 'Active Domains' Group
Message Sources: Only messages from my Sender Inventory
Date: 14 days starting on 2018-03-12
Displaying results based on the top 1,000 IPs
[Search for Failure Samples on 2018-03-25](#)

The top level of the SPF Problems report

Often, identifier misalignment is the largest issue.

Note that you can configure these reports to narrow their scope. (See "Configure Email Traffic Reports" on page 105 for details.) For example, you could show only the SPF problems for a single domain for the last 2 weeks like this:

Modify Report Settings

Select Domains

Domain Group: ☒ Active Domains

Single Domain: ☐ agari.com

View Messages From

Most Recent: ☒ 14 day(s)

Date Range: ☐ 2018-03-12 to 2018-03-25

Message Origin

Custom ☒ Default

Specific Sources: ☒ From All Sources

Known Forwarders: ☐ From Inside My Sender Inventory

Specific IP/CIDR Range: ☐ From Outside My Sender Inventory

Submit Reset to Defaults Cancel

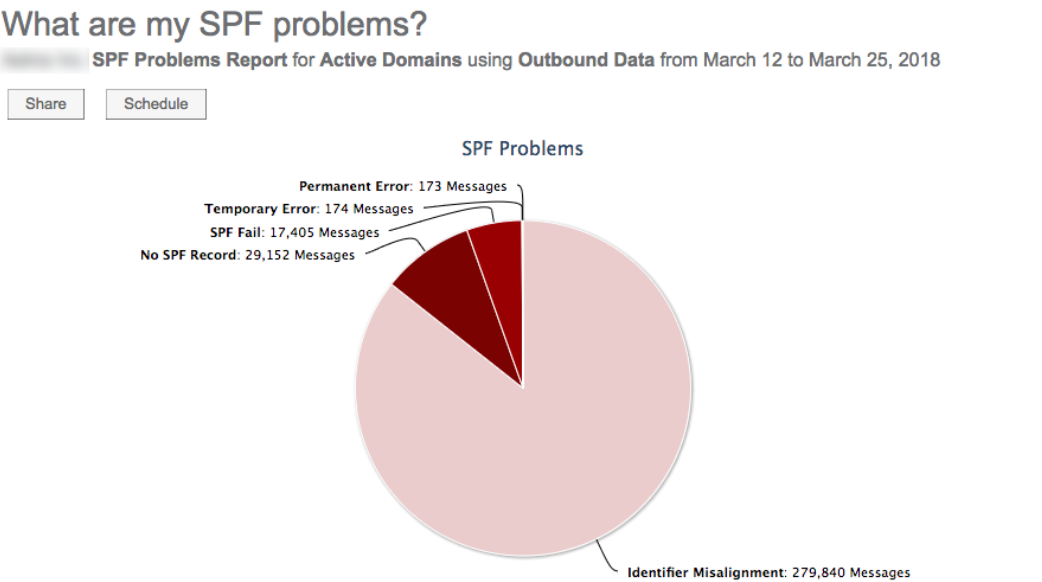
By increasing the scope to look for messages from all sources, senders outside your sender inventory will appear on the Unapproved tab on the Diagnostics > Senders page.

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, like this:

MailChimp	All Issues	1,546
	Identifier Misalignment	1,546

Identifier Misalignment issues with MailChimp

Click the link for the messages sent from sender MailChimp to drill into the details for that Sender:



Identifier Misalignment: These messages passed SPF check for the domain issued in the the SMTP MAIL FROM comm but the MAIL FROM domain does not match the domain seen in the From: header, which is required by DMARC. This mismatch in domains causes a DMARC-SPF failure. In the table below, click a number in the "Total" column to see the misaligned domain combinations.

Identifier Misalignment

Domains: 'Active Domains' Group
Message Sources: Only messages from MailChimp
Date: 14 days starting on 2018-03-12
Displaying all 8 results
[Search for Failure Samples on 2018-03-25](#)

Search within table:

IP	PTR Name	SBRS	Country	SPF Issue	Total
198.2.136.19	mail136-19.atl41.mandrillapp.com	3.5	United States	Identifier Misalignment	398
198.2.135.12	mail135-12.atl141.mandrillapp.com	3.5	United States	Identifier Misalignment	387
198.2.133.17	mail133-17.atl131.mandrillapp.com	3.4	United States	Identifier Misalignment	385
198.2.180.19	mail180-19.suw31.mandrillapp.com	3.5	United States	Identifier Misalignment	376
198.2.128.13	mail128-13.atl41.mandrillapp.com	3.5	United States	Identifier Misalignment	4
198.2.133.28	mail133-28.atl131.mandrillapp.com	3.5	United States	Identifier Misalignment	2
198.2.180.15	mail180-15.suw31.mandrillapp.com	2.3	United States	Identifier Misalignment	1
198.2.134.14	mail134-14.atl141.mandrillapp.com	3.5	United States	Identifier Misalignment	1
Total					1,554

MailChimp Misalignment Issues: Detail View

The view shows that Messages sent from MailChimp are failing alignment (presuming 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:

Sender Profile: MailChimp

Detailed information on specific well-known senders.



Web Site

www.mailchimp.com

Important Information

MailChimp: Set Up Custom Domain Authentication: DKIM and SPF: <http://kb.mailchimp.com/accounts/email-authentication/set-up-custom-domain-authentication-dkim-and-spf>

IMPORTANT NOTE: To pass DMARC with MailChimp you must implement DKIM per the instructions above. MailChimp does not support custom MailFrom domains so you cannot pass the DMARC-SPF alignment check.

Note that Mandrill is a MailChimp product and uses the same IPs, but has different configurations. If you are using Mandrill rather than MailChimp, follow these instructions instead: <https://mandrill.zendesk.com/hc/en-us/articles/205582267-About-SPF-and-DKIM>

NOTE: The Mandrill service does allow you to set the MailFrom domain to your own domain and you can pass DMARC-SPF alignment using Mandrill.

The SPF include mechanism for MailChimp is "include:servers.mcsv.net".

The SPF include mechanism for Mandrill is "spf.mandrillapp.com".

Contact Information

<https://mailchimp.com/contact/support/>

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.

Hosted SPF

Cisco can 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's Email Cloud Identity to authenticate email for a domain in just a few clicks.

You can:

- "Host Your SPF Records at Cisco" below
- "Stop Hosting Your SPF Records at Cisco" on page 42

Host Your SPF Records at Cisco

1. Go to Diagnostics > Senders.
2. Select a single domain to view the approved senders for that domain. If the SPF record for the domain is not already hosted at Cisco, the button to the right will read Modify SPF Record. If the SPF record for the domain is already hosted at Cisco, the button to the right will read Stop Hosting, and you will not be able to continue.
3. Click Modify SPF Record > Hosted SPF Record @ Cisco.

Senders

Discover which senders are authenticating email sent on behalf of your domains.

☐ All Domains
☒ Single Domain

☒ Most Recent: day(s) ☐ Date Range: to

[Modify SPF Record](#)

[EasySPF Analyzer](#)
[Host SPF Record @ Cisco](#)

Approved Unapproved

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

Host SPF Record @ Cisco

Reminder

An SPF Record hosted at Cisco will automatically include all Approved Senders for the selected domain.

Ensure that the list of Approved Senders is correct for the domain

[Continue](#) [Cancel](#)

4. Click Continue to begin hosting the SPF Record for the domain.

You will see a screen of instructions to follow to complete the process.

Hosted SPF Instructions

Host SPF Record @ Cisco

Host an SPF record for a specific domain at Cisco.

New SPF Record for:



Update DNS Record:

```
v=spf1 include:%{d}.fc.spf-protect.dmp-stage.cisco.com exists:%{i}._i.%{d}._d.espf.dmp-stage.cisco.com -all
```

Cisco has updated our systems and is ready to start processing SPF lookups on behalf of pwm.ciscofunds.com. The record will show as pending hosting on Diagnostics > Domains until you have updated the DNS entry for the domain, DNS has propagated, and our systems have identified the new record which can take up to 36 hours.

To complete the process, you must take action for this SPF record to be used:

Hosted SPF Record at Cisco: DNS Update Instructions

You must update (or create) the DNS for the domain [\[domain\]](#) to "point" to Cisco (redirect) for SPF evaluation. The exact steps to edit or create your SPF hosted 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 SPF record be published as a [TXT resource record for the domain pwm.ciscofunds.com](#). Be sure to include the full SPF record below. There should be no line-wraps, newlines, or whitespace other than the spaces explicitly shown within the record below.

- If you have direct access to manage DNS for your domain through an online DNS administration tool, look for a section to publish a TXT record or a section specific to SPF records.
- If you have access to manage DNS for your domain through a web hosting online administrative interface, look for DNS Settings and a place to enter a TXT record or an SPF record.
- If your company manages its DNS internally you may need to submit a request to publish the DNS record through your company's DNS management team.
- If a third party hosts DNS for your domain, you may need to submit a ticket with them to update the domain's DNS settings.

Domain: [\[domain\]](#)

```
v=spf1 include:%{d}.fc.spf-protect.dmp-stage.cisco.com exists:%{i}._i.%{d}._d.espf.dmp-stage.cisco.com -all
```

It may take up to 36 hours for the changes to appear within Domain Protection after the record is published by your DNS provider.

[Print instructions](#)

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:

e 6 to June 20, 2019
Filter Results

Approved Senders		Unapproved Senders		DMARC Policy	BIMI Record	SPF		DKIM	
#	Pass	#	Pass			Record	Pass	Key	Pass
0		0		[]					
0		0		[]					
97,347	100%	0		[]			100%		0%
0		0		[]					
27.49M	100%	3.5M	100%	[]			96.24%		98.64%
17.47M	99.54%	3.39M	4.03%	[]			54.03%		97.53%
1.09M	100%	7,794	100%	[]			96.31%		98.75%
216,023	99.02%	81,216	99.17%	[]			100%		0%
0		0		[]					
1.47M	100%	23,573	100%	[]			97.27%		98.67%
3.56M	99.12%	23,302	100%	[]			10.72%		88.4%
0		0		[]					

Previous
1
Next

Domains Per Page: 25

DMARC Policy

- No Record
- Monitor
- Quarantine
- Reject
- Inherited
- Hosted by Cisco

DNS Record

- Error
- Record Published
- No Record, Messages Pass
- Saved SPF Analyzer Record
- No Record
- Hosted by Cisco
- Hosting Pending DNS Update

Progress State

- Configuration Completed
- I Am Working On
- Ready To Start

Hosting Pending DNS Update

Stop Hosting Your SPF Records at Cisco

1. Go to Diagnostics > Senders.
2. Select a single domain to view the approved senders for that domain. If the SPF record for the domain is hosted at Cisco, the button to the right will read Stop Hosting. If the SPF record for the domain is not already hosted at Cisco, the button to the right will read Modify SPF Record, and you will not be able to continue.
3. Click Stop Hosting.

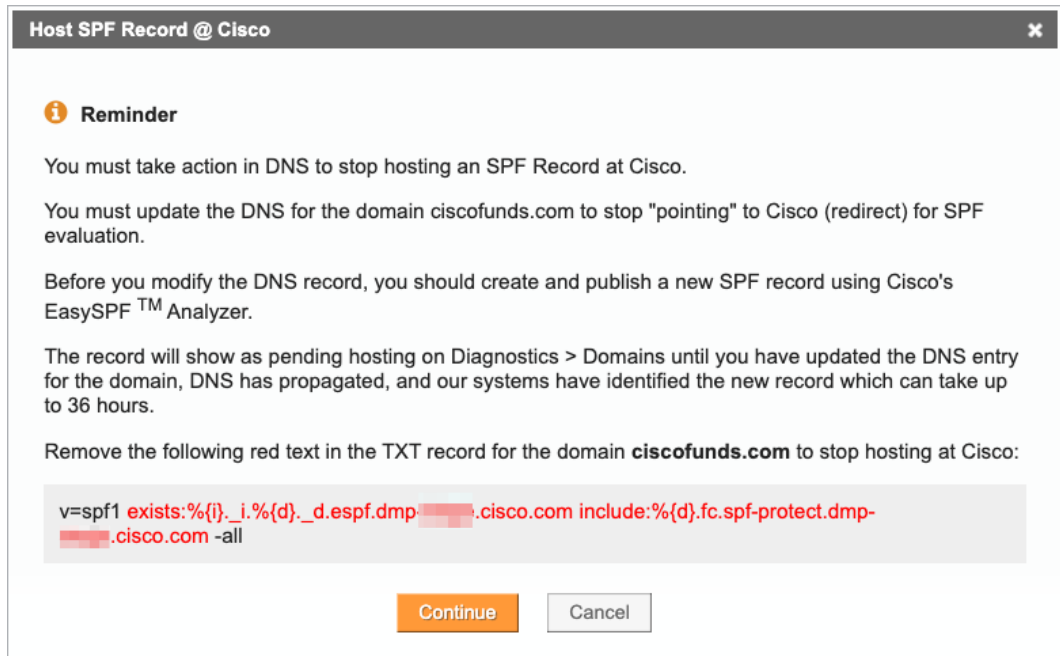
Senders

Discover which senders are authenticating email sent on behalf of your domains.

☐ All Domains
☒ Single Domain

Stop Hosting

A warning will remind you of the steps you need to take to begin hosting the SPF record within your own DNS infrastructure:



Stopping Hosting SPF Records at Cisco

4. Click Continue.

Using the EasySPF™ Analyzer for an SPF Record

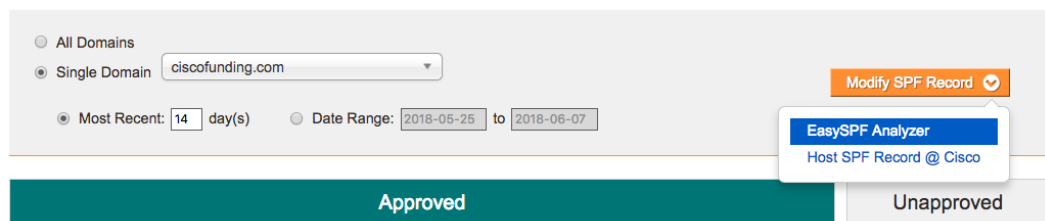
If you host your own SPF records, you can use EasySPF™ Analyzer to analyze an existing SPF record or to create a brand new SPF record based on your approved senders.

You can use EasySPF Analyzer only for domains that are not hosted by Cisco.

1. Go to Diagnostics > Senders.
2. Select a single domain.
3. Click Modify SPF Record > EasySPF Analyzer.

Senders

Discover which senders are authenticating email sent on behalf of your domains.



The EasySPF Analyzer has 3 steps that you will take to create or modify an SPF record:

1. Review the existing SFP record (if any)
2. Analyze the sender data
3. Publish the updated record

Review the Existing SPF Record

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
- 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.

EasySPF™ Analyzer

Use this tool to analyze and update the SPF record for a specific domain.

1 Review Existing SPF Record

2 Analyze With Data

3 Publish Updated Record

Domain to analyze:

agaribank.com

v=spf1 mx ip4:172.22.125.10/32 include:bfi0.com include:bigfootinteractive.com -all

DNS Querying mechanisms (10 maximum):

3

Syntax errors:

✔ No errors

IP addresses authorized:

IPv4: 4,098

IPv6: 0

Sender detail:

EPSILON

1 DNS querying mechanisms

2,688 IP addresses authorized

Senders Included in this SPF Record

Well-known Senders

EPSILON

Custom Senders

O Oregon Data Center

N New York Data Center

Go Back to Senders

Analyze With Data »

EasySPF Analyzer: Step 1

Analyze the Sender Data

1. Click Analyze with Data to modify the current SPF Record.

EasySPF™ Analyzer

Use this tool to analyze and update the SPF record for a specific domain.

- 1 Review Existing SPF Record
- 2 Analyze With Data
- 3 Publish Updated Record

Domain to analyze: **agaribank.com**

v=spf1 mx ip4:172.22.125.10/32 include:bfi0.com include:bigfootinteractive.com -all

[Reset to existing SPF record](#)

DNS Querying mechanisms (10 maximum): **3**

Syntax errors: **✓ No errors**

IP addresses authorized: **IPv4: 4,098**

IPv6: 0

Save

Save and Publish »

Details from Sender Data

seen in the last 14 days

Approved Senders	Supporting Data	DNS Querying Mechanism(s)	Include All	Select Subset	Exclude
N New York Data Center ip4:172.22.125.10/32 include:bfi0.com details include:bigfootinteractive.com details	0 messages from 0 IPs	0	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
		0	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
		1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
		1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
O Oregon Data Center mx details	0 messages from 0 IPs	0	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
		1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
U Unassigned	0 messages from 0 IPs	0	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
EPSILON include:bfi0.com details include:bigfootinteractive.com details	0 messages from 0 IPs	0	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
		1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
		1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Total DNS Querying mechanisms:		3			

Save

Save and Publish »

EasySPF Analyzer: Step 2

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
- 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:

```
v=spf1 mx ip4:172.22.125.10/32 include:bfio.com include:bigfootinteractive.com
ip4:67.228.245.98 -all
```

[Reset to existing SPF record](#)

Changes to the SPF Record

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 Subset of Sender Definition

Select portions of this Sender's SPF definition to include.

Sender:

eloqua.

Select all

Unselect all

SPF Definition:

☐ include:_netblocks.eloqua.com
 ☐ include:_trustedips1.eloqua.com

☐ ip4:204.92.19.0/24
 ☐ ip4:204.92.21.0/25
 ☐ ip4:204.92.22.0/24
 ☐ ip4:204.92.26.0/24
 ☐ ip4:204.92.31.0/24
 ☐ ip4:204.92.114.0/24
 ☐ ip4:66.48.80.0/25
 ☐ ip4:209.167.231.0/24
 ☐ ip4:129.145.16.0/21
 ☐ ip4:129.145.76.0/22
 ☐ ip4:141.145.8.0/21
 ☐ ip4:129.91.16.0/21

☐ include:_trustedips2.eloqua.com

☐ ip4:142.0.160.0/20

OK

Cancel

Selecting a subset of a Well-known Sender definition

2. Click

- Save to remain on Step 2 and continue to modify the SPF Record
- Save and Publish to move onto Step 3, Publish Updated Record.

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:

Manage the settings for [domain] ?

View, edit, and delete all the details for this domain.

Domain	Approved Senders		Unapproved Senders		DMARC Policy	BIMI Record	SPF		DKIM	
	#	Pass	#	Pass			Record	Pass	Key	Pass
[domain]	27.49M	100%	3.5M	100%	...		H	96.24%		98.64%

Is Third Party: ☐ ?

Is Defensive: ☐ ?

Is Primary: ☐ ?

Domain Groups: All Domains ?

Senders: [domain] Google, Unassigned ?

