Chapter: Firepower System User Management

Predefined User Roles

The Firepower System includes ten predefined user roles that provide a range of access privilege sets to meet the needs of your organization. Note that 7000 and 8000 Series devices have access to only three of the ten predefined user roles: Administrator, Maintenance User, and Security Analyst.

Although you cannot edit predefined user roles, you can use their access privilege sets as the basis for custom user roles. In addition, you cannot configure them to escalate to another user role.

The following table briefly describes the predefined roles available to you.

**Access Admin**

Provides access to access control policy and associated features in the **Policies** menu. Access Admins cannot deploy policies.

**Administrator**

Administrators have access to all functionality; their sessions present a higher security risk if compromised, so you cannot make them exempt from login session timeouts.

You should limit use of the Administrator role for security reasons.

**Discovery Admin**

Provides access to network discovery, application detection, and correlation features in the **Policies** menu. Discovery Admins cannot deploy policies.

**External Database User**

Provides read-only access to the Firepower System database using an application that supports JDBC SSL connections. For the third-party application to authenticate to the Firepower System appliance, you must enable database access in the system settings. On the web interface, External Database Users have access only to online help-related options in the **Help** menu. Because this role’s function does not involve the web interface, access is provided only for ease of support and password changes.

**Intrusion Admin**

Provides access to all intrusion policy, intrusion rule, and network analysis policy features in the **Policies** and **Objects** menus. Intrusion Admins cannot deploy policies.

**Maintenance User**

Provides access to monitoring and maintenance features. Maintenance Users have access to maintenance-related options in the **Health** and **System** menus.

**Network Admin**

Provides access to access control, SSL inspection, DNS policy, and identity policy features in the **Policies** menu, as well as device configuration features in the **Devices** menus. Network Admins can deploy configuration changes to devices.

**Security Analyst**

Provides access to security event analysis features, and read-only access to health events, in the **Overview**, **Analysis**, **Health**, and **System** menus.

**Security Analyst (Read Only)**

Provides read-only access to security event analysis features and health event features in the **Overview**, **Analysis**, **Health**, and **System** menus.

**Security Approver**

Provides limited access to access control and associated policies and network discovery policies in the **Policies** menu. Security Approvers can view and deploy these policies, but cannot make policy changes.

Externally authenticated users, if assigned no other roles, have minimum access rights based on the settings in LDAP or RADIUS authentication objects and in platform settings. You can assign additional rights to these users, but to remove or change minimum access rights, you must perform the following tasks:

* Move the user from one list to another in the authentication object or change the user's attribute value or group membership on the external authentication server.
* Update platform settings.
* Use the User Management page to remove the access from that user account.

**Related Concepts**
[User Account Privileges](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000007ef)

Custom User Roles

In addition to the predefined user roles, you can also create custom user roles with specialized access privileges. Custom user roles can have any set of menu-based and system permissions, and may be completely original or based on a predefined user role. Like predefined user roles, custom roles can serve as the default role for externally authenticated users. Unlike predefined roles, you can modify and delete custom roles.

Selectable permissions are hierarchical, and are based on the Firepower System menu layout. Permissions are expandable if they have sub-pages or if they have more fine-grained permissions available beyond simple page access. In that case, the parent permission grants page view access and the children granular access to related features of that page. Permissions that contain the word “Manage” grant the ability to edit and delete information that other users create.

**Intrusion Admin**

Provides access to all intrusion policy, intrusion rule, and network analysis policy features in the **Policies** and **Objects** menus. Intrusion Admins cannot deploy policies.

**Network Admin**

Provides access to access control, SSL inspection, DNS policy, and identity policy features in the **Policies** menu, as well as device configuration features in the **Devices** menus. Network Admins can deploy configuration changes to devices.

**Security Analyst**

Provides access to security event analysis features, and read-only access to health events, in the **Overview**, **Analysis**, **Health**, and **System** menus.

**Security Analyst (Read Only)**

Provides read-only access to security event analysis features and health event features in the **Overview**, **Analysis**, **Health**, and **System** menus.

**Discovery Admin**

Provides access to network discovery, application detection, and correlation features in the **Policies** menu. Discovery Admins cannot deploy policies.

**Maintenance User (OS, Risk and Patching)**

Provides access to monitoring and maintenance features. Maintenance Users have access to maintenance-related options in the **Health** and **System** menus.

**Security Approver**

Provides limited access to access control and associated policies and network discovery policies in the **Policies** menu. Security Approvers can view and deploy these policies, but cannot make policy changes.

