

Exchange Online Protection Installation

1. Establish separate college portal/tenant from LACCD. <http://lamission.onmicrosoft.com>

2. Verify campus/district domain ownership

Admin → Office 365 → Domain

Add domain. A TXT DNS record is generated which must be added to the public DNS server to verify ownership. Come back to the onmicrosoft.com portal to verify domain ownership once the TXT DNS record is implemented.

3. Setup connectors between Office 365 and campus Edge Transport Servers

Admin → Exchange → Mail flow → Connectors

- Create inbound connector to receive mail from On Premises Edge Transport Servers (campus outgoing mail).
- Create outbound connector to send mail to on premises Edge Transport Servers (campus incoming mail).

4. Add campus domain as accepted domain

Admin → Exchange → Mail flow → Accepted Domains

The college domain (lamission.edu) should be added as an accepted domain.

5. Update MX record to forward mail to Office 365

Admin → Office 365 → Domains

Select the college domain (after domain ownership).
Click Manage DNS
Update public DNS MX record to point to provided address.
SPF TXT record entry is also provided

mx:lamission.edu

Monitor This

mx

Pref	Hostname	IP Address	TTL		
0	lamission-edu.mail.protection.outlook.com	207.46.163.247	60 min	Blacklist Check	SMTP Test
10	mail.lamission.edu	207.62.63.154	60 min	Blacklist Check	SMTP Test
20	mail2.lamission.edu	207.62.63.155	60 min	Blacklist Check	SMTP Test

MX Server	Pref	Connect	Allowed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
lamission-edu.mail.protection.outlook.com [207.46.163.247]	0	OK (21ms)	OK (20ms)	OK (19ms)	OK (19ms)	OK (334ms)	OK (25ms)	OK (21ms)	OK (87ms)
mail.lamission.edu [207.62.63.154]	10	OK (73ms)	OK (73ms)	OK (74ms)	OK (73ms)	OK (641ms)	OK (76ms)	OK (73ms)	OK (581ms)
mail2.lamission.edu [207.62.63.155]	20	OK (93ms)	OK (91ms)	OK (93ms)	OK (91ms)	OK (362ms)	OK (97ms)	OK (93ms)	OK (715ms)
Average		100%	100%	100%	100%	100%	100%	100%	100%

spf:lamission.edu

[Monitor This](#)

[Refresh](#) spf

Prefix	Type	Value	PrefixDesc	Description
+	mx		Pass	Match if IP is one of the MX hosts for given domain name
+	ptr		Pass	Match if IP has a DNS 'PTR' record within given domain
+	ip4	207.62.63.154	Pass	Match if IP is in the given range
+	ip4	207.62.63.155	Pass	Match if IP is in the given range
+	ip4	208.93.120.245	Pass	Match if IP is in the given range
+	mx	mail.lamission.edu	Pass	Match if IP is one of the MX hosts for given domain name
+	mx	mail2.lamission.edu	Pass	Match if IP is one of the MX hosts for given domain name
+	include	spf.protection.outlook.com	Pass	The specified domain is searched for an 'allow'.
-	all		Fail	Always matches. It goes at the end of your record.

Admin → Exchange → Protection → Content Filter

Update Default content filter

Default

general

▶ spam and bulk email actions

international spam

advanced options

spam and bulk email actions

Select the action to take for incoming spam and bulk email. [Learn more](#)

Spam:

Move message to Junk Email folder

High confidence spam:

Quarantine message

Bulk email:

Mark bulk email as spam

Select the threshold. 1 marks the most bulk email as spam and 9 allows the most bulk email to be delivered.

7 (Default)

Quarantine

Retain spam for (days):

15

*Add this X-header text:

Admin→Exchange→Protection→Outbound spam

Update Default outbound spam

Default

general

▶ outbound spam preferences

outbound spam preferences

Send a copy of all suspicious outbound email messages to the following email address or addresses.

quarantine@lamission.edu

Send a notification to the following email address or addresses when a sender is blocked for sending outbound spam.

austrig@lamission.edu; garciacr@lamission.edu

Admin→Exchange→Protection→Connection filter

Update Default connection filter.