DMARC: Managed by Cisco ?

SPF: Managed by Cisco ?

DKIM: Not managed by Cisco ?

BIMI: Not managed by Cisco ?

Existing record:

```
v=spf1 include:%(d).02.spf-protect.[domain].com exists:%(i).%.%(d).d.espf.[domain].com -all
```

[View Record Details](#)

Last saved SPF Analyzer record:

```
v=spf1 mx ip4:172.22.125.0/24 ip4:10.44.140.67 ip4:10.44.140.68 include:_spf.[domain].com include:_spf.[domain].com -all
```

[View in SPF Analyzer](#)

Saved EasySPF Analyzer record for a domain

Publish the Updated Record

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.

EasySPF™ Analyzer

Use this tool to analyze and update the SPF record for a specific domain.

- 1 Review Existing SPF Record
- 2 Analyze With Data
- 3 Publish Updated Record

New SPF Record for: [domain]

```
v=spf1 include:servers.mcsv.net ip4:160.34.64.28 include:_spf.salesforce.com ip4:208.185.235.45 ip4:212.70.67.12 ip4:213.200.109.65 ip4:205.217.12.155 ip4:180.87.148.12 ip4:89.187.113.3 include:successfactors.eu include:_spf1.barclays.com ip4:216.74.162.17 ip4:216.74.162.18 ip4:94.236.35.193 ip4:193.148.38.199 ip4:217.11.0.38 ~all
```

DNS Querying mechanisms (10 maximum): 6

Syntax errors: ✔ No errors

IP addresses authorized: IPv4: 22,589
IPv6: 0

Warning: Your new SPF record includes one or more Senders which do not appear to Agari to support aligned SPF. You may need to take additional steps (for example, configuring aligned DKIM) in order to fully authenticate email originating from this sender to ensure delivery. See the following sender profile(s) for more information.

- Cvent - [Sender Profile](#)

Easy SPF Analyzer: Step 3 (upper portion)

The lower portion of the page will contain the new SPF record and instructions for creating the SPF record in DNS.

Click Print Instructions to create a printer-friendly version of the instructions.

You must take action for this SPF record to be published:

SPF Record - DNS Update Instructions

This revised SPF record is a recommendation. Be sure to monitor and review authentication rates for this domain and revise the SPF record as necessary.

The exact steps to get your SPF 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 SPF record be published as a TXT resource record for the domain `barclays.com`. Be sure to include the full SPF record below. There should be no line-wraps, newlines, or whitespace other than the spaces explicitly shown within the record below.

- If you have direct access to manage DNS for your domain through an online DNS administration tool, look for a section to publish a TXT record or a section specific to SPF records.
- If you have access to manage DNS for your domain through a web hosting online administrative interface, look for DNS Settings and a place to enter a TXT record or an SPF record.
- If your company manages its DNS internally you may need to submit a request to publish the DNS record through your company's DNS management team.
- If a third party hosts DNS for your domain, you may need to submit a ticket with them to update the domain's DNS settings.

Domain:

```
v=spf1 include:servers.mcsv.net ip4:160.34.64.28 include:_spf.salesforce.com
ip4:208.185.235.45 ip4:212.70.67.12 ip4:213.200.109.65 ip4:205.217.12.155
ip4:180.87.148.12 ip4:89.187.113.3 include:successfactors.eu include:spf1.barclays.com
ip4:216.74.162.17 ip4:216.74.162.18 ip4:94.236.35.193 ip4:193.148.38.199 ip4:217.11.0.38
~all
```

It may take up to 24-48 hours for the changes to appear within Agari after the record is published by your DNS provider.

[Print instructions](#)

EasySPF Analyzer: Step 3 (lower)

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).

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

Example DNS record for DKIM

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

Implement DKIM

The monitoring tools described in "Monitor Your Traffic" on page 75 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 Domain Protection, the insight into your mail flow helps you to enable DKIM.

DomainKeys Identified Mail

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 their 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.

Understanding Identifier Alignment

DMARC requires that a message not only pass DKIM or SPF validation, but that its identifier domains are "in alignment." Identifier alignment forces the domains authenticated by SPF (typically the MailFrom domain but can be the HELO domain if the MailFrom was empty) and DKIM (the DKIM signing domain as shown in the DKIM-Signature header's d= field) to have a relationship to the "header From" domain, which is more typically visible to a user in email clients. In "strict" alignment mode the domains must be an exact match. In "relaxed" alignment mode the domains can be different sub-domains of the same organizational domain.

For SPF, the message must pass the SPF check and the domain in the From: header must match the domain used to validate SPF (must exactly match for strict alignment, or may be a sub-domain for relaxed alignment, which is the default). See also "SPF Alignment" on page 29.

For DKIM, the message must pass the DKIM check and the d= domain of the valid signature must align with the domain in the From: header (must exactly match for strict alignment, or must be a sub-domain for relaxed alignment).

Even if SPF and DKIM pass authentication, DMARC will still fail if the identifiers are not aligned.

These are the terms used in identifier alignment:

- **Header From domain:** This is the domain portion of the email address that is most commonly visible to end users in the "From:" field displayed in an email client. It is not the display name, which is also commonly displayed in the same "From:" field. For example, the following may be displayed in an email client "From: Cisco <donotreply@blah.cisco.com>". In this example "Cisco" is the display name, while "cisco.com" is the organization domain although "blah.-cisco.com" is the actual domain of the From header.
- **SPF domain:** This identifier is used by the SPF authentication mechanism. Most commonly this is the domain used in the SMTP conversation's mail-from. However if the mail-from is empty (as with bounces, OOO notifications, and some other scenarios), then receivers will usually check for SPF passes with the host given in the HELO/EHLO of the message submission.
- **DKIM domain:** This identifier is used by the DKIM authentication mechanism. It is the domain designated by the 'd=' tag in the DKIM-Signature header.
- **DKIM public key:** used to decode the DKIM signature in a message is discovered from a DNS lookup that combines this 'd=' domain with the DKIM selector ('s='), also found in the DKIM-Signature header. The public key is specifically found in DNS at the TXT location of: {s}._domainkey.{d}, where s and d are found in the DKIM-Signature header of an email message.

DKIM 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:"

<https://technet.microsoft.com/en-us/library/mt695945>

OpenDKIM:

<http://opendkim.org/>

Wikipedia entry for DKIM:

https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail

RFC 6376, "DomainKeys Identified Mail (DKIM) Signatures"

<https://tools.ietf.org/html/rfc6376>

Word to Wise blog, "A DKIM Primer Resurrected:"

<https://wordtothewise.com/2016/04/a-dkim-primer-resurrected/>

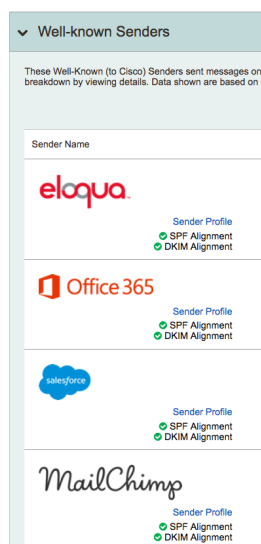
Request DKIM Signing From Third-Party Owners

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

1. Go to Diagnostics > Senders.
2. Select an individual domain.

The list of approved, well-known senders is shown in the top portion of the page.

For this example, assume that Salesforce is an approved, well-known sender for one of your domains:



Sender Salesforce and its Sender Profile link

3. Click the Sender Profile link for Salesforce to learn about Salesforce's DKIM capabilities:

Sender Profile: Salesforce.com

Detailed information on specific well-known senders.



Definition

Use Agari's definition ☐ Custom definition (advanced)

Web Site

<http://www.salesforce.com>

Important Information

For SPF: Salesforce supports aligned-SPF provided you take some additional configuration steps. Instructions can be found [here](#). Their sending IP-space can be added to your SPF record with "include:_spf.salesforce.com".

For DKIM: Salesforce supports aligned DKIM. Instructions are available [here](#). Our customer support would be happy to assist you with next steps.

Contact Information

<https://www.salesforce.com/form/contact/contactme.jsp>

Sender Profile details for Salesforce

- Click the link for the DKIM Instructions. This 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.

[← BACK TO HOME](#)

DOCUMENTATION

Create a DKIM Key in Salesforce Classic

Use the DKIM (DomainKeys Identified Mail) key feature to enable Salesforce to sign outbound emails sent on your organization's behalf. A valid signature provides recipients confidence that the email was handled by a third party such as Salesforce in a way authorized by your organization.

Available in: Salesforce Classic
Available in: All Editions

User Permissions Needed
Manage DKIM Keys
Customize Application

When you create a DKIM key, Salesforce generates a public and private key pair. Publish the public key in the DNS. This key tells recipients that you, as the owner of the domain, have authorized the use of this key to sign your mail. Salesforce uses the private key to create DKIM signature headers on your outgoing email. Recipients of the mail can compare the signature header with the public key in the DNS to determine that the mail was signed with an authorized key. If your domain also publishes a Domain-based Message Authentication, Reporting and Conformance (DMARC) policy, recipients can use the DKIM signature to verify that the mail conforms to DMARC.

To create a new key:

- From Setup, enter **DKIM Keys** in the Quick Find box, then select **DKIM Keys**.
- Click **Create New Key**.
- For Selector, enter a unique name.
- Enter your Domain name.
- Select the type of Domain Match you'd like to use.
- Click **Save**.

- The key defaults to Inactive state. Make sure that you add the public key to the DNS record before activating the key. DKIM signing is active whenever you have an active DKIM key.
- When publishing to the DNS, use these guidelines to format the name and values of the public key.
 - The name of the txt file is formed from the selector, followed by ".", then the domain key, followed by ".", then the domain name: selector._domainkey.domain.com.
 - The value in the txt file is in the format v=DKIM1; k=rsa; p=966w..., where the value after p= is the public key.
- You can't have more than one active DKIM key per domain name. You can have multiple active DKIM keys if your organization sends mail from more than a single domain or if you use a subdomain under your organizational domain and have specified domain matching at the subdomain level.
- When you insert or update a domain key, it's possible that the change affects existing DKIM keys. For example, if you've set DomainMatch to DomainAndSubdomain for the example.com domain, and you then set DomainMatch to SubdomainOnly for the mail.example.com domain, either key could be used. Here's how we resolve conflicts in the case when domain keys overlap.
 - If two keys are equally specific about matching for the same domain, the new key replaces and deactivates the existing key.
 - If a new key is more specific about matching than an existing key, the new key is used. The existing key is modified to no longer apply to the case covered by the new key. For example, because DomainOnly and SubdomainOnly are more specific than DomainAndSubdomain, a new DomainOnly key would change the DomainMatch to an existing DomainAndSubdomain key to become SubdomainOnly.
 - If multiple keys have different domains that match the sending domain, the key with the longest domain name is used. In a tie, the most specific key is used.

For information about DKIM, see <http://dkim.org>

See Also
[Improve Deliverability of Emails Sent from Salesforce](#)
[Import a DKIM Key in Salesforce Classic](#)

Salesforce DKIM documentation

Implement DKIM Keys for Third-Party Senders

Reading the documentation for each Sender (as in the Salesforce example in "Request DKIM Signing From Third-Party Owners" on the previous page), 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.

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>).

1. Go to Tools > DKIM.
2. Enter a domain name and selector. For example:

Check specific DKIM records

Enter the name of a domain and a specific selector to view the requested DKIM record.

Selector:

Domain:

Lookup of s1024._domainkey.agari.com resulted in this raw data being found in DNS:

```
v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDQwPqBxkIOc1YVnJv3Ocfbd3S68p8E5BafsiRMBaSPxqIgnzaxNSyPp8INEPL61cIRKo3u19
5Px5XHnWjEfQ76BvDu7eUYXxY8zKcAS74heKAeyfpVaMFWHUzCoujPNzzorCIRtP5CuY+ILw+Vj1SKN6x1BWhouCSHWhOr/vcYQIDAQAB
```

Key length: 1024

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

Message ID	<6B88EFC2-0C5A-4A25-B5A6-72D230269124@cisco.com>
Created at:	Tue, Jun 19, 2018 at 2:46 AM (Delivered after 6 seconds)
From:	[REDACTED]@cisco.com>
To:	[REDACTED]
Subject:	[REDACTED]
SPF:	PASS with IP 173.37.142.88 Learn more
DKIM:	'PASS' with domain cisco.com Learn more
DMARC:	'PASS' Learn more

