IP Threat Lookup

Armor Knowledge Base

Topics Discussed

⚠ To fully use this screen, you must add the following permissions to your account:

- Read IP Threat Lookup Rule(s)
- Write IP Threat Lookup Rule(s)
- Write IP Threat Lookup Rule Never Expire IP
- Read IP Threat Lookup(s).

At a high-level, you can use the **IP Threat Lookup** screen to:

- Perform an IP lookup to research the safety of an IP address.
- Create a rule to allow (whitelist) or block (blacklist) an IP address.
  - Although you can use this screen to research, create, and organize rules, you are responsible for implementing the actual rules in your environment.
- Review users who have performed an IP lookup in your account.

Access IP Threat Lookup

Overview

Graph / Table	Description
IP Lookups	This graph displays all the IP lookups that have taken place in your account. ⚠ An **IP Lookup** indicates a user has searched for Armor's recommendation regarding to whitelist or blacklist an IP address.
DTB User	This table lists: • The name of the AMP user who performed an IP lookup (**IPTL User**). • The date of their last IP lookup (**Last Query Date**). • The total number of IP lookups performed (**Total Requests**).
IP Lookup	You can use this box to perform an IP lookup. To learn more, see Perform an IP Lookup.

Events

You can use this screen to view the IP addresses that your users have researched in AMP.

Column	Description
Source IP	This column displays the IP address that was researched.
Request Type	Standard - This lookup took place using the Armor API system. Detailed - This lookup took place when a user used the IP Lookup feature in AMP.
Requestor	This column displays the full name of the AMP user who researched the IP address.

Date	This column displays when the search took place.
Recommendation Action	This column displays the **Final Recommendation**that was displayed during an IP lookup. When you performed a search, you will receive two types of recommendations: • The **Recommendation** entry is based on Armor's default policy. • The **Final Recommendation** entry is based on any rules that you have previously created. • For example, if you created a rule to blacklist 123.444.555.777, and then you perform a search on 123.555.777.999, then the **Final Recommendation** will most likely say **Block** because of your previously created rul
Rules	This column displays the corresponding rule, if applicable. If the column says **None**, then you can create a rule for this IP address. Hover over the rule, click the vertical ellipses, and then click **Add Rule**.

Rules

This section displays the rules that have been created in your account.

Column	Description
IP	The IP address that is included in the rule.
Added By	The name of the AMP user that created the rule.
Date Added	The date that the rule was created.
Expiration Time	The date that the rule expires, if applicable.
Rule	The type of rule (**Whitelist** or **Blacklist**).

Add a Rule

Before you create a rule, Armor recommends that you perform a search on the IP address to view Armor's recommendation. To learn how to perform an IP lookup, see Perform an IP Lookup.

Before you create a rule, consider the following statements:

- When you add a rule, your rule may actually override Armor's default whitelist and blacklist policies.
- You cannot use the same IP address in multiple rules, even if the rules are similar in action.
  - For example, if you create a rule to allow 1.1.1.1, then you cannot create a separate whitelist rule for 1.1.1.1/2.
- You cannot edit a rule.
  - If you want to edit a rule to a different list, then you must delete the rule, and then create a new rule.
- Although you can use this screen to research, create, and organize rules, you are responsible for implementing the actual rules in your environment.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **IP Threat Lookup**.
3. Click **Rules**.
4. Click the plus (+) icon.
5. Select **Whitelist** or **Blacklist**.
6. Enter an IP address or CIDR.
7. Select an expiration date.
   - You will not receive a notification when a rule has expired; however, you can filter the **Rules** table to view expired rules.
   - If your account contains the **Write IP Threat Lookup Rule Never Expire IP** permission, then as an option, you can mark **Never Expire**.
8. Click **Add Rule**.
   - The newly created rule will appear in the **Rules** section.

Delete a Rule

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **IP Threat Lookup**.
3. Click **Rules**.
4. Locate and hover over the desired rule.
5. Click the vertical ellipses.
6. Click **Remove Rule**.
7. Click **Remove Rule** again.

Perform an IP Lookup

There is a cost associated with performing an IP lookup.

You can use the **IP Lookup** feature to review Armor's recommendation regarding to allow or block an IP. Later, you can use this information to create an IP rule.

When you perform a search, you will receive two types of recommendations:

- The **Recommendation** entry is based on Armor's default policy.
- The **Final Recommendation** entry is based on any rules that you have previously created.
    - For example, if you created a rule to blacklist 123.444.555.777, and then you perform a search on 123.555.777.999, then the **Final Recommendation** will most likely say **Block** because of your previously created rule.

When you look up an IP address, the action will be logged in the **Events** section.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **IP Threat Lookup**.
3. Click **IP Lookup**.
4. Enter an IP address, and then click **Lookup**.
    - The **Recommendation** entry is based on Armor's default policy.
    - The **Final Recommendation** entry is based on any rules that you previously created.
5. (Optional) You can convert this IP lookup into an IP rule. Next to **Rule Status**, click the vertical ellipses, and then click **Add Rule**.
6. Select **Whitelist** or **Blacklist**.
7. Select an expiration date.
    - If your account contains the **Write Iprm Rule(s) - Never Expire IP** permission, then you can mark **Never Expire**.
    - You will not receive a notification when a rule has expired; however, you can filter the **Rules** table to list expired rules.
8. Click **Add Rule**.

Troubleshooting

If you do not see any data in this screen, consider that:

- You have not created a rule.
- You have not performed an IP lookup.
- You do not have permission to view this screen.
    - To fully use this screen, you must have the following permission enabled for your account:
        - Read IP Threat Lookup Rule(s)
        - Write IP Threat Lookup Rule(s)
        - Write IP Threat Lookup Rule Never Expire IP
        - Read IP Threat Lookup(s).

To learn more about roles and permissions, see Roles and Permissions.

Additional Information

This feature includes GeoLite data, created by MaxMind. For more information, please visit the MaxMind website.

Was this helpful?

Your Rating:  Results:  18 rates