Default

general

• [connection filtering](#)

connection filtering

IP Allow list

Always accept messages from the following IP addresses.

+  -

Allowed IP Address
207.62.63.130
207.62.63.117
207.62.63.24
207.62.63.25

IP Block list

Always block messages from the following IP addresses.

+  -

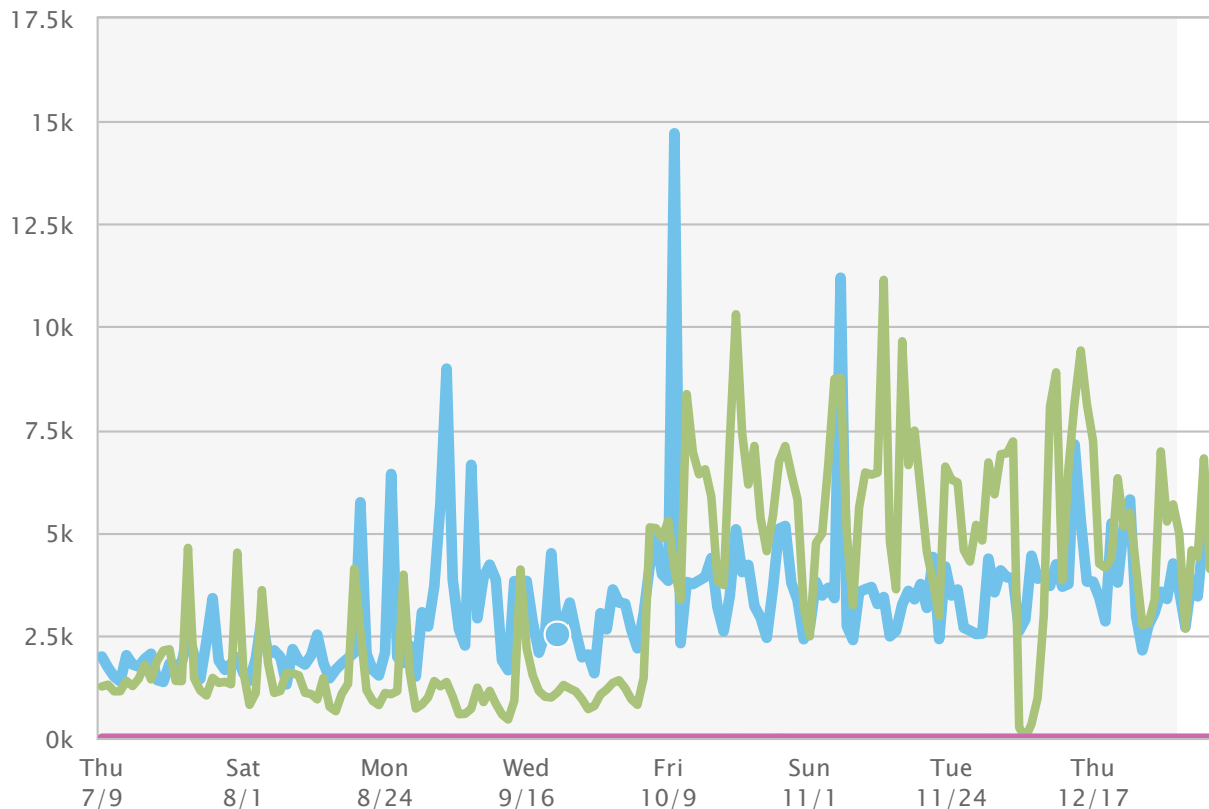
Blocked IP Address

Spam detections ⓘ

Date selection:

- 7 Days
- 14 Days
- 30 Days
- Custom

[View table](#)



Series slicing:

- Content filtered
- SMTP blocked
- IP blocked
- Directory blocked

Data selection:

- Received
- Sent

[Schedule this report](#)
[View scheduled reports](#)

[View pending or completed requests](#)

Messages that are older than 7 days have a gray background. When you select a data point in this area, a link appears that lets you specify parameters for a downloadable detail report. All dates and times are in Coordinated Universal Time (UTC).