Examining the headers for the message, you can see that Salesforce inserted the proper DKIM headers:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
d=cisco.com; i=@cisco.com; l=5289592; q=dns/txt;
s=iport; t=1529401619; x=1530611219;
h=from:to:subject:date:message-id:references:in-reply-to:
mime-version;
bh=wwnGqrNevIbPG97FceJsWcspPFmLJJludpJAODKqgzM=;
b=Cr5VTd6UKKVC8ixQr4G/FwA3gOWTezZNM8YYUpDf/06uxRm1lepYH9XF
exxCsMcmhtauyH7CUXFfl2csTgWOnutzrhWhIU3p01U2fX821e8VXH1eI
bDnRiQb9C+gaVVgv27MRcpmaJZCnxOaBjJUC/Ubs5Go+vZE+tfADyXX/0
o=;
```

d=cisco.com - The domain is cisco.com

s=iport - The selector is 'iport'

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.

For more details on the contents and construction of the DKIM header stamped by the sending agent, refer to https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail#Technical_details.

Enable 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 a tool to create the DKIM public/private key pairing and the policy record. The public key is a key that you will place in your public-facing DNS record along with the DKIM 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/>

<http://dkimcore.org/tools/keys.html>

<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 creating a new record for each domain.

Cisco can host the DKIM records for your domains. This still requires that you add nameserver (NS) records to your domain, but with Cisco hosting the DKIM records themselves, any changes that you make in Domain Protection will be published automatically and you will not have to touch your own DNS records again.

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:



- IronPort: https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide/b_ESA_Admin_Guide/b_ESA_Admin_Guide_chapter_010101.html
- Symantec: https://support.symantec.com/en_US/article.HOWTO126432.html
- Postfix: <https://petermolnar.net/howto-spf-dkim-dmarc-postfix/>

Host Your DKIM Records at Cisco

Allowing Cisco to host your DKIM records means that when you make changes in Domain Protection that affect any DMARC records, the records are updated quickly, securely, and automatically.





1. Go to Diagnostics > Senders.
2. Select a single domain.
3. Click Monitor DKIM Keys.
 - If you are taken to the Manage Hosted DKIM Keys page, the DKIM keys for this domain are already hosted by Cisco.
 - If you are taken to the DKIM Management page, the DKIM keys for this domain are not hosted by Cisco.
4. If you are on the DKIM Management page. review the DKIM key information for the domain. If there are no DKIM keys, you can click Add New Key for... to add a new DKIM key for the domain.
5. Click I'm ready to start hosting.
6. Review the DKIM information. For some selectors, you will have an option of selecting whether you want Cisco to host the CNAME or the TXT record.
 - CNAME (default): Means the CNAME key is likely hosted by a third party, and any changes made to the DKIM key by the third party for the domain will be detected automatically by Cisco.
 - TXT: Select this only if you want to always keep the DKIM key for the domain as-is. Any third-party changes to the DKIM key will not be detected automatically by Cisco. (This is not common when the option to use a CNAME record is available, but is the default when no CNAME is available.)
7. Click Start Hosting.

At this point, you will have to update the nameserver information (the NS records) at your domain host. The page you will see gives you the information you will need for the NS records.


Once you update your DNS and the update is propagated, then on the Diagnose the DMARC status of your domains page (Diagnostics > Domains), you will see an "H" next to the symbol in the DKIM column (). Until you update your DNS, you will see a hosting pending symbol () in the DKIM column.

Verify That DKIM is Working

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:

Sender Name	Domains	Volume	SPF Pass	SPF Record	DKIM Pass
	9 (total)	126,949	99%	--	99%
	Details				
		113,995	99%		99%
		10,576	99%		100%
		1,162	100%		100%

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:

Sender Name	Domains	Volume ▼	SPF Pass	SPF Record	DKIM Pass
 marketing cloud		1,608,507	99%	●	100%
Sender Profile					

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.

Find DKIM Problems

Using the What are my DKIM Problems? report, you can often identify domains and categories of issues to be addressed as you work through authentication and achieving DKIM signing for each sender in a given domain.

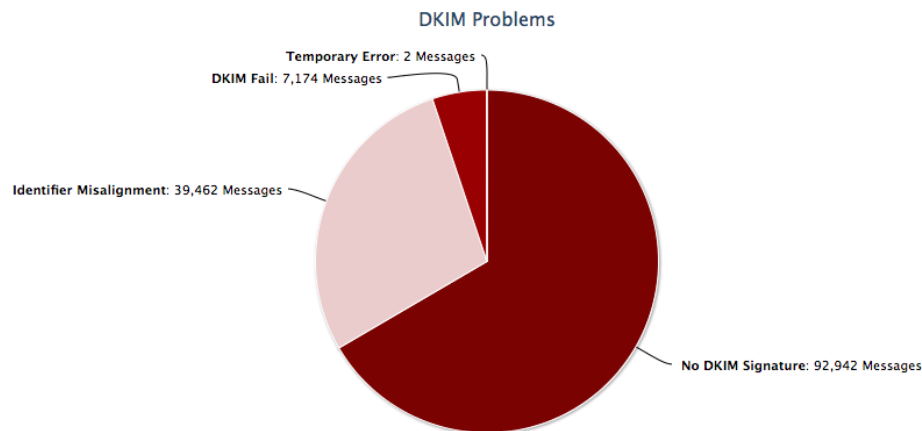
1. Go to Analysis > Email Traffic.
2. Click What are my SPF Problems? to view the initial report.

What are my DKIM problems?

Inc. **DKIM Problems Report for Active Domains** using **Outbound Data** from March 13 to March 26, 2018

[Share](#)

[Schedule](#)



Hover over a chart section for an explanation of the corresponding problem or click on a section to investigate further.

DKIM Problems

Domains: 'Active Domains' Group
Message Sources: Only messages from my Sender Inventory
Date: 14 days starting on 2018-03-13
Displaying results based on the top 1,000 IPs
[Search for Failure Samples on 2018-03-26](#)

The top level of the DKIM Problems report

DKIM Problems Example

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). See " Configure Email Traffic Reports" on page 105 for details.

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:

Sender	DKIM Issues	Total
Google	All Issues	107,981
	Identifier Misalignment	106,858
	No DKIM Signature	1,057
	DKIM Fail	66

Identifier Misalignment issues with Google

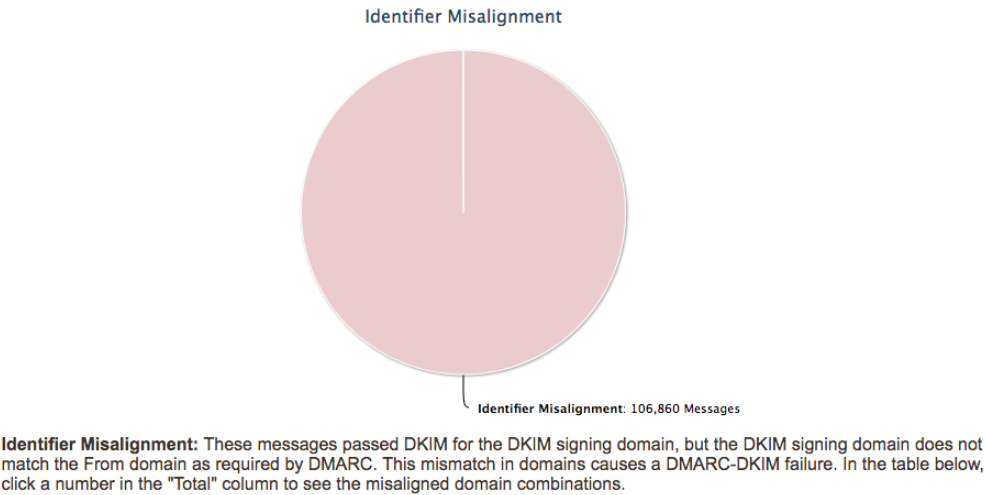
Click the links for the messages sent from Sender Google to drill into the details for that sender:

DKIM Problems

DKIM Problems Report for Active Domains from March 13 to March 26, 2018

Share

Schedule



Identifier Misalignment

Domains: 'Active Domains' Group
Message Sources: Only messages from Google
Date: 14 days starting on 2018-03-13
Displaying all 9 results
[Search for Failure Samples on 2018-03-26](#)

Search within table:

IP	PTR Name	SBRS	Country	DKIM Issue	Total
209.85.220.69	mail-sor-f69.google.com	4.3	United States	Identifier Misalignment	106,800
209.85.220.41	mail-sor-f41.google.com	4.3	United States	Identifier Misalignment	37
209.85.220.101	mail-sor-f101.google.com	4.4	United States	Identifier Misalignment	13
209.85.220.55	mail-sor-f55.google.com	1.0	United States	Identifier Misalignment	4
209.85.220.97	mail-sor-f97.google.com	4.4	United States	Identifier Misalignment	2
2607:f8b0:4001:c06::245	mail-io0-x245.google.com	2.5		Identifier Misalignment	1
2607:f8b0:400e:c01::242	mail-pl0-x242.google.com	2.5		Identifier Misalignment	1
74.125.83.43	mail-pg0-f43.google.com	3.5	United States	Identifier Misalignment	1
209.85.160.53	mail-pl0-f53.google.com	3.4	United States	Identifier Misalignment	1
Total					106,860

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.

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 that is mis-aligned with the DKIM key:

Identifier Misalignment from 209.85.220.69

Domains: 'Active Domains' Group
 Message Sources: 209.85.220.69
 Date: 14 days starting on 2018-03-13
 Displaying all 40 results
[Search for Failure Samples on 2018-03-26](#)

Search within table:

Domain	DKIM domain	Google	Yahoo!	AOL	Microsoft	Others	Total
a.com	u.ia.com	50,660	0	0	0	0	50,660
		42,819	0	0	0	0	42,819
		5,395	0	0	0	0	5,395
		5,201	0	0	0	0	5,201
		1,125	0	0	0	0	1,125
		1,118	0	0	0	0	1,118
		258	0	0	0	0	258

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. See "Share an Email Traffic Report" on page 105 and "Schedule an Email Traffic Report" on page 106 for details.

Keep in mind that all scheduled reports maintain the scope of the current view. 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 DKIM records for your domains.

EasyDKIM Analyzer

You can use the Domain Protection EasyDKIM Analyzer to analyze an existing DKIM record or to create a brand new DKIM record based on your approved senders.

View DKIM Keys for a Domain in EasyDKIM Analyzer

Domain Protection's EasyDKIM Analyzer helps you view information about and make changes to the DKIM records for your domains. It also makes it easy to host your DKIM records at Cisco if you do not do so already.

1. Go to Diagnostics > Senders.
2. Select a single domain.

3. Click Monitor DKIM Keys.

If you are taken to the Manage Hosted DKIM Keys page, the DKIM keys for this domain are already hosted by Cisco. If you are taken to the DKIM Management page, the DKIM keys for this domain are not hosted by Cisco. In either case, what you see and what you can do here, except related to DKIM hosting, is the same.

The Manage Hosted DKIM Keys/DKIM Management page lists the DKIM key information for the domain in a table with details about each key. The default view displays the DKIM keys sourced from aggregate and forensic data for the domain and seen by Domain Protection since the domain was verified. Click the Search for selector radio button and enter all or part of a selector to filter the list by what you enter.

DKIM Management

Use this tool to manage and monitor DKIM keys for a specific domain.

Domain to analyze:

☒ All

☐ Search for selector

I'm ready to start hosting >

Selector	Key	Senders	Key Dates	Notes	Type
feb2018	▶ 1024	--			Manual


Add New Key for sashimicu.org

An example DKIM Management page.

DKIM key information will have a blue background if it was manually entered into Domain Protection.

The following table describes the information available for each DKIM key for the domain on the DKIM Management page.

Item	Description
Selector	The s= part of the DKIM signature.
Key	Shows the key length, in bits. Click on the number to see the details of the DKIM record in DNS. The details will be headed with CNAME: if the DKIM record is in a CNAME DNS record. You may also see (in yellow or red) or icons next to the key length, indicating issues with the DKIM record. The icon indicates one or more missing parts from the DKIM record in DNS. The indicates an excessive amount of time has elapsed since the key has been rotated (if yellow, 60 to 90 days, if red, more than 90 days). Click on either icon for more details.
Senders	Lists the senders that use this DKIM key for the domain. Click to see the senders for the DKIM key. an envelope icon () next to a sender name indicates that the sender is a known mailbox provider and may not be the origin of messages with this DKIM selector.
Key Dates	Click the next to a sender to see when the DKIM key was first seen and more recently seen by Domain Protection in a message sent by the sender for the domain.
Notes	You can enter notes about the DKIM record for the domain for your own reference. Click to add, edit, or delete the note.
Type/Edit	If the DKIM records for the domain are not hosted by Cisco, then the heading for this column is Type, and the information is the type of record for the domain. This will usually be

Item	Description
	<p>DNS.</p> <p>If the DKIM records for the domain are hosted by Cisco, the heading for this column is Edit.</p> <p>Click the  icon to edit the DKIM record.</p>

Add a Domain DKIM Record for Domain Protection to Monitor

If you have a DKIM record for a domain that is not yet visible in Domain Protection, you can add it manually.

You must know the selector for the DKIM record.

1. Go to Diagnostics > Senders.
2. Select a single domain.
3. Click Monitor DKIM Keys.
4. Click Add New Key for [DomainName].
5. Enter the selector for the DKIM key you want to add.
6. Click Lookup. Review the DKIM record to make sure it is accurate.
7. Click Add DKIM Key.

The DKIM key is added to the Manage Hosted DKIM Keys/DKIM Management page. The key information will have a blue background and will show Manual in the Type column to show that it was manually added, not automatically detected by Domain Protection.

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.

Example DNS record for DMARC:

