

Sender Policy Framework Record

What is an SPF record?

An SPF record lists the IP addresses that are authorized to send mail on behalf of a domain, and is commonly used as a security check to prevent delivery of spam with forged From addresses. An SPF record also provides some assurance to hosts receiving mail that the mail is not spam.

What do I need to do?

1. Register mail senders (not including campus copiers, scanners, servers, websites, Gmail, mail.appstate.edu, or applications that use the bulk mailer to send messages) If your unit sends email from an @appstate.edu addressing using:

- an outside vendor,
- third party system, or
- an internal application other than Gmail, mail.appstate.edu, or the bulk mailer to relay messages

then you need to:

- identify any applications sending email from an @appstate.edu email address and contact our Help Desk (262-6266) to discuss your needs.

2. If you write scripts (BASH, Powershell, etc.) that send emails from servers or devices on-campus, the emails should follow the appropriate RFC for email format, and use a valid reply-to/from email address.

3. Don't configure your client to send mail through your ISP. Users with email clients configured to send their appstate.edu mail through their Internet Service Providers' (ISP) SMTP relay need to reconfigure their email clients to send mail through gmail. Otherwise, mail sent through the ISP's SMTP relay may be rejected or marked as spam by the recipient's mail service. Mail configuration Instructions can be found here: <http://gogoogle.appstate.edu/training-support/mountaineeremail#ClientSetup>

Do I have to worry about email from my server being rejected?

If the external mail service is not registered in our SPF record, mail sent through the external service may be rejected or marked as spam by the recipient's mail service. To try to mitigate any problems with unregistered mail services sending on behalf of appstate.edu email addresses, we will first set up our SPF record with a soft fail and a short time to live. The soft fail means that most mail services will still allow mail to be delivered from a sender not listed in the SPF record, and the short time to live means that we can easily add newly discovered external mail services to the SPF record.

Questions?

If you have any questions or concerns, please contact the Help Desk at 262-6266, or submit a Support Ticket through support.appstate.edu.

Related Articles

- [Allowing Less Secure Apps in Google Workspace](#)
- [E-Mail Attachment Limits](#)
- [E-Mail Disappears from Inbox After Sending a Reply](#)
- [Gmail](#)
- [Gmail Sending Limits](#)
- [How to Delegate \(share\) the Inbox of an App State Email Account.](#)
- [How to Obtain Headers from Email](#)
- [How to request a Generic Appstate Email Account](#)
- [I am being redirected when I try to log into my gmail account.](#)
- [Migrate Outlook Local Contacts into Gmail](#)
- [Retirees](#)
- [Security and Google Apps](#)
- [Sender Policy Framework Record](#)
- [Sending Mail from a Different Address in Gmail](#)
- [Setting Gmail to be the Default Email Handler](#)
- [Setting up Gmail & Calendar on Android](#)
- [Setting up Google Apps in Apple Mail, Contacts & Calendars on Mac OS 10.11](#)
- [Setting up Mail Delegation in Gmail](#)
- [Should I Forward Email Outside Gmail](#)
- [View multiple @appstate Gmail Accounts in the Same Browser](#)

[Search Knowledge Base](#)

[Submit a Service Request](#)