Fannie Mae

IP Address Restrictions

WHAT TO KNOW

Help safeguard your organization's data with IP (Internet Protocol) Address Restriction by validating a user or system against the organization's list of allowable IP addresses, ensuring that stolen or compromised credentials cannot be used to gain unauthorized access by only allowing users to access from approved devices or locations.

Benefits

Increased Security
Provide Data Loss Protection (DLP) capability for customers allowing users to only login from approved devices/locations

Reduced Risk
Ensure stolen or compromised credentials cannot be used from anywhere.

Capabilities

User Types
Customer administrators can select to enforce IP Authorization for: System IDs, User IDs, or both.

IP Allow List
Custom IP allow list with ranges of IP addresses is managed by customer administrators.

IP Range Updates
Updates to IP allow ranges take effect in near real time.

IP Validation
IP validations are performed during authentication.

FAQs

Q1: What is IP (Internet Protocol) Address Restrictions and how is it applicable to Fannie Mae customers?
IP Address Restrictions is an optional feature, which, when enabled, will block access to Fannie Mae technology if the request was not initiated from specified and registered IP address ranges. Administrators from customer organizations can self-enable the feature in Technology Manager by providing a list of allowable IP address ranges.

Please refer to the applicable Technology Manager job aid associated with your role:

- Corporate Administrators - Manage IP Address Restrictions
- User Administrators - Manage IP Address Restrictions

Q2: Who is permitted to add/view allowable IP addresses for a customer's organization?
Both Corporate Administrators (CAs) and User Administrators (UAs) are able to update and view the allowable IP address ranges for their organization in Technology Manager. For organizations that have both CA and UAs, only the CAs will be able to view or update the allowable IP address ranges.

Q3: Is there an associated cost to utilizing the feature?
No, there is no cost associated with enabling or using the feature.

Q4: Can we use IP Address Restrictions to ensure all our users connect to Fannie Mae applications via our company VPN (Virtual Private Network)?
Yes, you can register your company VPN's public IP address(es) as the allowable IP addresses to force users to access Fannie Mae technology using your VPN.

Q5: Will all users within a customer's organization be impacted by IP Address Restrictions?
Yes, if the IP Address Restrictions feature is enabled in Technology Manager, or IP address ranges are removed/added by an administrator, all of the organization's User IDs, System IDs or both will be impacted. Note: there will be an impact to User IDs, System IDs, or both if any IP addresses are not included. If all IP addresses are added, User IDs, System IDs, or both will continue to be able to log in as they had previously.

Q6: Will customers using a Loan Origination System (LOS) be impacted by IP Address Restrictions?
Yes, if your users or systems access Fannie Mae applications through a Technology Service Provider's (TSP) solution (e.g., an LOS), you will also need to provide of list of allowable IP address ranges that will apply to the TSP's system(s) in Technology Manager. If you enable the IP Address Restrictions feature but do not provide such list for the TSP's system, your users/systems may be blocked when trying to access Fannie Mae resources through the TSP's system.

Q7: Does a user have the ability to update the allowable IP Address list?
Only top-level administrators from your organization can update the allowable IP address ranges in Technology Manager. If a user is NOT a top-level administrator, they must contact their administrator to update the allowable IP address list.

Q8: If a user is a top-level administrator and is locked out of Technology Manager due to their own IP address not being included on the allowable IP address list, what options do they have to resolve the issue?
If other administrators within the organization can log in to Technology Manager, they can add the missing IP addresses to the customer's list. If that option is not available, contact Technology Support Center or call 1-800-2FANNIE (1-800-232-6643).

Q9: If I am an Administrator, may I enable IP Address Restrictions for User or System IDs?
Yes, Administrators may enable IP Address Restrictions for either User IDs, System IDs, or both.

Q10: How long will it take for an update to my IP Address Restrictions to become effective?
Depending on the number of users in the organization, updates may take anywhere between a few minutes to a few hours to become effective. If changes still do not appear to be effective 24 hours after an update has been submitted in Technology Manager, please contact Technology Support Center or call 1-800-2FANNIE (1-800-232-6643).

Q11: What information do I need to enable IP Address Restrictions for my organization?
Administrator should have the following information readily available to enable the IP Address Restrictions feature:

- IP address ranges in CIDR (Classless Inter Domain Routing) format (e.g., 192.168.0.1/24) that will be applicable for User IDs, System IDs, or both.
- If your organization is using a Technology Service Provider (TSP) solution, you will also need the applicable IP address ranges for the TSP's system in CIDR format.

Q12: Where do I find instructions on how to manage IP Address Restrictions?

Refer to the applicable Technology Manager s job aid associated with your role:

- Corporate Administrators - Manage IP Address Restrictions
- User Administrators - Manage IP Address Restrictions

Q13: Do I have the ability to opt out of IP Address Restrictions?

The IP Address Restrictions feature is inactive by default unless your organization registers its allowable IP addresses in Technology Manager. You may also choose to opt out of using the IP Address Restrictions feature for all of your organization's User IDs, System IDs, or both. If you initially choose to use the IP Address Restrictions feature and wish to opt out later, your administrator can select that option in Technology Manager and all IP Address Restrictions that were set up previously will be removed.

Please refer to the applicable Technology Manager job aid associated with your role for further instructions:

- Corporate Administrators - Manage IP Address Restrictions
- User Administrators - Manage IP Address Restrictions