```
dmARC.domain.com. IN TXT "v=DMARC1; p=reject; rua=mailto:d@rua.cisco.com; ruf=mailto:d@ruf.cisco.com;"
```



DMARC builds upon DKIM and SPF to provide both protection and reporting

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 Domain Protection, and, indirectly, a way 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 Domain Protection to analyze the data and modify your mail streams as appropriate.

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.")

To publish a DMARC record at monitor, you

- "Create a DMARC Record With DMARC Builder" below
- "Publish the DMARC Record in DNS" on page 66
- "Add Organization Domains for DMARC Policy Publication" on page 68

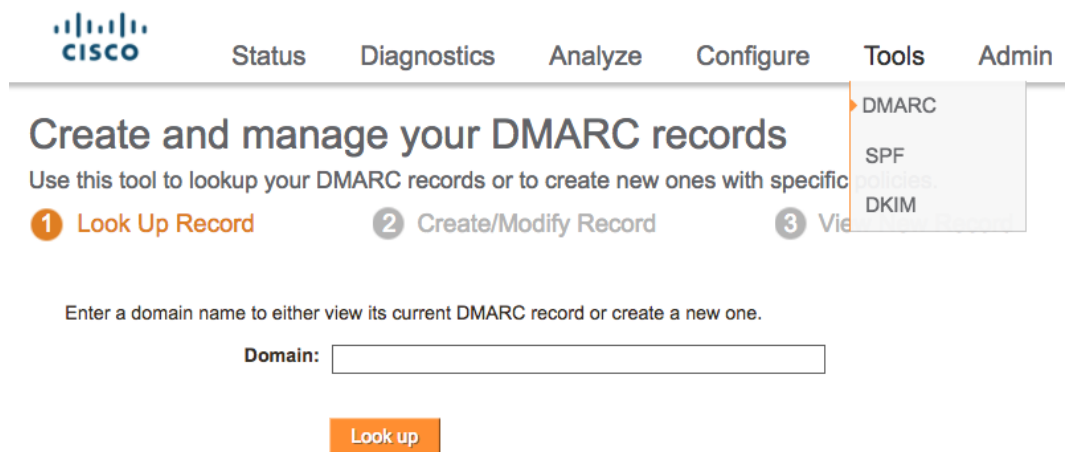
Create a DMARC Record With DMARC Builder

Domain Protection'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.

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

1. Go **Tools > DMARC**.



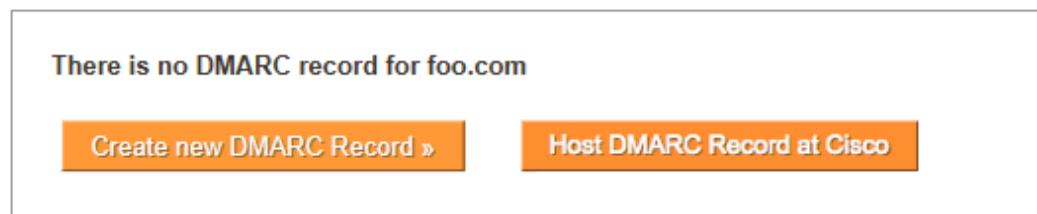
Enter a domain name to either view its current DMARC record or create a new one.

Domain:

Look up

DMARC Builder Step 1

2. Enter a domain name.
3. 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:



There is no DMARC record for foo.com

Create new DMARC Record » Host DMARC Record at Cisco

4. Click **Create new DMARC record**.
5. Enter the settings for the DMARC record. See "DMARC Builder Settings" on page 69 for details.
6. Click **Continue**.
7. Click **Create Instructions**. This will download a text file (.txt) to use in the next step.

Repeat for each domain you plan to protect in Domain Protection.

DMARC 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 "cisco-demo@rua.cisco.com" and "cisco-demo@ruf.cisco.com."

Create and manage your DMARC records

Use this tool to lookup your DMARC records or to create new ones with specific policies.

- 1 Look Up Record
- 2 Create/Modify Record
- 3 View New Record

Choose and review settings below to create a DMARC record. [Read the help documentation](#) for details about each setting.

Domain(s):

foo.com

Policy:

Monitor

Send Aggregate Data to:

cisco-demo@rua.dmp.cisco.com

additional email address (optional)

Send Forensic Data to:

cisco-demo@ruf.dmp.cisco.com

additional email address (optional)

Advanced Settings

« Back

Continue »

DMARC Builder Step 2

This DMARC record is for the domain “bar.com”:

Create and manage your DMARC records

Use this tool to lookup your DMARC records or to create new ones with specific policies.

- 1 Look Up Record
- 2 Create/Modify Record
- 3 View New Record

Your new DMARC records are below. You must take action for DMARC records to be published!

Click 'Create Instructions' for guidance on getting your DMARC record published. It may take up to 24-48 hours for the changes to appear within Domain Protection after the record is published by your DNS provider.

Domain Protection will detect published changes and update various dashboard screens accordingly. You may notice changes to your To-Dos.

Create Instructions

Domain	DNS Record Location	DMARC Record
bar.com	_dmarc.bar.com	v=DMARC1; p=none; fo=1; ri=3600; rua=mailto:cisco-demo@rua.dmp.cisco.com; ruf=mailto:cisco-demo@ruf.dmp.cisco.com

« Back

DMARC Builder Step 3

It 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
- **fo=1** – The directive to send a DMARC failure report to the domain owner if authentication/alignment vulnerabilities are found is 1, or if anything other than an aligned (pass) is produced
- **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.

Publish the DMARC 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 "Create a DMARC Record With DMARC Builder" on page 63. 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:

- If you have direct access to manage DNS for your domain through an online DNS administration tool, look for a section to publish a TXT record or a section specific to DMARC records.
- If you have access to manage DNS for your domain through a web hosting online administrative interface, look for DNS Settings and a place to enter a TXT record or a DMARC record.
- If your company manages its DNS internally you may need to submit a request to publish the DNS record through your company's DNS management team.
- If a third party hosts DNS for your domain you may need to submit a ticket with them to update the domain's DNS settings.

Congratulations!

Once you have published your DMARC record with your DNS provider, it may take up to 24-48 hours for the changes to appear within Domain Protection.

Host Your DMARC Records at Cisco

Allowing Cisco to host your DMARC records means that when you make changes in Domain Protection that affect any DMARC records, the records are updated quickly, securely, and automatically.

Adding a new DMARC record (see "Create a DMARC Record With DMARC Builder" on page 63) and hosting the DMARC record at Cisco cannot be done all at once.

You can host the DMARC record for a domain at Cisco once the domain has been verified.

1. Go to Configure > Manage Domains.
2. Click All Domains.
3. Select one or more domains with No in the DMARC Hosted column.
4. Click Manage DMARC.
5. Click Host DMARC Record at Cisco.

- Click Get Hosting Instructions. This will download a text file with the information you will need for the next step.
- In the DNS records for each domain, create a new CNAME record. The file you downloaded has an entry for each domain. In your host records for each domain, add a CNAME record with the Name using the DNS Record Location value from the file and the Record using the CNAME Record value from the file. Copy the values exactly as they exist, with no added characters, carriage returns, and so on.

This last step is performed outside of Domain Protection and is necessary to make Cisco the host of record for DMARC.

Create a Hosted DMARC Record for a Domain That Has No DMARC Record

- Go to Configure > Manage Domains.
- Click No DMARC.

Manage your Domains

Edit or delete domains, create Custom Domain Groups, add or remove domains from Custom Domain Groups.

Domains which do not have a published DMARC record. They are not protected by DMARC at all. To create a record, select the domain from the list and click on the "Create DMARC" button.

System Domain Groups	Domain	Agari Policy	DMARC	Date Added
All Domains	authmetrics.com	Reject	No DMARC	2014-01-30
Active Domains	fsisacdemo.authmetrics.com	Reject	No DMARC	2014-01-30
Defensive Domains	isspooling.com	Reject	No DMARC	2014-01-30
Monitor Policy				
Quarantine Policy				
Reject Policy				
No DMARC				
Third Party				
DMARC Hosted by Cisco				
SPF Hosted by Cisco				
DKIM Hosted by Cisco				
Primary Domains				
Custom Domain Groups				
+ Add New Group				

- Select the domain(s) you want to have DMARC records hosted at Cisco.
- Click Manage DMARC.
- Review the DMARC settings for the domain(s).
- Click Host DMARC Record at Cisco.
- Click Get Hosting Instructions. This will download a text file with the information you will need for the next step.
- In the DNS records for each domain, create a new CNAME record. The file you downloaded has an entry for each domain. In your host records for each domain, add a CNAME record with the Name using the DNS Record Location value from the file and the Record using the CNAME Record value from the file. Copy the values exactly as they exist, with no added characters, carriage returns, and so on.

Add Organization Domains for DMARC Policy Publication

If you published DMARC records with a p=None policy for all of the domains you are planning to protect with 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 have not published a p=None policy, then just add them in Domain Protection. In Domain Protection, most activities are centered around the domain. Your activity in this step will be to let Domain Protection know which domains are associated with your organization.

- 1. Go to Status > Protection.
- 2. Click Add Domains.
- 3. Enter the information about your domains.

How do you want to add your domains?	<p>You can type one or more domains or upload a file with domain information.</p> <ul style="list-style-type: none">• Select Type in your domain(s), then enter one or more domains in the text field, separated by commas.• Select Upload a file of domain names (txt or csv), then click Choose File and select a file that contains one or more domain names separated by commas.
Add to these Custom Domain Groups	<p>Click in the field to add the domain(s) to one or more domain groups. (See "Domain Groups" on page 117.)</p> <p>You can also click Add a new group to create a new domain group.</p>
Set the Cisco Policy	<p>This determines the DMARC policy level for the domains you are adding.</p>
Mark as Defensive	<p>A defensive domain is a domain similar to your company domain that does not send email but that you own to keep others from owning it.</p>
Mark as Third Party	<p>A third-party domain is a domain where the content and email are managed by a third party. This is common for subdomains. For example, warriors.nba.com.</p>
Mark as Primary	<p>Your important domains that you want to move to reject as soon as possible.</p>

- 4. Click Add your domains.

You will see a verification message. At this point, Cisco will verify that your organization is responsible for these domains, which may take up to 24 hours.

You can see a list of unverified domains by going to Configure > Unverified Domains.

What’s an Unverified Domain?

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

An Cisco representative takes an action to ensure that any domain uploaded into the system domain is ready to be managed, verifying the domain. Cisco will periodically check all unverified domains to see if changes have occurred that 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. To do this, see "Publish the DMARC Record in DNS" on page 66. 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 authority over the domain. (By verifying every domain entered into the system, Cisco can ensure that no domains are mistakenly or inadvertently entered.)

Once Cisco verifies the domain, you can have the DMARC record hosted by Cisco. See "Host Your DMARC Records at Cisco" on page 66 for details. Once a domain's DMARC record is hosted by Cisco, any changes in Domain Protection that affect the DMARC record are made to the record quickly, securely, and automatically.

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 Domain Protection. 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 Domain Protection. 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).

DMARC Builder Settings

A DMARC policy allows a sender to indicate that their emails are protected by SPF and/or DKIM and tells a receiver what to do if neither of those authentication methods passes, such as quarantine or reject the message. Domain Protection'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). DMARC Builder also provides information about the DNS provider for the domain and how to get the DMARC record published.

This topic describes all the settings in DMARC Builder. (The Advanced Settings are optional and will default to the recommended settings. It is recommended that you not change these settings.)

Setting	Description
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.

Setting	Description
Policy	<p>The action that a domain owner requests email receivers to take on received messages with their domain in the <i>header From</i> address that fail DMARC. Select:</p> <ul style="list-style-type: none"> • 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. 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	<p>The email address where DMARC forensic data will be sent. 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.</p> <p>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.</p>
Advanced Settings	
Report Format	Specifies the format of DMARC forensic reports. While the DMARC specification allows both AFRF and IODEF, currently the only format sent by DMARC receivers is AFRF.
DKIM identifier alignment	<p>Defines how sub-domains are handled in DKIM. Select:</p> <ul style="list-style-type: none"> • Relaxed: to allow the DKIM signing domain and header from domain to be sub-domains of each other • Strict: to require the DKIM signing domain and header from domain be an exact match
SPF identifier alignment	<p>Defines how sub-domains are handled in SPF. Select:</p> <ul style="list-style-type: none"> • Relaxed: to allow the MailFrom domain and header from domain to be sub-domains of each other • Strict: to require the MailFrom domain and header from domain be an exact match
Apply to %	This is the percentage of messages from the domain for which the policy will be applied. For example, if you specify a "reject" policy and 50% here, then the reject policy will only be applied to a random 50% of the messages failing DMARC Authentication by the receiver.
Reporting Interval	The DMARC specification allows you to request DMARC aggregate reports covering different time intervals. In reality all current DMARC implementations only send reports in 24 hour increments.

Setting	Description
Subdomain Policy	By default, a domain's DMARC policy applies to all of its sub-domains. DMARC 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, publish a DMARC records specifically for those sub-domain.
Forensic Report Options	You can tell DMARC receivers under which failure conditions you would like to receive forensic reports. Customer Protect will set this to send reports for any SPF or DKIM failure by default. You can change this to send reports only if both SPF and DKIM fail.



CHAPTER 4

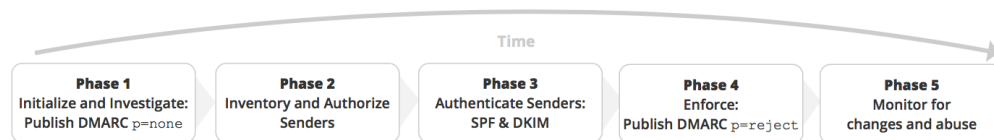
Implementing DMARC

This section will walk you through the process of implementing DMARC at your organization.

The Overall Process

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

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



The phases of implementing DMARC

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:

The overall process for Implementing Cisco Domain Protection

Phase	Step
Phase 1	1. Obtain access to Domain Protection 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)
	7. Create a spreadsheet to track all third-party Senders

Phase	Step
Phase 3	8. Propose new SPF Record
	9. Publish new SPF Record
	10. Identify internal business owners
	11. Request DKIM signing from third-party owners
	12. Implement DKIM keys for all third-party senders
	13. Verify DKIM working for all third-party senders
	14. Enable DKIM signing on email gateway
	15. Verify DKIM working on email gateway
Phase 4	16. Obtain sign-off from all business owners
	17. Move DMARC record(s) to Reject (work with Cisco for final review)
Phase 5	18. Review Alerts and Reports

You can think about steps 2 and steps 4-18 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.

Get Credentials and Training

As part of the typical initiation and onboarding process, you should receive a instructions on how to access Cisco Domain Protection.

During this kick-off meeting, your Cisco representative will provide access to Cisco Domain Protection at <https://dp.cisco.com>.

Cisco sends you an email with your initial account credential information; this account is the first administrative account for your organization. You will use this account to create additional user accounts for your organization.

Get info here'. Then, there is a label 'Your Email:' followed by a white text input box. Below the input box is an orange button with the word 'Next' in white text."/>

The Domain Protection login.

Contacting Support

If you have not received access, contact Cisco support at <https://www.cisco.com/c/en/us/support/all-products.html>.

Advanced Topics

Some items to consider at this stage:

- Domain Protection contains role-based permissions and access control (RBAC), which grants differing levels of permissions to user accounts. You may want to think about creating a read-only user, an audit-only user, or a user who can only administer reports within the portal, for example. To learn more about permissions, see "User Accounts" on page 127.
- Once you sign in to Domain Protection, you will be redirected to a URL that 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, see "Single Sign-On (SSO)" on page 131.

The administrator account (and any subsequent accounts with user creation permissions) can reset passwords for users you create.

Monitor Traffic and Senders

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

You can now begin the process of monitoring email traffic, identifying domains to secure, and identifying and classifying all Senders, and finally, creating a spreadsheet to track all third-party Senders.

Monitor Your Traffic

As DMARC reporting data (aggregate and forensic) begins to be sent into Domain Protection, you can begin the process of monitoring your traffic. As one customer for Cisco has said, the process of being able to monitor traffic from DMARC reporting data, “Turning on Cisco was like turning on the lights in a dark room.”

In most cases, it is recommended to obtain at least two weeks of data collection to achieve 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)
- 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

Go to [Analyze > Email Traffic](#) to familiarize yourself with the available reports in Domain Protection.

The [Analyze Email Traffic](#) pages provide a list of common questions to provide you with helpful views into your email ecosystem. See “[Email Traffic Reports](#)” on page 101 for more information about what you can see and do with these reports.

Take some time to explore all views and drill-down capabilities in these reports.

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

Identify a Target Domain or Set of Domains

After spending a period of time monitoring the data in 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 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. support.foo.com) 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 "Domain Groups" on page 117.

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).

Senders

The Senders page helps you organize and track the well-known and custom senders for every domain in the Domain Protection system. On the Senders 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 the specific DNS record sources that we used to discover them. You can use the Senders page to help organize and track the well-known and custom senders for every domain in the system.

To view your senders, go to Diagnostics > Senders. The Senders page shows

- Approved well-known senders and custom senders
- Unapproved senders and IP addresses

By default, Domain Protection will recognize well-known third party senders by their sending infrastructure. For example, in this view, the organization has identified and approved Marketo, Acxiom, Taleo, and Epsilon as legitimate third-party senders.

Senders

Discover which senders are authenticating email sent on behalf of your domains.

☒ All Domains
 ☐ Single Domain < Choose Domain >

☒ Most Recent: 14 day(s)
 ☐ Date Range: 2018-06-06 to 2018-06-19






Approved

Unapproved

Well-known Senders

These Well-Known (to Cisco) Senders sent messages on your behalf. When there are multiple domains using a sender, you can view the per-domain breakdown by viewing details. Data shown are based on the top 100 IPs by volume; click the links for additional data where available.

Search:

Sender Name	Domains	Volume	SPF Pass	DKIM Pass
 <div> Sender Profile ✓ SPF Alignment ✓ DKIM Alignment </div>	3 (total) ciscofunds.com & 2 more Details	4,790	0%	52%
 <div> Sender Profile ✓ SPF Alignment ✗ DKIM Alignment </div>	3 (total) ciscofunding.com & 2 more Details	706	0%	49%
 <div> Sender Profile ✓ SPF Alignment ✓ DKIM Alignment </div>	3 (total) ciscofunds.com & 2 more Details	349	0%	51%
 <div> Sender Profile ✓ SPF Alignment ✓ DKIM Alignment </div>	3 (total) ciscofunds.com & 2 more Details	287	0%	54%
 <div> Sender Profile ✓ SPF Alignment ✓ DKIM Alignment </div>	ciscofunds.com	0	0%	0%

Displaying 1-5 of 5 Well-Known Senders

Previous 1 Next

 Well-known Senders Per Page: 10

Marketo, Acxioim, Taleo, and Epsilon in the Well-known Senders section on the Senders page.

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

As data begins flowing into Domain Protection, it is aggregating information for your entire organization, as well as on a per-domain basis. 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.

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

- Unapproved well-known senders
- Unapproved IP addresses

You can filter the data on the Senders page by domain and by date range. See "Senders Filters" on page 85 for details.

What is the point of the Senders page?

As data begins flowing into Domain Protection, it 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 custom 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.) This act of authorizing senders within Domain Protection, moving them from Unapproved to Approved, will be the basis of (and reflected in) the SPF and DKIM policies you manage for your domains. You will then work to authenticate all email from approved Senders for your domains, and your DMARC policies will instruct receivers on what to do with message that fail authentication.

From here, you can:

- "Approve a Sender for a Domain" below
- "Ignore a Sender for a Domain" on page 81
- "Add an Unapproved IP Address to a Custom Sender" on page 84
- "Ignore an Unapproved IP Address" on page 84

Approve a Sender for a Domain

As Domain Protection accumulates data about the entities that send mail on behalf of your domains, you will want to approve well-known senders for each domain so...

1. Go to Diagnostics > Senders.
2. Click Single Domain, then select a domain. This list contains all of the domains you manage in Domain Protection.
3. Click the Unapproved tab.

4. Click the name of an unapproved sender to review the information about that sender to make sure it is one you want to approve. Key things you should verify include
 - What is the volume and regularity of traffic from the unapproved sender? A sender that is sending with a consistent cadence is more likely to be a legitimate sender.
 - Is there any Failure Sample data that can be used to understand the traffic? If samples are available using the Failure Samples explorer, you may be able to determine whether there is legitimate use of the unapproved sender
5. Click the browser's Back button.
6. If you still want to approve the sender, click its Approve link.
7. In the Add Sender dialog box, review the IP space (the IP addresses and netblocks). You will also see a Select Additional Domains field if there are other domains that this sender sends email on behalf of. You can select these domains to be approved also for this sender at this time if you do not want to review the sender for those domains individually.
8. Click Add to Approved.

Add a Sender to a Domain

When senders are sending traffic on behalf of your domains, part of the process is approving those senders. (see "Approve a Sender for a Domain" on the previous page.) You can also approve a sender for a domain that in the case where Domain Protection has not detected any traffic.

The process for adding well-known senders is slightly different from adding custom senders.

Add a well-known sender to a domain

1. Go to Diagnostics > Senders.
2. Click Single Domain, then select a domain. This list contains all of the active domains you manage in Domain Protection.
3. Click the Approved tab.
4. In the Well-known Senders section, click Add Well-known Sender.
5. Select a sender. The list contains all unapproved well-known senders for the domain.
6. Click Add to Approved.

Add a custom sender to a domain

1. Go to Diagnostics > Senders.
2. Click Single Domain, then select a domain. This list contains all of the active domains you manage in Domain Protection.
3. Click the Approved tab.
4. In the Custom Senders section, click Add Custom Sender.
5. Select a sender. This list contains any unapproved custom senders that have no traffic for the domain.
6. Click Add to Approved.

Ignore a Sender for a Domain

When you discover a sender sending mail on behalf of a domain you manage that you do not want Domain Protection to classify, you can tell Domain Protection to ignore that sender for that domain.

1. Go to Diagnostics > Senders.
2. Click Single Domain, then select a domain. This list contains all of the domains you manage in Domain Protection.
3. Click the Unapproved tab.
4. Click the name of an unapproved sender to review the information about that sender to make sure it is one you want to ignore. Key things you should verify include
 - Is it possible that the unapproved sender is acting as a forwarder? Hosting services and Mailbox providers are sometimes used to forward messages, but most often in relatively low volumes. There is no need to authorize these senders unless you actually use them for originating traffic.
5. Click the browser's Back button.
6. If you still want to ignore the sender for the domain, click the sender's Ignore link.
7. In the Ignore Sender dialog box, you will see in the Select Additional Domains field the other domains that this sender sends email on behalf of. You can select these domains to be ignored also for this sender at this time if you do not want to review the sender for those domains individually.
8. Click Add to Ignore List.

Add an IP Address to a Custom Sender

You can manually add IP addresses or netblocks to existing customer senders or use them to define new customer senders.

The same IP address cannot belong to more than one well-known sender or more than one custom sender at the same time. No portion of an IP address range (netblock) can belong to (overlap with) more than one well-known sender or more than one custom sender at the same time. The same IP address or portion of an IP address range can belong to (overlap with) no more than one well-known sender and no more than one custom sender.

1. Go to Diagnostics > Senders.
2. Click Single Domain, then select a domain. This list contains all of the domains you manage in Domain Protection.
3. Click the Approved tab.

4. In the Custom Senders section, click Add IP Address.

Add IP Address

IP Address:

Look Up

Example: 73.154.1.23 or 73.154.0.0/16

Domain:

.com

Look up IP addresses to see if they match a Sender.

In most cases, it is recommended to add the known Sender to your sender inventory.

Custom Sender:

☒ Add to Custom Sender

☐ Create Custom Sender

Add to Approved

Cancel

5. In the IP Address field, enter either a single IP address or a netblock (IP address range, which must be entered in CIDR (Classless Inter-Domain Routing) notation).
6. Click Look Up.

At this point, there are several things that can happen, and the actions you can take depend on the lookup result.

Lookup	Lookup Result	Possible Actions
IP address	Already included in the definition of a well-known sender.	<div>Do nothing, which leaves the IP address in the approved sender.<ul style="list-style-type: none">Click Cancel.</div> <div>Add the IP address to an existing approved custom sender.<ol style="list-style-type: none">Click Add to Custom Sender, and then select an existing custom sender.Click Add to Approved.</div> <div>Add the IP address to a new custom sender and approve that custom sender.<ol style="list-style-type: none">Click Create Custom Sender, and then enter a custom sender name.Click Create and Approve.</div>
IP address	Already included in the definition of a custom sender.	<div>The IP address cannot be added to an existing custom sender, nor can it be used to create a new custom</div>

Lookup	Lookup Result	Possible Actions
		sender. Different custom senders cannot include the same IP address. You can only Cancel.
IP address	No sender detected.	<p>Add the IP address to an existing approved custom sender.</p> <ol style="list-style-type: none"> 1. Click Add to Custom Sender, and then select an existing custom sender. 2. Click Add to Approved. <p>Add the IP address to a new custom sender and approve that custom sender.</p> <ol style="list-style-type: none"> 1. Click Create Custom Sender, and then enter a custom sender name. 2. Click Create and Approve.
netblock	Netblock overflows multiple custom senders (already included in the definitions of multiple custom senders).	The netblock cannot be added to an existing custom sender, nor can it be used to create a new custom sender. Different custom senders cannot include the same IP addresses or sections of netblocks. You can only Cancel.
netblock	Netblock overflows one approved custom sender (already included in the definition of one approved custom sender).	The netblock cannot be added to an existing custom sender, nor can it be used to create a new custom sender. Different custom senders cannot include the same IP addresses or sections of netblocks. You can only Cancel.
netblock	Netblock overflows one unapproved custom sender (already included in the definition of one unapproved custom sender).	The netblock cannot be added to an existing custom sender, nor can it be used to create a new custom sender. Different custom senders cannot include the same IP addresses or sections of netblocks. You can only Cancel.
netblock	Netblock overflows well-known sender(s)	<p>Add the netblock to an existing approved custom sender.</p> <ol style="list-style-type: none"> 1. Click Add to Custom Sender, and then select an existing custom sender. 2. Click Add to Approved. <p>Add the netblock to a new custom sender and approve the sender for the netblock.</p> <ol style="list-style-type: none"> 1. Click Create Custom Sender, and then enter a custom sender name. 2. Click Create and Approve.
IP address/ netblock	IP address or range entered is invalid.	No actions get enabled. Only the Cancel button can be clicked. You can re-enter a valid IP address or netblock and click Look Up again.

Add an Unapproved IP Address to a Custom Sender

It is impossible for Domain Protection to classify IP addresses used to send email that may be part of an organization's sending infrastructure, such as for dedicated mail exchange servers they own and manage to send outbound email. When Domain Protection recognizes an IP address that it cannot classify and that is not associated with a domain, that IP address is listed in the Unapproved IP Addresses section of the Senders page. For recognized IP addresses in the Unapproved IP addresses section for a given domain that are not determined to be forwarders or suspicious, you can classify these IP addresses by adding them to a Custom Sender.

1. Go to Diagnostics > Senders.
2. Click Single Domain, then select a domain. This list contains all of the domains you manage in Domain Protection.
3. Click the Unapproved tab.
4. Click the name of an unapproved IP address in the Actionable section of Unapproved IP Addresses (you may have to scroll down) to review the information about that IP address to make sure it is one you want to approve. Key things you should verify include
 - On the IP Information tab, what the hostname for the IP address is, and how many of the sent message are passing DMARC authentication. (A low number for the latter indicates configuration that needs to be done.)
 - On the Domains tab, if the domains in the From header of the messages sent from this IP address are ones you recognize and manage.
5. Click the browser's Back button.
6. If you still want to approve the IP address, click its Approve link.
7. In the Add IP Address dialog box, select a customer sender.
8. Click Add to Approved.

Ignore an Unapproved IP Address

It is impossible for Domain Protection to classify IP addresses used to send email that may be part of an organization's sending infrastructure, such as for dedicated mail exchange servers they own and manage to send outbound email. When Domain Protection recognizes an IP address that it cannot classify and that is not associated with a domain, that IP address is listed in the Unapproved IP Addresses section of the Senders page. For recognized IP addresses in the Unapproved IP addresses section for a given domain that are not determined to be forwarders or suspicious, you can choose not to work on them by adding them to the Ignored list.

1. Go to Diagnostics > Senders.
2. Click Single Domain, then select a domain. This list contains all of the domains you manage in Domain Protection.
3. Click the Unapproved tab.
4. Click the name of an unapproved IP address in the Actionable section of Unapproved IP Addresses (you may have to scroll down) to review the information about that IP address to make sure it is one you want to approve. Key things you should verify include

- On the IP Information tab, what the hostname for the IP address is, and how many of the sent message are passing DMARC authentication. (A low number for the latter indicates configuration that needs to be done.)
 - On the Domains tab, if the domains in the From header of the messages sent from this IP address are ones you recognize and manage.
5. Click the browser's Back button.
 6. If you still want to ignore the IP address, click its Ignore link.
 7. Click Add to Ignore List.

Senders Filters

You can filter the "Senders" on page 77 page by domain and by date. This topic describes the filters at the top of the Senders page.

Filter	Description
Domains	<p>Select from:</p> <ul style="list-style-type: none"> • All Domains (default): Shows all the senders that are authenticating email on behalf of all of your domains. • Single Domain: Shows all the senders that are authenticating email on behalf of the selected domain. <p>When you select a single domain, if you have the correct permissions, you can modify the SPF record of that domain.</p>
Period	<p>Select from:</p> <ul style="list-style-type: none"> • Most recent (default): Shows the senders that authenticated email during the most recent number of days you enter. • Date Range: Shows the senders that authenticated email on and between the start and end dates you select.

Nominate a Custom Sender to be a Well-Known Sender

As Domain Protection collects data on senders, you may find that your organization is using senders that are not (yet) well known to Cisco. The data about those senders is in the Custom Senders section of the Senders page.

The Custom Senders section may also have data about other senders as well, including for domains of infrastructure within your own organization and custom well-known senders.

You can nominate custom senders to be added to the list of well-known senders. If the nomination is successful, those senders also become well-known senders for other Domain Protection customers. Custom senders that can be nominated have a *Nominate* link next to their name.

Before you nominate a custom sender to be a well-known sender, you should investigate the sender, including its domain and IP address(es), to ensure its legitimacy.

1. Go to **Diagnostics > Senders**.
2. In the Customer Senders section, click **Nominate** next to the custom sender you want to nominate.
3. Enter the information about the sender.


Sender Information	Description
Sender Name	This is the name of the sender, taken from its entry. You should not change this.
Sender URL	Enter a fully-qualified URL of the sender. This URL is part of the information Cisco will use in its investigation.
Notes	Enter the reasons why you think this custom sender should be a well-known sender.
Netblocks	The section lists the IP addresses of the sender. Make sure only the IP addresses you know are associated with the sender are selected.


4. Click **Submit for Nomination**.

Convert a Custom Sender to a Well-Known Sender

When you have a custom sender with netblocks that match or overlap a well-known sender, you can convert the custom sender to a well-known sender. This can often happen when Cisco adds new well-known senders to Domain Protection and "discovers" the match.

When there is an exact netblock match, you can simply convert the customer sender to a well-known sender and delete the custom sender. When there is an overlap, that is, when just some of the netblocks in the custom sender match a well-known sender and some do not, you will have several options for which type of sender the netblocks will be assigned to. You make the choice of what to do, and Domain Protection does all the work for you.

1. Go to **Configure > Manage Custom Senders**.
2. Click on a custom sender that displays the  icon. This icon indicates that the custom sender contains netblocks that match or overlap an existing well-known sender.
3. Click:
 - Use Well-Known Sender to add the matching netblocks as a well-known sender in your organization. If the netblocks overlap, instead of being an exact match, the result will be as detailed below.
 - Keep Custom Sender to leave your sender definitions as-is.

If you choose to leave your sender definitions as is, the  icon will remain on the custom sender and you will have the option to convert to a well-known sender at any time in the future.

IP Address Overlap

There are three possible cases when custom sender netblocks overlap a well-known sender's netblocks. The table below explains what happens in each case when you select Use Well-known Sender.

Case	Result
All of the custom sender's netblocks are a subset of a well-known sender's netblocks.	The custom sender will be removed and replaced with the well-known sender in your organization.
All of a well-known sender's netblocks are a subset of the custom sender's netblocks.	A well-known sender will be added to your organization with the definition of the netblocks that match the ones in the custom sender. The custom sender will remain, but its definition will have the netblocks that matched the well-known sender removed.
Some of the custom sender's netblocks are the same as some of a well-known sender's netblocks.	

Track All Senders

Using the domains you've entered into Domain Protection (either directly or indirectly by publishing a DMARC p=none policy) and the information gathered from the Senders page from monitoring data for a period of time, you should be able to gather information about all third-party senders used by your organization.

An easy way to track this information is in an external spreadsheet. See "Example Domain-to-Senders tracking spreadsheet" below for an example.

You'll use the information in this spreadsheet to create the SPF records and DKIM keys needed for proper authentication, as well as to communicate the status of your authentication project internally.

Example Domain-to-Senders tracking spreadsheet

Domain	Sender(s)	Internal Contact	Account Details
foo.com	Marketo Zendesk CustomSender 1	bob@foo.com	
receipts.foo.com	Taleo MailChimp	jane@foo.com rita@foo.com	MailChimp account 1
newsletters.foo.com	MailChimp	john@foo.com	MailChimp account 2: Use 'jim@foo.com' credentials (former admin)
help.foo.com	Freshdesk (SendGrid)	bill@foo.com	SendGrid
sales.foo.com	Toutapp (Marketo)	alex@foo.com	Marketo account
foo.net	None (defensive)	IT@foo.com	

Domain	Sender(s)	Internal Contact	Account Details
	domain)		
fuuu.com	None (defensive domain)	IT@foo.com	

You may discover, as shown above, that different departments in your organization are using multiple accounts at the same Sender. You may also be using senders that send for multiple system types. For example, SendGrid offers mailing services and also provides mailing infrastructure for the Freshdesk CRM service.

Move to Reject

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

- "Review Your Email Traffic" on the next page
- "Review Domain Status" on the next page

Using these tools and reports, 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:

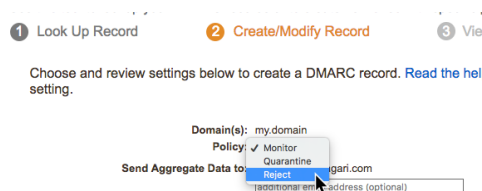
1. Obtain sign-off from all business owners.

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.

Work with the list of contacts you made in "Track All Senders" on the previous page.

2. 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 "Create a DMARC Record With DMARC Builder" on page 63. However, now that you have gained visibility you can set the policy to be Reject:



Modifying a DMARC policy to be Reject

The modified policy will contain the p=Reject notation:

1	DMARC Record
	v=DMARC1; p=reject; fo=1; ri=3600; rua=mailto:b

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.

Review Your Email Traffic

The email traffic reports in Cisco Domain Protection are one set of tools you will use to evaluate when you are ready to move to reject. Each of these reports provides valuable insight from DMARC aggregate and forensic data, and they represent the power of the Cisco Domain Protection solution. Most reports have multiple, “drill-down” views that allow you to hone in on specific mail flows and areas to address.

You can:

- Configure the view of any report. See "Configure Email Traffic Reports" on page 105 for details.
- Sort report views by clicking on any column header.
- Filter graph views by clicking on any item in the graph key to enable or disable that item in the view.
- Share and schedule any reports. See "Share an Email Traffic Report" on page 105 and "Schedule an Email Traffic Report" on page 106 for details.

See "Email Traffic Reports" on page 101 for a description of all the email traffic reports you can view.

Review Domain Status

The Diagnostics > Domains page has a detailed view for each domain. Click a domain to see its status:

Manage the settings for [redacted]

View, edit, and delete all the details for this domain.

Domain	Approved Senders		Unapproved Senders		DMARC Policy	BIMI Record	SPF		DKIM	
	#	Pass	#	Pass			Record	Pass	Key	Pass
[redacted]	27.49M	100%	3.5M	100%	... H		H	96.24%	98.64%	

Is Third Party: ☐ ?

Is Defensive: ☐ ?

Is Primary: ☐ ?

Domain Groups: All Domains ?

Senders: [redacted], Google, Unassigned ?

DMARC: Managed by Cisco ?

SPF: Managed by Cisco ?

DKIM: Not managed by Cisco ?

BIMI: Not managed by Cisco ?

Name Server (NS): [redacted] ?

Progress State: ☒ Configuration Completed ?
☐ Ready To Start
☐ I Am Working On

Date Added: 2018-04-27 ?

Notes: ?

Save Changes

Cancel

Remove [redacted] from Domain Protection

The details page for a domain

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.

Domain Setting	Description
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.
Is Primary	A primary domain is a domain that you identify as being a high priority for your project. Top candidates for a primary domain label include high email volume, ones used as brands themselves, or the domains you'd like to focus on first.
Brand Mark Identifier	If you are using BIMI and have a Brand Mark Identifier file, displays the file. If you do not, this field is hidden.
Domain Groups	A list of the domain groups that this domain belongs to.

Domain Setting		Description		
Senders		A list of the senders that have had activity with this domain recently.		
DMARC		Indicates the domain's DMARC record hosting status. DMARC records can be either hosted solely within your DNS infrastructure or hosted by Cisco's DNS servers. If your DNS servers contain a CNAME entry that points to Cisco's DNS servers for this domain, that DMARC record is considered to be hosted at Cisco. See "Host Your DMARC Records at Cisco" on page 66 for details.		
SPF		Indicates the domain's DMARC record hosting status. SPF records can be either managed solely within your DNS infrastructure or hosted by Cisco. If your published SPF record for this domain contains an include referencing " esp-f.cisco.com" , the domain's SPF record is considered to be hosted at Cisco. See " Hosted SPF" on page 39 for details.		
DKIM		Indicates the domain's DKIM record hosting status. DKIM records can be either managed solely within your DNS infrastructure or hosted by Cisco. If you publish an NS record that all point to subdomains of " hosted-dkim.cisco.com" , the domain's DKIM record is considered to be hosted at Cisco. See " Host Your DKIM Records at Cisco" on page 55 for details.		
BIMI		Indicates the domain's BIMI record hosting status. BIMI records can be either managed solely within your DNS infrastructure or hosted by Cisco. If you publish an NS record that all point to subdomains of " hosted-bimi.cisco.com" , the domain's BIMI record is considered to be hosted at Cisco. See " Host Your BIMI Records at Cisco" on page 99 for details.		
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. Use the progress state to affect the state of the Domain Progress Meter of your overall progress on the Status > Protection page:		
		<table><tr><td>Configuration Completed</td><td>When a domain is fully protected and Cisco has detected no remaining issues, it will automatically be marked as 'Configuration Completed' by Cisco. 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.</td></tr></table>	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. 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.
		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. 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.	
		<table><tr><td>I Am Working On</td><td>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.</td></tr></table>	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.
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.			
<table><tr><td>Ready To</td><td>Most domains will begin in this state. There are actions Cisco</td></tr></table>	Ready To	Most domains will begin in this state. There are actions Cisco		
Ready To	Most domains will begin in this state. There are actions Cisco			

Domain Setting		Description
	Start	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 it's progress state.
Date Added	The date the domain was approved in Cisco and added to your organization.	
Notes	A free-form text field where you can store notes about the domain. Simply add or append new text or delete existing text that is no longer relevant.	

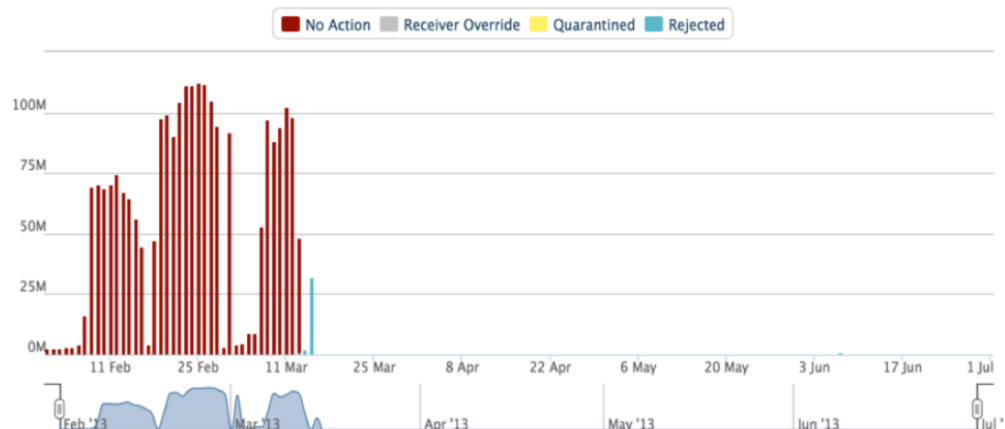


CHAPTER 5

Monitoring DMARC

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 does my DMARC trend look like? report for this Cisco customer shows that, after moving a domain to Reject policy, the spammers simply moved on and stopped attempting to spoof the domain:



The benefits of moving to Reject

Once you have moved to reject, Domain Protection keeps providing the information you need to keep you there. This is important because your email infrastructure will never be static, but it will evolve. The pages available in the Status menu will give you a lot of that information, pages that include

- Protection status
- Threat status
- Recent alerts
- Executive overview

Domain Protection provides a number of tools gives you information about your email infrastructure, including reports about your email traffic and alerts about changes in your systems. See "Email Traffic Reports" on page 101 and "Alerts" on page 113 for more information on these features.

What's Next...

This guide covers the basics of implementing a DMARC policy for your organization and getting started on monitoring once you have implemented DMARC.

Contact Cisco Support to learn more about some of the advanced features of 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 Domain Protection from an application programming interface (API) to work in conjunction with your other security tools.
- SSO Access - Enable logging into to Domain Protection from a single sign-on (SSO) capability.



CHAPTER 6

Brand Indicators for Message Identification

Brand Indicators for Message Identification (BIMI) is an emerging industry standard that will allow email receivers to display brand logos in user agents alongside DMARC authenticated messages. Email receivers can display BIMI brand logos only for senders whose domains have implemented DMARC quarantine or reject policies. The idea is to associate brand recognition with DMARC authentication.

Like DMARC (and SPF and DKIM), BIMI instructions are added to a domain's DNS records. Domain Protection simplifies the creation of BIMI instructions for one or more domains by providing a workflow with validation. If Cisco hosts your BIMI records, Domain Protection also automates the management of the logos being displayed.

The RFC for Brand Indicators for Message Identification is currently (as of mid 2019) in draft state with the IETF (Internet Engineering Task Force), which you can read at <https://datatracker.ietf.org/doc/draft-blank-ietf-bimi/>. However, it is both thorough and specific and is already being adopted. This draft specifies the BIMI mechanism as follows:

Domain owners publish brand indicator assertions for domains via DNS.

Then, for any message received by a mail receiver:

- a. Receivers authenticate the messages using DMARC, as well as internal reputation indices and other proprietary authentication mechanisms they wish to apply.
- b. The receiver queries the DNS for a corresponding BIMI record and proof of indicator validation.
- c. If both the email and the logo authenticate, then the receiver adds a header to the message, which can be used by the MUA (mail user agent) to determine the domain owner's preferred brand indicator.

The MUA retrieves and displays the brand indicator as appropriate based on its policy and user interface.

The proof of indicator validation is provided by a Mark Verified Certificate.

BIMI Record Syntax

BIMI records (assertion records) are DNS TXT records in subdomains named `_bimi` and follow the tag-value syntax for DNS-based key records. BIMI records are constructed with the following tags:

Tag Description		Value(s)	Notes
v=	Version.	BIMI1	This tag is required. It MUST have the value of BIMI1 for implementations compliant with this version of BIMI. The value of this tag MUST match pre-

Tag Description		Value(s)	Notes
			cisely; if it does not or it is absent, the entire retrieved record MUST be ignored. It MUST be the first tag in the list.
a=	BIMI trust authorities.	<ul style="list-style-type: none"> • self • cert • mva 	<p>These options are not yet available and the a= tag should be left blank (as a=) or not included.</p> <p>This tag is optional and takes one of the three values. The values represent:</p> <ul style="list-style-type: none"> • self - No validation option (the same as omitting the tag). • cert - An https URL to a Mark Verified Certificate that can be used to validate the indicator. • mva - An https URL to an API endpoint that can be queried for validation information.
l=	URL(s) to image resource(s).	http URL	<p>This tag is required, but its value may be empty. The tag is a lowercase "L." The image resource must be an SVG (scalable vector graphics) file. The protocol must be https.</p> <p>The graphic file should conform to:</p> <ul style="list-style-type: none"> • Square • SVG • White/transparent background • Logo/mark centered and as large as possible in the space • Iconography instead of text

An example BIMI record:

v=BIMI1; a=; l=https://www.mycompany.com/bimi/brandlogo.svg;

A BIMI record can be used to indicate refusal. From the recommendation:

If both the "a" and "l" tags are empty, it is an explicit refusal to participate in BIMI. This is critically different than not publishing a BIMI record in the first place. For example, this allows a subdomain to decline participation when its organizational domain has default Indicators available. Furthermore, messages sent using a selector that has declined to publish will not show an Indicator while messages with other selectors would display normally.

An explicit declination to publish looks like:

v=BIMI1; a=; l=;

The BIMI record syntax is exact, including capitalization. Mail receivers are not allowed to attempt fixing syntax or capitalization errors in BIMI records. Missing required tags are errors. Records that do not start with a v= tag, or that start with a v= tag that does not identify the current BIMI version must be discarded.

BIMI Implementation

While the recommendation is rigid in how BIMI DNS records are formed, it is flexible in how BIMI can be implemented. Domain owners can ask that receivers display brand indicators, but receivers have the option to display them or not, or even to display alternate indicators. From the recommendation:

A Domain owner advertises BIMI participation of one or more of its domains by adding a DNS TXT record to those domains. In doing so, domain owners make specific requests of MUAs regarding the preferred set of indicators to be displayed with messages purporting to be from one of the domain owner's domains.

A domain owner may choose not to participate in BIMI. In this case, the domain owner simply declines to advertise participation by not publishing any BIMI assertion record.

An MUA implementing the BIMI mechanism SHOULD make a best-effort attempt to adhere to the domain owner's published BIMI policy. However, MUAs have final control over the user interface published to their end users, and MAY use alternate indicators than those specified in the BIMI assertion record or no indicator at all.

The BIMI record should be published in a zone named `default._bimi`, located directly under the second-level domain. For example, if the desired second-level domain is `foo.com`, the BIMI TXT record for that domain would be published at `default._bimi.foo.com`.

Create a BIMI Record

You can create a BIMI record in Domain Protection only for domains (and sub-domains) that you manage in Domain Protection. To review the domains you manage in Domain Protection, go to **Configure > Manage Domains**, and then click **All Domains**, and go to **Configure > Unverified Domains**.

Prerequisites

- A brand logo file in SVG (scalable vector graphics) format in a location accessible by a secure (https) URL.
- The URL to the above.

1. Go to **Tools > BIMI**.
2. Enter a domain or sub-domain that you manage in Domain Protection.
3. Click **Look Up**.
4. Click **Create New BIMI Record**.
5. Enter a Brand Mark Identifier value. This is a fully qualified https URL to a resource, which must be an SVG (scalable vector graphics) file, and click **Apply**.
6. Enter an optional BIMI Certificate value. This is a fully qualified https URL to a certificate or an API that can be queried for validation, and click **Apply**.
7. Click **Continue**.
8. Click **Create Instructions**.

A text file with the extension .txt will be downloaded to your computer. Where it is saved will depend on the default file download location you have set in your browser. The file will contain instructions for what DNS records should be added to the domain and the exact TXT record for BIMI that you can copy and paste.

Edit a BIMI Record

You can change the graphic resource you use for your BIMI record (which must be a scalable vector graphics (SVG) file) and the URL to a BIMI Trust Authority. See "Brand Indicators for Message Identification" on page 95 for more information on these values.

1. Go to Tools > BIMI.
2. Enter a domain or sub-domain that you manage in Domain Protection and that has a BIMI record.
3. Click Look Up.
4. Click Modify BIMI Record.
5. Make any desired changes.
 - In the Brand Mark Identifier field, enter a fully qualified URL to an SVG graphic resource and click Apply.
 - In the BIMI Certificate field, enter an optional https URL to a certificate or API endpoint and click Apply.
 - To remove a value, leave that field blank and click Apply.
6. Click Continue.
7. Click Create Instructions.

A text file with the extension .txt will be downloaded to your computer. Where it is saved will depend on the default file download location you have set in your browser. The file will contain instructions for what DNS records should be added to the domain and the exact updated TXT record for BIMI that you can copy and paste.

Preview Your Brand Mark Identifier

Once you have published your BIMI record, you can preview from within Domain Protection what your Brand Mark Identifier will look like in some email clients.

1. Go to Configure > Manage Domains.
2. Go to Manage > BIMI.
3. In the Brand Mark Identifier column, click on a BIMI graphic.

Host Your BIMI Records at Cisco

Allowing Cisco to host your BIMI (Brand Indicators for Message Identification) records means that when you make changes in Domain Protection that affect any BIMI records, the records are updated quickly, securely, and automatically.

You can host a domain's BIMI record at Cisco at any time, but mail receivers are not allowed to display BIMI brand images unless the domain is at DMARC quarantine or reject.

1. Go to Configure > Manage Domains.
2. Click All Domains.
3. Select one or more domains.
4. Click Manage > BIMI.
5. Click Host BIMI Record at Cisco.

Create and Manage BIMI records

Use this tool to lookup your BIMI records or to create new ones.

- 1 Look Up Record 2 Create/Modify Record

All selected domains will not be hosted by Cisco.

Host BIMI Record @ Cisco

6. Click Continue.
7. Click:
 - Apply next to a single domain to host the BIMI record for that domain at Cisco.
 - Apply All to host the BIMI records for all the domains at Cisco.

Stop Hosting Your BIMI Records at Cisco

1. Go to Configure > Manage Domains.
2. Click All Domains.
3. Select one or more domains.
4. Click Manage > BIMI.
5. Click Do Not Host BIMI Record at Cisco.

Create and Manage BIMI records

Use this tool to lookup your BIMI records or to create new ones.

- 1 Look Up Record 2 Create/Modify Record

All selected domains will be hosted by Cisco.

Do Not Host BIMI Record @ Cisco

6. Click Continue.

7. Click:

- Apply next to a single domain to host the BIMl record for that domain at Cisco.
- Apply All to host the BIMl records for all the domains at Cisco.



CHAPTER 7

Monitor Your Outgoing Messages

Once you have moved all of the domains that send email on your behalf to reject, you can use Domain Protection to monitor your outgoing mail. Domain Protection provides visibility not only into the messages you explicitly send and the mail that others send on your behalf, but also messages that purport to be from you and are not, enabling you to discover and act on campaigns that attempt to damage your brand.

Email Traffic Reports

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 and shows you both a graphical representation and a list of the information in each report.

When viewing the reports, you can:

- Hover over the sections of the graphical representation to see pop-up capsule summaries of the specific data presented.
- Click on a section of the graphical representation to filter by that subset of data.
- Click on any link in the list to filter by that subset of data.
- "Share an Email Traffic Report" on page 105
- "Schedule an Email Traffic Report" on page 106

Available Reports

Domain Protection provides a variety of reports for your outbound email traffic.

The following table indicates the reports available for you to view. Reports are categorized into three types.

List of email traffic reports.

Report Name	
The Big Picture	
What does my DMARC trend look like?	
What's happening to messages failing DMARC?	
What messages pass DMARC with SPF & DKIM?	

Report Name	
Which ISPs do I send email to?	
How much email using my domains is legitimate?	
Things I Can Fix	
What are my SPF problems?	
What are my DKIM problems?	
Are any legitimate messages being rejected?	
What legitimate subdomains don't I know about?	
Who is Spoofing Me?	
How much spoofed email am I blocking?	
What subdomains are being used to spoof me?	

You can adjust the filter options for every report to help you get to the information you need. 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. It is recommended to increase the date range, for example to 90 days, to see trends and patterns in your sending. (For example, 2 weeks is too short of a time span to see data from 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.

See "Configure Email Traffic Reports" on page 105 for more details on how you can customize email traffic report views.

When you're just getting started monitoring your email traffic in Domain Protection, you could get useful information by reviewing the following reports first:

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 is passing DMARC checks so that you can move to a Reject policy with confidence.

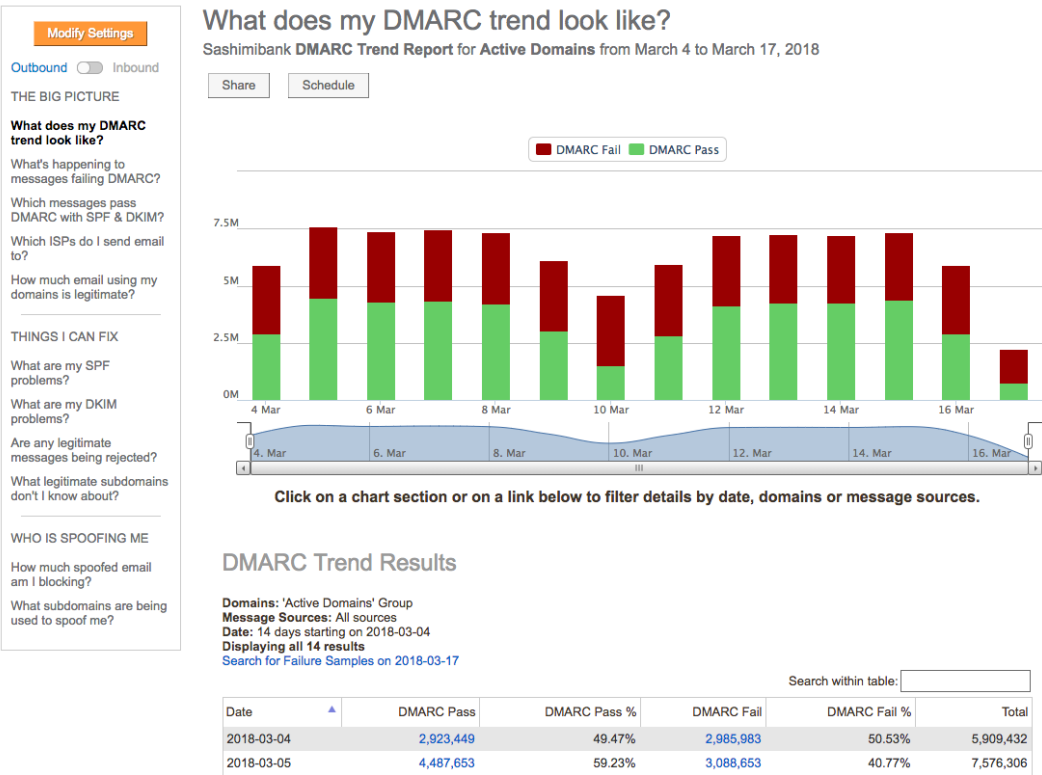
A great place to start monitoring data is with the default view: the What's My DMARC Trend Look Like? report.

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

Drill into 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.



The What's my DMARC Trend Look Like? view for the Active Domains group.

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.

What are my SPF problems?, What are my DKIM problems?

As discussed in "Identify SPF Problems" on page 35 and "Find DKIM Problems" on page 57, you can use these reports to drill into details about SPF and DKIM authentication progress and problems for any domain.

Are any legitimate messages being rejected?

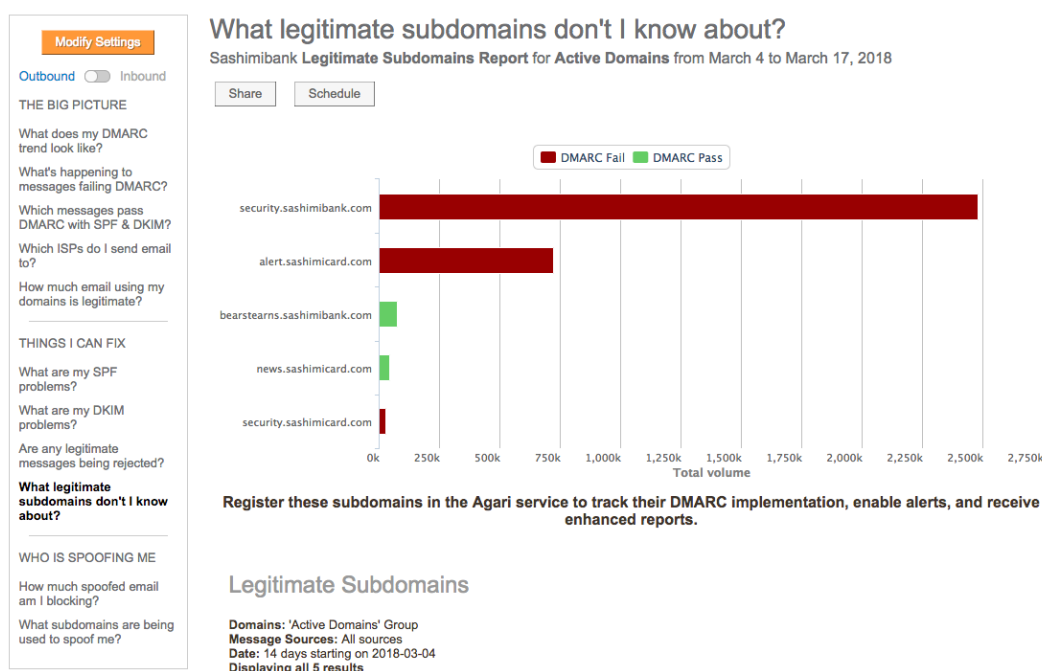
Use this report to determine if any false positives are being rejected at receivers due to your DMARC policy.

What Legitimate Subdomains Don't I Know About?

Use this report to discover subdomains being used to send messages for your organization.

This is another useful view in the initial stages of monitoring.

The results of this view may shed light on subdomains of your primary domain that may be being used to send email.



The "What legitimate Subdomains don't I know about?" view.

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

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 Domain Protection to work towards a DMARC reject policy.

Configure Email Traffic Reports

When you're viewing any outbound or inbound email traffic report, you can configure that report to help you get to the information you need.

1. In the left column of the Email Traffic Reports page (Analyze > Email Traffic), click the name of a report and select Outbound or Inbound.
2. Click Modify Settings.
3. Make any desired changes to the report. See "Email Traffic Report Settings" on the next page for details.

Click Reset to Defaults to remove any custom configuration and return the report to its default settings.

4. Click Submit.

Share an Email Traffic Report

On the Email Traffic page (Analyze > Email Traffic), you can share any report with any Domain Protection user.

1. In the left column, click the name of the report you want to share.
2. If you want the report to be different from what you are currently viewing, configure the report.
 - a. Click Modify Settings.
 - b. Change the report settings. See "Email Traffic Report Settings" on the next page for details.
 - c. Click Submit.
3. Click Share.
4. In the To field, select the Domain Protection users you want to receive the report.
5. In the Include list, select the formats that you want included in the report. The default is a link to the report, plus a PDF (Adobe Acrobat) file attached to the email.
6. Optionally add any free-form notes.
7. Click Send Email.

Keep in mind that all scheduled reports maintain their scope as defined in the "Email Traffic Report Settings" on the next page dialog box when the report is created. 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.

Schedule an Email Traffic Report

On the Email Traffic page (Analyze > Email Traffic), you can schedule any report to be sent to any Domain Protection user at an interval you define.

1.

In the left column, click the name of the report you want to share.
2.

If you want the report to be different from what you are currently viewing, configure the report.

a.

Click Modify Settings.

b.

Change the report settings. See "Email Traffic Report Settings" below for details.

c.

Click Submit.
3.

Click Schedule.
4.

In the Send field, select when you want the report sent. (Reports are sent at midnight local time.)

Select from:

•

Daily: The report will be sent every day.

•

Weekly: The report will be sent on the day of the week you select. The default is Mondays.

•

Monthly: The report will be sent on the day of the month you select. The default is the 1st.
5.

In the Include list, select the formats that you want included in the report. The default is a PDF (Adobe Acrobat) file attached to the email.
6.

In the To field, select the Domain Protection users you want to receive the report. The default is the scheduled report's creator.
7.

In the Owner field, select the Domain Protection user you want identified at the report owner. The default is the scheduled report's creator.
8.

Optionally change the report Name.
9.

Click Schedule.

Keep in mind that all scheduled reports maintain their scope as defined in the "Email Traffic Report Settings" below dialog box when the report is created. 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.

Email Traffic Report Settings

This section describes the settings you can define for viewing all of the different email traffic reports. Once you define a view, you can use it when you "Share an Email Traffic Report" on the previous page or "Schedule an Email Traffic Report" above an email traffic report.

Setting	Description
Select	Determines which domains are in the report. Select from:

Setting	Description								
Domains	<ul style="list-style-type: none"> Domain Group (default), then select a System Domain Group (Active Domains is the default) or a Custom Domain Group (a domain group you created). Single Domain, then select one of the domains you monitor. 								
View Messages From	<p>Determines the time period of the report. Select from:</p> <ul style="list-style-type: none"> Most Recent (default), then enter a number of days back from when the report will be generated. (14 is the default.) Date Range, then select a start and end date. <p>Reports cannot cover a range longer than 428 days. That means you cannot enter a number larger than 428 in the Most Recent field nor select Date Range dates that are farther than 428 days apart.</p>								
Message Grouping*	<p>Defines how report data is grouped: daily (default), weekly (available if a report range is 30 days or longer), or monthly (available if a report range is 90 days or longer). The grouping will apply to both the graph and the table below the graph. Grouping (or not grouping) data gives you insight at different levels and at granularity useful for the report time period. For example, for an annual report, grouping data into weekly or monthly chunks could give you a better view of any yearly trends than a daily view.</p>								
Message Origin	<p>Allows you to filter the messages in the report by several origin characteristics. Select from:</p> <ul style="list-style-type: none"> Default (default): The sources, forwarders, and IP addresses/CIDRs defined as default in the Custom setting. Custom: Select one of the following custom filters: <table border="1"> <thead> <tr> <th>Filter</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Specific Sources (default)</td><td> <p>Limits the report to specific sources. Select from:</p> <ul style="list-style-type: none"> From All Sources (default): The report will include all messages. From Inside My Sender Inventory: The report will include all messages from sources in your sender inventory (default) or messages from a single sender from the list of senders in your sender inventory. From Outside My Sender Inventory: The report will include all messages from sources outside your sender inventory (default) or messages from a single sender from the list of senders outside your sender inventory. <p>You can also select to exclude Known Forwarder IP Addresses from the report.</p> </td></tr> <tr> <td>Known Forwarders</td><td>Limits the report to only messages from Known Forwarder IP addresses.</td></tr> <tr> <td>Specific IP/CIDR Range</td><td>Limits the report to only messages from specific IP addresses, IP address ranges, or CIDRs. Enter one or more, separated by commas.</td></tr> </tbody> </table>	Filter	Description	Specific Sources (default)	<p>Limits the report to specific sources. Select from:</p> <ul style="list-style-type: none"> From All Sources (default): The report will include all messages. From Inside My Sender Inventory: The report will include all messages from sources in your sender inventory (default) or messages from a single sender from the list of senders in your sender inventory. From Outside My Sender Inventory: The report will include all messages from sources outside your sender inventory (default) or messages from a single sender from the list of senders outside your sender inventory. <p>You can also select to exclude Known Forwarder IP Addresses from the report.</p>	Known Forwarders	Limits the report to only messages from Known Forwarder IP addresses.	Specific IP/CIDR Range	Limits the report to only messages from specific IP addresses, IP address ranges, or CIDRs. Enter one or more, separated by commas.
Filter	Description								
Specific Sources (default)	<p>Limits the report to specific sources. Select from:</p> <ul style="list-style-type: none"> From All Sources (default): The report will include all messages. From Inside My Sender Inventory: The report will include all messages from sources in your sender inventory (default) or messages from a single sender from the list of senders in your sender inventory. From Outside My Sender Inventory: The report will include all messages from sources outside your sender inventory (default) or messages from a single sender from the list of senders outside your sender inventory. <p>You can also select to exclude Known Forwarder IP Addresses from the report.</p>								
Known Forwarders	Limits the report to only messages from Known Forwarder IP addresses.								
Specific IP/CIDR Range	Limits the report to only messages from specific IP addresses, IP address ranges, or CIDRs. Enter one or more, separated by commas.								

* The Message Grouping setting is available only for the following reports:

- What does my DMARC trend look like?
- What's happening to messages failing DMARC?
- Which messages pass DMARC with SPF & DKIM?
- How much email using my domains is legitimate?
- Are any legitimate messages being rejected?
- How much spoofed email am I blocking?

Threat Feed

The Threat Feed in Domain Protection is where DMARC failures based on RUF data is detailed. You can use the information in the Threat Feed to help you identify threat campaigns and commonalities in failure samples.

The Threat Feed is a list of DMARC failure samples. Each sample contains specific information passed into the reporting environment about a message that did not pass DMARC from messages sent from one of your domains or from messages not sent from one of your domains but that contain a brand identifier.

You can use the Threat Feed to:

- Identify campaigns by using the filters to see failure samples with commonalities, such as the same IP address or subject.
- Identify URLs in messages that fail DMARC.
- Use the API endpoint to have your SIEM system correlate with email data.

The table on the Threat Feed page lists the following for each Threat Feed item:

- Count: The number of times the URL has been seen in the Threat Feed.
- URI: The specific URL in the message.
- From Domain/Email Source IP: The domain in the From header and the IP address that represents that domain.
- Subject: The Subject from the message header.
- Last Reported: The date and time that the threat was most recently reported.
- Detected By: How the threat was detected. Visible only if the Include detected by: threat source in feed emails setting is enabled. See "Threat Feed Settings" on page 111 for details.

Each row in the Threat Feed table represents a URL found in a failure sample. You may see a unique URL represented multiple times (indicated by a Count value greater than 1) in messages from the same domain and with the same subject, and you may see several URLs found messages from the same domain and with the same subject (indicated by duplicate values in the From Domain/Email Source IP and Subject columns).

Configure the Threat Feed

1. Go to Analyze > Threat Feed.
2. Click Configure your Threat Feed.
3. Select the Threat Feed settings. See "Threat Feed Settings" on page 111 for details.
4. Click Done.

Whitelist a URL

You can whitelist a URL directly from the URL list in the Threat Feed. Whitelisting a URL means that messages containing that URL will no longer be added to your Threat Feed.

1. Go to Analyze > Threat Feed.
2. Click on a URL in the URI column.
3. Click:
 - ...root domain or its subdomains - to whitelist all URLs that contain the root domain. You might choose this for a shared service domain such as Facebook, where you would want to whitelist your_company.facebook.com while not whitelisting all facebook.com URLs.
 - ...exact path, excluding the query string - to whitelist only the specific URL. You might choose this when you know a specific fully qualified URL and path, such as facebook.com/safestuff, is good but you still want messages that contain only facebook.com to be considered for the Threat Feed.

The URL turns green to indicate it has been whitelisted.

View a Failure Sample

1. Go to Analyze > Threat Feed.
2. Click a link in the Subject column.


1	Ⓢ http://luismachado.site/aquinasb.php	abc25.com 176.56.63.104	USPostalService ticket #2379	2019-11-21 08:30	DMARC Failure
13	Ⓢ http://mteestore.com/untyingh.php	abc25.com 189.84.159.67	USPostalService ticket #5977	2019-11-22 06:31	DMARC Failure
11	Ⓢ http://lintastoday.com/peninsulasqp.php	abc25.com 103.129.220.253	USPostalService ticket #83624	2019-11-22 06:31	DMARC Failure

This URL appeared in 13 messages with the same From Domain/Email Source IP and Subject.

Understand your top failures

Samples	Subject	From	Timeframe	# of IPs
1	USPostalService ticket #5977	USPS <corne@abc25.com>	less than a minute	1

Dig into the details of specific failed messages

Origin	Source	SBRS	SPF	DKIM	DMARC SPF	DKIM	Time
	189.84.159.67 (pop3.3ax.com.br)	-10.0	Fail	None	Fail	Fail	2019-11-22 06:30
SPF Issue: domain of abc25.com does not designate 189.84.159.67 as permitted sender DKIM Issue: message does not contain a DKIM signature Mail From Domain: abc25.com From: USPS <corne@abc25.com> Subject: USPostalService ticket #5977							
Share this sample							
Source: Yahoo!							
Additional Headers Received-SPF: fail (domain of abc25.com does not designate 189.84.159.67 as permitted sender) Date: Fri, 22 Nov 2019 04:30:10 -0600 (CST) Message-ID: <164814.467151.9974.JavaMail.wsadmin@abc25.com>							
URLs (5) http://mteestore.com/untyingh.php http://usps.com http://www.usps.com/ https://reg.usps.com/forgot https://www.usps.com/global-elements/header/images/utility-header/logo-sb.svg							

The failure sample contains several URLs. This one was identified as a threat, and is the same one that appears in the Threat Feed list. You can also see that the message did not pass SPF or DMARC, and did not have a DKIM signature.

Share a Failure Sample

You can share a failure sample with others in your organization for them to analyze.

- Go to Analyze > Threat Feed.
- Click a link in the Subject column.
- Click:
 - Share (button at the top of the page) - to share the entire failure report, which can contain multiple messages
 - Share this sample (link in a specific message) - to share just that message from the failure report
- In the Share Report dialog box, select what to include:
 - Link (selected by default) - the link to the failure sample report included in the message
 - PDF (selected by default) - a generated Adobe Acrobat version of the report attached to the message
 - CSV - a comma-separated values version of the report attached to the message in a text file
 - Enter any Additional Notes. This is a free-form field where you can enter information that you think will be useful to the report's recipients.

You cannot add or delete email addresses from the To: field. The failure sample report will be sent to all Domain Protection users.

5. Click Send Email.

Threat Feed Settings

Setting	Description
Enable Threat Feed	Enables or disables the Threat Feed entirely. This setting is enabled by default.
Resubmit threats which are seen again after	<p>Determines when URIs that are seen repeatedly in authentication failure samples will be resubmitted to your Threat Feed. Select from:</p> <ul style="list-style-type: none"> • 2 weeks (default) • 1 month • 3 months <p>If your Threat Feed contains a significant number of false positive (in most cases, legitimate) or junk/spam URLs, the latter not being actual threats and typically not requiring action, you may want to choose one of the longer durations. The default 2 week period is good for most organizations so you can see if there are URLs for which you missed taking necessary action, especially if you use a take-down vendor that charges by the link and limits the time by contract for you to take action.</p>
Signal strength	<p>Determines what threats are included in the Threat Feed. Select from:</p> <ul style="list-style-type: none"> • Send all threats - Includes both URIs spoofing brand and threats failing DMARC. Recommended setting for highest signal strength. • Send all threats with brand identifiers - Includes only URIs with brand identifiers. • Send all DMARC failure threats (default) - Excludes URIs with brand identifiers.
Include detected by: threat source in feed emails	Determines if the Detected By column will appear in the Threat Feed table. The Detected By column separates threat feed submissions into their threat source, which can be from DMARC data or Brand Spoofs.
Exclude URIs on the Domain Protection Whitelist	Domain Protection maintains a global whitelist of known legitimate URI patterns. This setting determines if the whitelisted URIs appear in your Threat Feed. Select it (the default value) to ensure that URIs matching these patterns are not submitted on your Threat Feed.
Exclude URIs on my Whitelist	You can add a URI to a whitelist for your organization. This setting determines if these whitelisted URIs appear on your Threat Feed. Select it (the default value) to ensure that URIs matching these patterns are not submitted on your Threat Feed.
Exclude URIs from sources with an SBRS threshold greater than	<p>SBRS is a reputation score for the source IP address of an email message. SBRS values range from -10 (worst) to +10 (best). You can exclude URIs extracted from messages whose source has an SBRS above a designated threshold. The default value is 0.</p> <p>You might choose, for example, to have your Threat Feed ignore any URIs com-</p>

Setting	Description
	ing from messages where the source has a highly positive SBRS.
Send Threat Feed to email recipients	<p>Determines if items in your Thread Feed will be sent to the recipients you designate. Enter a comma-separated list of valid email addresses. This list should include the email address of any take down vendors that you wish to directly receive your Threat Feed.</p> <p>This email feed is potentially high volume. It is recommended for automated processing and not a personal email address.</p> <p>These email messages will contain malicious URIs. You should whitelist these messages from your anti-spam and anti-virus filters.</p> <p>Threat Feed email messages:</p> <ul style="list-style-type: none"> Will come from a source IP address in the following ranges 199.255.192.0/22, 199.127.232.0/22, 54.240.0.0/18 Will use a From header email of Cisco <no-reply@cisco.com> Will use the Subject line you designate in the Subject of feed emails: field
Include header From: domains in feed emails	<p>Determines if the From: header domain used in the message the URI was extracted from will be included in the Threat Feed email. The default is not selected.</p> <p>This can provide additional information about which domain the abuse was from. In general, you will want to enable this option unless it breaks automated processes with tolls or third-party services you use.</p>
Include Subject: lines in feed emails	<p>Determines if the Subject line used in the message that the URI was extracted from will be included in the Threat Feed email. The default is not selected.</p> <p>This can provide additional information about abuse messages, such as subject commonalities. For example, subjects that all contain viagra" or "accounts." In general, you will want to enable this option unless it breaks automated processes with tolls or third-party services you use.</p>
Subject of feed emails	<p>Determines the Subject line of Threat Feed emails. This can help you to filter these messages and direct them to specific folders.</p> <p>The default is " Cisco threat feed for Cisco, Inc.."</p>
Whitelist header From: domains	<p>Determines if URIs contained in messages that use specific domains in the From header are omitted from your threat feed. Enter valid domain names in a comma separated list to exclude URIs in messages from these domains.</p> <p>For example, the domain email.mycorp.com is used by your corporate employees to send email. The authentication failures from this domain tend contain a lot of valid URLs and you don't want to include any URLs in messages from email.mycorp.com in your organization's Threat Feed. You should select this option and enter email.mycorp.com in the text field.</p>
Send threat feed to Internet Identity (target to provide IID: 'Cisco, Inc.')	<p>If your takedown vendor is Internet Identity (IID, now Infoblox), you can select this option to submit your Threat Feed directly to IID without sending Threat Feed emails. The default is not selected.</p>

Alerts

Cisco Domain Protection generates alerts for numerous events, events that include spikes in threats or authentication failures, new senders and brand spoofs, and changes in your customer senders and your SPF, DKIM, and DMARC records. These alerts can provide the information you need to maintain the authentication status of all your domains. You can:

- "View Alerts" on the next page
- "Subscribe to Alerts" on page 115
- "Configure Alerts" on page 116

Alert Types

This topic describes all of the alerts that Domain Protection generates. Alerts are sent per their respective frequency if there is any new content to report on the subject of any alert.

Alert	Frequency	Configurable	Description
Authentication Failure Spike	Hourly	<ul style="list-style-type: none"> • Threshold • Exceptions 	The volume of DMARC failure samples received in the last hour, originating from your Sender Inventory, has exceeded a pre-set statistical threshold. This may indicate a serious SPF, DKIM, or identifier alignment problem in your email infrastructure or at an authorized 3rd party sender. This alert evaluates failure sample data each hour for your Active domains.
Brand Spoofing Alert	Hourly	No	Messages from a domain not owned by you that are potentially spoofing your brand. These messages are not protected by your DMARC policy. This alert evaluates non-DMARC data each hour for new brand spoofing threats.
Custom Sender Changed	On event	No	Due to a change in your Sender Inventory a custom sender IP range has been modified.
DKIM Record Change	Daily	<ul style="list-style-type: none"> • Exceptions 	DKIM record(s) has changed related to one of your domains.
DMARC Record Changed	<ul style="list-style-type: none"> • Hourly (active domains) • Daily (defensive domains) 	<ul style="list-style-type: none"> • Exceptions 	A DMARC record changed for one of your domains.
Infrastructure Alert	Daily	<ul style="list-style-type: none"> • Threshold • Exceptions 	The percentage of messages failing either DMARC-DKIM or DMARC-SPF from any

Alert	Frequency	Configurable	Description
			server in your sender inventory that is higher than the normal daily failure percentage. The difference in the overall failure percentage on the alert date for the server must be at least 10.0 percentage points higher than the overall failure percentage on a normal day. This alert contains DMARC aggregate data for all of your active domains.
New DKIM Selector	Daily	<ul style="list-style-type: none"> Exceptions 	New DKIM selector(s) has been found related to one of your domains.
New Sender Alert	Daily	<ul style="list-style-type: none"> Threshold Exceptions 	A sender outside your sender inventory has been sending for your domain.
New Well-known Sender	Daily	No	A new well-known sender overlaps with your custom sender.
SPF Record Changed	Daily	<ul style="list-style-type: none"> Exceptions 	An SPF record (or include) changed for one of your domains.
Threat Spike	Hourly	<ul style="list-style-type: none"> Threshold Exceptions 	The volume of DMARC failure samples received in the last hour originating from outside of your sender inventory that has exceeded a preset statistical threshold. This may indicate the start of a phishing attack against the domain in the alert.
Unauthorized Netblock	Daily	No	Messages from a Well-known Sender using an unspecified IP address have been detected.

View Alerts

1. Go to Status > Alerts.

You will see a list of all alerts that have been triggered in the default view, which is

- The past week
- All your domains
- All alert types

You can filter the list of alerts.

Filter the Alerts List

1. Change any of the following fields above the table to filter the list of alerts, and then click Go to apply the filters.

From: 2018-08-02 To: 2018-08-09 ¹

All Domains ² All Alert Types ³ Go ⁴ Search by ID or Domain

Alert Filter	Description
1: From and To dates	The default is one week prior to the current date, that is, the To date is the current date and the From date is the date one week prior to the current date. Click in either field to select a different date for the start or end date.
2: Domain groups	The default is All Domains. Click in the field to select one or more system or custom domain groups to restrict the list to alerts only for domains in those groups. Note that if you select one or more system or custom domain groups, you should remove the All Domains item. Otherwise, Domain Protection will still display alerts for all domains in the list.
3: Alert types	The default is All Alert Types. Click in the field to select one or more alert types to restrict the list to alerts only of those types. Note that if you select one or more alert types, you should remove the All Alert Types item. Otherwise, Domain Protection will still display alerts for all alert types in the list.
4: ID or domain	You can enter a specific alert ID to see only that alert in the table or a specific domain to see all alerts for that domain in the table. As you type , the items in the table get filtered for each character you enter.

Subscribe to Alerts

As an alternative to viewing alerts in Domain Protection, you can subscribe to any alert type. A subscription to an alert type will send you an email whenever an alert is triggered of that alert type with the contents of the alert.

1. Go to Status > Alerts.
2. Click Manage My Subscriptions.
3. Move the slider right for any alert type you want to subscribe to. Your selection is saved automatically.

Unsubscribe to Alerts

1. Go to Status > Alerts.
2. Click Manage My Subscriptions.
3. Move the slider left for any alert type you want to unsubscribe from. Your selection is saved automatically.

Configure Alerts

Only users who have the Organization Administrator role can configure alerts.

For all alert types except Brand Spoofing and Custom Sender Changed, you can exclude domain groups.

For Authentication Failure Spike, Infrastructure Alert, New Sender Alert, and Threat Spike alert types, you can also configure the alert threshold.

You should be cautious when changing the configuration of an alert type:

- Make sure any domain groups you select in the Exception List do not include domains that you need to see this type of alert for. If you're not sure, review the domains in all your domain groups before excepting any domain group.
- Make sure any Threshold amount does not affect when you need to be alerted. For example, a too-small threshold may generate so many alerts that you tune them out and miss ones that you need to act upon, and a too-large threshold may not generate an alert for a situation that requires your action.

To configure an alert

1. Go to Status > Alerts.
2. Click Manage Organization Alert Settings.
3. Click the Alert Type Settings tab.
4. Click the Edit (Threshold and) Exceptions link for an alert type.
5. Make any desired changes. See the Alert Configuration Options section below for details.
6. Click Save.

Alert Configuration Options

All alert types that can be configured can exclude one or more domain groups in an exception list. Some alert types can also have thresholds defined for one or more domain groups.

Exception List

Alerts are not triggered for any domains in any domain group in the Exception List.

In the Domain groups to exclude field, click in the field and select one or more system or custom domain groups from the drop-down list.

Do not select All Domains. Doing so means that all domains are excepted from that alert type, and no alerts of that type will be triggered.

Threshold

Enter a threshold amount (the default is 100), then click in the Domain Groups field and select one or more domain groups from the drop-down list.

Click + Add another threshold to add additional thresholds for more domain groups.

Manage Organization Alert Subscriptions

You can manage (subscribe and unsubscribe) subscriptions for all of the Domain Protection users in your organization. Only users who have the Organization Administrator role manage subscriptions at an organization level.

1. Go to Status > Alerts.
2. Click Manage Organization Alert Settings.
3. Click the Subscribers tab.
4. For any user, click an alert type slider to the right to subscribe that user to that alert, and click an alert type slider to the left to unsubscribe that user to that alert. Selections are saved automatically.

Domain Groups

Domain Protection allows you to group domains in a customizable 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 Domain Protection.

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

Manage your Domains



Edit or delete domains, create Custom Domain Groups, add or remove domains from Custom Domain Groups.

All of the verified domains that you have access to in your organization.

System Domain Groups		Search Domains	Manage	Edit	Add to Domain Group	
		<input checked="" type="checkbox"/>	Domain	DMARC	DMARC Hosted	Date Added
All Domains	25	<input checked="" type="checkbox"/>	agaribank.com	No DMARC	No	2014-02-13
Active Domains	16	<input checked="" type="checkbox"/>	alerts.sashimibank.com	Reject	No	2014-02-14
Defensive Domains	9	<input checked="" type="checkbox"/>	anthony.com.au	No DMARC	No	2017-02-08
Monitor Policy	6	<input checked="" type="checkbox"/>	cheese.sashimibank.com	Reject	No	2019-05-16
Quarantine Policy	1	<input checked="" type="checkbox"/>	corp.sashimibank.com	Quarantine	No	2014-02-14
Reject Policy	6	<input checked="" type="checkbox"/>	corp.sashimisavings.com	Reject	No	2019-03-29
No DMARC	12	<input checked="" type="checkbox"/>	ibd.sashimibank.com	Reject	No	2014-02-24
Third Party	3	<input checked="" type="checkbox"/>	jobs.sashimibank.com	Monitor	No	2014-02-14
DMARC Hosted by Agari	0	<input checked="" type="checkbox"/>	mortgage.sashimibank.com	DMARC Error	No	2014-02-14
SPF Hosted by Agari	4	<input checked="" type="checkbox"/>	offers.sashimibank.com	Monitor	No	2014-02-14
DKIM Hosted by Agari	1	<input checked="" type="checkbox"/>	pwm.sashimibank.com	Monitor	No	2014-02-14
Primary Domains	0	<input checked="" type="checkbox"/>	sashimibank.com	Monitor	No	2014-02-13
Custom Domain Groups		<input checked="" type="checkbox"/>	sashimicard.com	No DMARC	No	2014-02-13
Bank group	1	<input checked="" type="checkbox"/>	sashimisavings.com	Reject	No	2019-03-01
Cards	1	<input checked="" type="checkbox"/>	sochi.sashimibank.com	Reject	No	2014-02-24
Checking/Savings	5	<input checked="" type="checkbox"/>	tuna.sashimibank.com	Monitor	No	2014-02-24
Events	1					
HR	1					
Marketing	4					
Mortgage	1					
Personal Wealth Management	1					
+ Add New Group						

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

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 that 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.

Add a Domain Group

1. Go to Configure > Manage Domains.
2. At the bottom of the Customer Domain Groups list, click Add New Domain Groups.
3. Enter the name of your new domain group.
4. Press Enter.
5. Select a domain group that contains domains.
6. Select one or more domains.
7. Click Add to Domain Group.
8. Select the domain group you just created.
9. Click Apply.

Delete a Domain Group

1. Go to Configure > Manage Domains.
2. Hover over the Custom Domain Group that you no longer want to use.
3. Click on the trash can icon to remove the group.
4. Click OK to confirm.

Once a Custom Domain Group is deleted, it can not be recovered.



CHAPTER 8

Administration

Domain Protection administration includes defining an organization's settings, reviewing the activity in an organization, and managing Domain Protection users in an organization.

You can make changes to the organization settings, view the audit trail, and manage users only if you have the Organization Administrator role.


Organization Settings

You manage your organization settings on the Manage customer organizations page, where you configure the following categories of settings:

- Administrative
- Organization
- User Account

To edit organization settings, go to Admin > Organization, and then click Edit Organization Details.

You can make changes to the organization settings only if you have the Organization Administrator role.

Setting		Description	
Administrative			
Organization Name	The name of your organization. This is what you see wherever there is information displayed about or relating to your organization, such as audit trails. Contact your Cisco representative to change the organization name.		
Nickname			
Subdomain	The part of the application URL that is unique to your organization. It is a subdomain of dmp.cisco.com. Use caution when deciding to change this value. You may break links, bookmarks, and other connections to Domain Protection.		
Creation Date	Shows the date and time that the organization was created. Click  to toggle between local time and UTC (Coordinated Universal Time).		
Notes	This field allows you to add free-form information about your organization and how it is configured, or anything else you would like to make visible. The content you enter here is visible to all users within your organization when they view the organization settings page.		
Organization Settings			




Setting	Description
Primary Administrative Contact	The organization user selected here will be the person who will receive all administrative communications from Cisco.
Data Collection Policy	<p>Determines whether personally identifiable information (PII) is retained or stripped from messages and failure reports before being stored in Domain Protection. Select:</p> <ul style="list-style-type: none"> • Collect All Available Data (default) • Modified Data Collection <p>When <i>Modified Data Collection</i> is selected, the following parts of all failure reports are stripped, not retained, and unrecoverable:</p> <ul style="list-style-type: none"> • Full message text • URLs in the message body • Certain header fields <p>Because any of these could contain PII, and because PII could be encoded in a way to make it difficult to discern, they are permanently discarded before messages and failure reports are stored in Domain Protection. The lack of this data could make some functionality of Domain Protection, such as URL Thread Feeds, unavailable to your organization.</p> <p>When All Available Data is selected, Domain Protection makes that data assailable only to registered users within your organization.</p>
Attachment Names	
Ignore non-actionable errors	<p>Determines if a missing v= attribute in a DKIM record is ignored when determining DKIM errors. When selected, this means a missing v= attribute in a DKIM record for a domain:</p> <ul style="list-style-type: none"> • will not result in the DKIM record being listed in the serious or minor DKIM problems list • will allow the DKIM record to be listed in the valid keys list <p>when you click on the DKIM Key icon for a domain.</p> <p>Also, if a missing v= attribute is the only DKIM error for a domain, the error indicator (!) will not be displayed next to the DKIM Key icon for the domain.</p> <p>The DKIM specification (https://www.ietf.org/rfc/rfc6376.txt) defines the v= attribute as required, but DKIM will not fail if the v= attribute is missing from a DKIM record. While Cisco recommends that DKIM records adhere to the specification, it is understood that it is not always easy to update DKIM records when an organization does not have access to DKIM records for a domain. You can have Cisco host the DKIM records (see "Host Your DKIM Records at Cisco" on page 55) for the domains you control to make updating those records easy.</p>
User Account Settings	
Single Sign-On	Determines whether your users need to enter a password in addition to their user name to access Domain Protection or whether they can use your existing authentication. See "Single Sign-On (SSO)" on page 131 and "Enable Single Sign-On for

Setting	Description
	Your Organization" on page 132 for more information.
Session Inactivity Logoff	<p>Determines how long users can stay signed in to Domain Protection before they get signed out automatically. The default is 4 hours.</p> <p>Also select how automatic log off happens. Select from:</p> <ul style="list-style-type: none"> Relative (default): Automatic log off happens if no activity in Domain Protection happens within the time period set in the Session Inactivity Logoff setting. Absolute: Automatic log off happens when the time period set in the Session Inactivity Logoff setting expires after log in. In other words, the Session Inactivity Logoff clock starts at log in and does not reset for any user activity. This setting may result in users being logged off while they are in the middle of an activity.
Password expiration	Determines the time period before users have to select a new password. The default is Never.
Maximum failed login attempts	Determines how many times a user can attempt logins without success before being locked out and requiring a new activation link to be sent. Select Disable if you do not want to limit login attempts. The default value is 5.
Password policy	<p>When you require a password for login (non-SSO), determines the minimum complexity of the password.</p> <p>Enter values for any requirement to modify any of the following password requirements for your users:</p> <ul style="list-style-type: none"> Minimum length (default: 5) Minimum upper case characters (default: 0) Minimum lower case characters (default: 0) Minimum symbols (non-alpha-numeric characters) (default: 0) Minimum numbers (default: 0) <p>Per Federal Risk and Authorization Management Program (FedRAMP) processes, when a Domain Protection user changes their password, it cannot be changed to any of the 24 previously used passwords by that user.</p>
IP-Based Access Control	<p>Defines and limits where Domain Protection can be accessed from.</p> <p>For added security, you may require your users to access Domain Protection from only a specific set of IP addresses that you define. Enter one or more IP addresses or CIDR blocks, separated by spaces or commas.</p>

Click Audit Organization Activity to see the audit log for your Organization, including information such as user log in/out and configuration changes See "View Organization Activity" on the next page for details.

Audit Trail

Domain Protection creates a thorough and detailed audit trail to document and authenticate all activity in an organization. All activity is listed in reverse chronological order on the Audit the activity log pages for both your organization and each user in your organization. The list uses icons to categorize the type of activity.

Icon	Activity Category
	Indicates that a user signed in, either of Domain Protection itself or an organization in Domain Protection.
	Indicates that a user signed out, either of Domain Protection itself or an organization in Domain Protection.
	Indicates that a user created, edited, or deleted a user account, or that the system performed a task.
	Indicates that a create, edit, delete, or other action was performed on a domain by either a Domain Protection user or by or on the system managing the domain. When available, information about those actions will also be listed. For example, when a domain's nameservers change, both the previous and new nameservers will be included in the audit log.
	Indicates that a user created, edited, deleted, or performed other actions on a sender.
	Indicates that a user created a report request.
	Indicates that a user created, edited, deleted, or performed other actions on a domain group.
	Indicates that your Sender inventory has been changed.
	Indicates that a user performed an organization-level activity, such as accepting the Cisco Terms of Service (TOS) or changing organization settings.

View Organization Activity

Domain Protection creates a thorough and detailed audit trail to document and authenticate all activity in an organization.

You must have the Organization Administrator role to view organization activity.

1. Go to Manage > Organizations.
2. Click Audit Organization Activity.

All of the activity in the Domain Protection organization is listed in reverse chronological order. The list uses icons to categorize the type of activity. See "Audit Trail" on the previous page for details. Click Help (?) at the top of the page for more information about searching and using the log.

Click Download CSV to download a list all events that Domain Protection tracks as a comma-separated values (CSV) text file.

Search Organization Activity

When you are viewing the list of an organization's activity, you can also search within the list. There are two types of search available:

- Simple text search. Like with web search engines, enter a term and it will be found if it exists. For example, you could enter a username to see just that user's activity in the organization.
- Query keys. You can enter specific keywords to narrow the list to specific actions. For example, every time a report request was created.

Query Keys

Put simply, query keys represent the items tracked by Domain Protection's audit trail. They represent various objects, and can also be combined with verbs, connected by a dot (.). Because query keys define an action on a specific object, when you use a query key in the Search field, you always preface it with action:.

Most query key objects can be combined with create, update, and destroy verbs. In technical terms, "CRUD" actions, minus the "R." Several keys also have additional verbs.

The search format is `action:object[.verb]`

This means that `action:` is required, followed by an object name (with no space after the :, followed optionally by a dot (.) and valid verb.

The following is a list of all query keys:

`bimi_record_source`

Additional Verbs: None

Description: Any changes to BIMi (see "Brand Indicators for Message Identification" on page 95) records.

Example: A search for `action:bimi_record_source.create` might include "123 Inc. (admin@123.-com) created the BIMi record 123.com" in the results.

`dkim_record_source`

Additional Verbs: None

Description: Any changes to DKIM (see "DomainKeys Identified Mail" on page 49) records.

Example: A search for `action:dkim_record_source.update` might include "123 Inc. (admin@123.-com) updated the DKIM record abc123.com" in the results.

domain

Additional Verbs: None

Description: Any changes to domain records.

Example: A search for action:domain.destroy might include " 123, Inc. (admin@123.com) deleted the domain ABC123.com" in the results.

domain_sender

Additional Verbs: None

Description: Any changes to sender approval records. This object is created when a sender is approved for a domain and is deleted when the approval is revoked. This is often because of automated processes, but it is possible for a user to manually approve a sender for a domain, and if the sender was manually approved, it can manually be unapproved. This is especially relevant for a hosted SPF record where all domain/sender relationships are handled manually.

Example: A search for action:domain_sender.create might include " 123, Inc. automatically created the domain sender #<DomainSender:hash>" in the results.

domain_set

Additional Verbs: add_domains, remove_domains

Description: Any changes to domain group (see "Domain Groups" on page 117) records.

Example: A search for action:domain_set.remove_domains might include " 123, Inc. (admin@123.-com) modified the domain group third party" in the results.

organization

Additional Verbs: accept_agreement, reject_agreement, add_netblock_source, remove_netblock_source

Description: Any changes to organization information or settings.

Create and destroy actions are actions performed only by affiliate organizations, that is, organizations with sub-organizations, so only affiliate organizations will see those actions in their audit trails.

Example: A search for action:organization.accept agreement might include " 123, Inc. (admin@123.-com) accepted the End_User License Agreement ABC123.com" in the results.

organization_sender

Additional Verbs: None

Description: Any changes to the relationship between an organization and a sender.

There is no explicit action a user can take to affect this object. An organization_sender is created as a secondary object based exclusively on domain/sender relationships. It is created when a domain is the first to be related to a sender in an org (when the sender is approved for the domain); it is deleted when there are no longer any domains in the org related to the sender. It is updated when domains gain or lose their relationship with a sender.

Example: A search for action:organization_sender.destroy might include " 123, Inc. (admin@123.com) removed the sender New Sender" in the results.

report_request

Additional Verbs: None

Description: Any changes to a report request.

Example: A search for `action:report_request.destroy` might include "123, Inc. (admin@123.com) deleted the report request Daily Domain Diagnostic Report (123, Inc.) (csv, pdf)" in the results.

sender

Additional Verbs: None

Description: Any changes to the definition of a sender (see "Senders" on page 77).

Example: A search for `action:sender.destroy` might include "123, Inc. (admin@123.com) deleted the sender New Sender" in the results.

sender_netblock

Additional Verbs:

Description: Any creation or deletion of a netblock.

The `sender_netblock` object does not have an update verb.

Example: A search for `action:sender_netblock.create` might include "123 Inc. (admin@123.com) created the sender netblock ###.###.###.###" (where # are digits in a netblock) in the results.

sender_netblock_source

Additional Verbs: None

Description: Any change to the sender inventory.

Example: A search for `action:sender_netblock_source` with any verb might include "123, Inc. (automatically) modified ABC's Sender Inventory" in the results.

user

Additional Verbs: activated, login, logout, update_roles

Description: Any change to a user account, a user account activation, or a user logs in or out.

Example: A search for `action:user.update` or `action:user.update_roles` might include "123, Inc. (admin@123.com) changed the roles for newuser123.com" in the results.

How Search Works

When you type characters into the Search field, Domain Protection starts searching when you pause or stop typing. In technical terms, it's a "starts with" search. This concept is important to understand the search results you're seeing, especially because several objects begin with the same characters.

For example, as mentioned above, the `.verb` is optional. But if you search for `action:sender_netblock`, with the goal of seeing all of the audit trail entries for that object, you will get results that also include audit trail entries for the `sender_netblock_source` object. To see just the `sender_netblock` object entries, add a `.` without a verb, like this: `action:sender_netblock..`

User Accounts

User accounts define the credentials and access capabilities of Domain Protection users. Domain Protection uses Role-Based Access Control (RBAC), which allows you to assign each user one or more roles for access to Domain Protection functionality.

Cisco support personnel do not have access rights to create, enable, edit, or delete user accounts in your Domain Protection organization.

Create a User Account

Only users with the User Administrator role can create user accounts.

1. Go to Admin > Users.
2. Click Add New User.
3. Enter a Full Name and an E-mail address.

You must enter a valid email address. The email address is where the invitation email message is sent. The invitation email message contains a unique link that the new user must click to validate the new account.

4. Configure the other user account settings and select one or more user roles. See "User Account Settings" on the facing page for details.
5. Click Invite New User.

An email will be sent to the email address you entered with a link to validate the user and for the user to set an account password.

Edit a User Account

1. Go to Admin > Users.
2. Click the name of a user.
3. Make any desired changes to the user information and settings. See "User Account Settings" on the facing page for details.
4. Click Update.

Delete a User Account

1. Go to Admin > Users.
2. Click the name of a user.
3. In the lower left, click the Delete [username] entirely from Domain Protection link.
4. Click OK.

View User Activity

Domain Protection creates a thorough and detailed audit trail to document and authenticate all activity of all users in an organization.

You must have the Organization Administrator role to view a user's activity.

- 1. Go to Admin > Users.
- 2. Under a user's name, click the Audit link.

All of the user's activity in the Domain Protection organization is listed in reverse chronological order. The list uses icons to categorize the type of activity. See "Audit Trail" on page 123 for details. Click Help (?) at the top of the page for more information about searching and using the log.

Click Download CSV to download a list all events that Domain Protection tracks as a comma-separated values (CSV) text file.

User Account Settings

This topic describes the settings for Domain Protection user accounts.

User Information

Setting	Description
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.
Secondary Authentication	<div>If your organization uses single-sign on (SSO), this option determines whether secondary authentication (username and password) is optional or required. If you do not select this option, SSO is always used, and if the SSO provider is unavailable at the moment of sign in, application access is not possible. If you select this option, you are then given two additional options:</div> <ul style="list-style-type: none">• Only when SSO fails: The user is prompted with a password field if the SSO provider fails• Exclusively (do not authenticate with SSO): The user is always prompted for a password (SSO is not used)

Roles

Roles define what functionality of Domain Protection a user can access, and each role is defined by specific and unique access permissions. At least one rule must be selected for a user.

The role list is hierarchical in that selecting a role selects every role below it automatically, but roles do not inherit the permissions of the roles beneath them. You can clear individual roles for a user underneath any selected role, but clearing certain combinations may result in unexpected user interface behavior.

There are 2 categories of user roles:

- Administrator Roles: Can make changes to settings in your organization
- Read-only Roles: For receiving alerts or viewing data

Role	Description
Administrator Roles	
Organization Administrator	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 Domain Protection users.
Domain Policy Administrator	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 Administrator	Manage threat level settings. This includes configuring your organization's Threat Feed and editing your organization's URI Whitelists.
User Administrator	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	
Auditing User	View audit logs for your organization and users in your organization.
Readonly User	View data and schedule reports in the web portal.
Report User	Receive scheduled reports and alerts. User with only this role, assigned by itself, cannot view data directly in Domain Protection. Such users can only receive emailed reports that are scheduled by other users, receive emailed alerts when subscribed by other users, and view the list of reports subscribed to. To create an account to use in sending reports 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.

Role	Description
Threat Feed Submission API User	<p>To retrieve only threat feed data via the Domain Protection application programming interface (API) via the threat_feed_submissions endpoint. This allows third-party take-down vendors to access only the specific information they need without allowing broader API access such as to failure sample data that could include personal information.</p> <p>User accounts who are assigned this role should be assigned only this role. User accounts that are assigned only this role do not have access to the Domain Protection product, any other APIs, or the API documentation.</p> <p>To use the user account with this role to access the API for threat feed data, obtain the access token and the endpoint URL from your administrator.</p>

Domain Access

By default, new user accounts 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 to select specific domain groups.

View the available domains groups, and select one or more custom Domain Groups from the list.

The user will only be able to

- See information about domains
- View only the reports
- Receive alerts

for the set of domains that are part of the selected domain groups.

For example, 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 Examples

This topic contains examples of how you would configure roles for some specific use cases.

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.

Single Sign-On (SSO)

Domain Protection now includes the ability for you to enable a Single Sign-On (“SSO”) mechanism for authenticating users in your organization via the SAML 2.0 protocol.

With Single Sign-On, you can:

- Create a “one-click” login experience. You can bind your existing corporate login identities (accounts) to the Domain Protection username, which eliminates the need for a separate Domain Protection password.
- Revoke user access centrally. When an employee leaves the company, you can remove Domain Protection access within the SSO provider rather than within Domain Protection separately.
- Provide optional secondary authentication. You can allow specific users (for example, contractors not available in your identity provider system) to authenticate exclusively with the credentials stored in Domain Protection (which effectively bypasses the single sign-on mechanism). You can also allow specific users to authenticate with the credentials stored in Domain Protection only in the event when the SSO identity service fails (for example, during outages).

Enable Single Sign-On for Your Organization

Before you begin, you must get two pieces of information from your single sign-on provider:

- SAML 2.0 Endpoint (HTTP) URL (This is sometimes referred to as the “destination” or “SAML Recipient” in Identity Provider systems.)
- Public Certificate (X.509)

You must have the Organization Admin role to perform this task.

1. Go to Admin > Organization.
2. Click Edit Organization Details.
3. In the User Account Settings section, select Enable Single Sign-On.
4. In the confirmation message, click OK.
5. Enter the SSO parameters:

Single Sign-On Parameter	Description
Name Identifier Format	Select from: <ul style="list-style-type: none"> • urn:oasis:names:tc:SAML:1.1nameid-form-at:unspecified • urn:oasis:names:tc:SAML:1.1nameid-form-at:emailAddress • urn:oasis:names:tc:SAML:2.0nameid-format:persistent (default)
SAML 2.0 Endpoint (HTTP Redirect)	Enter the SAML 2.0 endpoint URL you obtained from your single sign-on provider.
Public Certificate	Enter the entire text of the certificate you received from your single sign-on provider. (It is probably easiest to copy-and-paste.

6. Click Test Settings to validate the Endpoint URL and certificate values provided by your identity provider. Domain Protection calls the Identity Provider with the public certificate credential at the location you enter.

You may be required to authenticate with your Identity Provider if you are not already logged in there.

7. Click Save Settings.
8. In the confirmation message, click OK.
9. Click Update Information.

At this point, Single Sign-On will be enabled and:

- All existing users will receive an email that instructs them to use their Single Sign-On identity provider credentials when accessing Domain Protection.
- Users currently logged into Domain Protection will continue their sessions without interruption; however, they will be directed to the Identity Provider on subsequent login attempts.



CHAPTER 9

Application Programming Interface

Domain Protection includes an application programming interface (API) that allows developers within your organization to programmatically access data within Domain Protection.

The Domain Protection API is built on RESTful principles with JSON data representations. Clients authenticate API requests using the [OAuth 2.0 protocol](#). A user account may be assigned one API credential consisting of an API Client ID and Client Secret. The resources and data made available with those credentials is directly tied to the permissions assigned to that user by an account administrator in the Domain Protection user interface.

Generate API Credential

An API (application programming interface) credential, also known as an API secret, must be generated for a user before that user can use the Cisco Domain Protection API.

Only users with the User Administrator role can generate API credentials.

1. In Cisco Domain Protection, go to Admin > Users.
2. Click a username.
3. In the API Client Secret section, click Generate API Credentials.
4. Copy and save the API Access UID and credential in a secure place. You will need to enter it on the API Documentation page when you test an API or when you are using an Cisco integration via API.

View API Documentation

Before you can view the Domain Protection API (application programming interface) documentation, you must first have an API credential generated for your user account. See "Generate API Credential" above for details.

1. In the upper-right of a Domain Protection page, click your name, and then click Settings.
2. Click Domain Protection API Documentation.