**External Database User**

Provides read-only access to the Firepower System database using an application that supports JDBC SSL connections. For the third-party application to authenticate to the Firepower System appliance, you must enable database access in the system settings. On the web interface, External Database Users have access only to online help-related options in the **Help** menu. Because this role’s function does not involve the web interface, access is provided only for ease of support and password changes.

Chapter: Firepower System User Management

Chapter Contents

[User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000738)

[Predefined User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000750)

[Custom User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000007cb)

[Example: Custom User Roles and Access Control](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2176-00000155)

[User Account Privileges](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000007ef)

[Overview Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000803)

[Analysis Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000981)

[Policies Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000dbe)

[Devices Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-0000107f)

[Object Manager Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000010ef)

[Cisco AMP](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00001102)

[Deploy Configuration to Devices](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#reference_A30E167F2A8142B3BC3BF55814523235)

[System Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-0000117a)

[Help Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-0000136b)

[Managing User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00001384)

[Activating and Deactivating User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000013bb)

[Creating Custom User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000013e0)

[Copying User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00001413)

[Editing Custom User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#task_9BA004CE32094C40AC6A4CF204D84CFE)

[User Role Escalation](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000015e9)

[Setting the Escalation Target Role](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000015fd)

[Configuring a Custom User Role for Escalation](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00001625)

[Escalating Your User Role](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2209-0000012c)

[User Accounts](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#concept_96C6A9709BB54F4D8BCE5CC19C92B7C3)

[Managing User Accounts](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#task_C7D5318FF0D6457BB4C96D625F472643)

[Creating a User Account](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#task_B5DDF67D2A01409E9468BE7691B5CC0C)

[Editing a User Account](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#task_DAB131F67FE24A61AFA76F4A75A10F43)

[Assigning User Roles in Multiple Domains](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#task_6696BC3060024E9C80235BAEBC80D370)

[Converting a User from Internal to External Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#task_AAB47849D3694F52A1766807AE96BF18)

[User Account Login Options](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000014a0)

[Command Line Access Levels](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000014fa)

[Firepower System User Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000006)

[Internal Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000025)

[External Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000040)

[LDAP Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000067)

[Required Information for Creating LDAP Authentication Objects](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000088)

[CAC Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000000e3)

[Configuring CAC Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000000fc)

[Creating Basic LDAP Authentication Objects](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-0000016b)

[Creating Advanced LDAP Authentication Objects](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000001dc)

[LDAP Authentication Server Fields](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000252)

[Identifying the LDAP Authentication Server](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000288)

[LDAP-Specific Fields](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000002d3)

[Configuring LDAP-Specific Parameters](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000359)

[LDAP Group Fields](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000003d1)

[Configuring Access Rights by Group](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000003fe)

[LDAP Shell Access Fields](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-0000043d)

[Configuring LDAP Shell Access](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-0000045e)

[Testing LDAP Authentication Connections](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000004a2)

[Troubleshooting LDAP Authentication Connections](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000004dc)

[RADIUS Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-0000052e)

[Creating RADIUS Authentication Objects](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000549)

[Configuring RADIUS Connection Settings](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000005aa)

[Configuring RADIUS User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000005ff)

[Configuring RADIUS Shell Access](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000640)

[Defining Custom RADIUS Attributes](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000670)

[Testing RADIUS Authentication Connections](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000006b2)

[Single Sign-on (SSO)](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00001650)

[Configuring SSO](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00001674)

Close

Firepower System User Management

The following topics describe how a user with Administrator access can manage user accounts in the Firepower System:

[User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000738)

[User Accounts](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#concept_96C6A9709BB54F4D8BCE5CC19C92B7C3)

[Firepower System User Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000006)

[LDAP Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000067)

[RADIUS Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-0000052e)

[Single Sign-on (SSO)](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00001650)

User Roles

The Firepower System lets you allocate user privileges based on the user’s role. For example, you can grant analysts predefined roles such as Security Analyst and Discovery Admin and reserve the Administrator role for the security administrator managing the Firepower System. You can also create custom user roles with access privileges tailored to your organization’s needs.

In the platform settings policy for a managed device, you set a default access role for all users from that device who are externally authenticated. After an externally authenticated user logs in for the first time, you can add or remove access rights for that user on the User Management page. If you do not modify the user’s rights, the user has only the rights granted by default. Because you create internally authenticated users manually, you set the access rights when you create them.

If you configured management of access rights through LDAP groups, the access rights for users are based on their membership in LDAP groups. They receive the default access rights for the group that they belong to that has the highest level of access.

If they do not belong to any groups and you have configured group access, they receive the default user access rights configured in the authentication object for the LDAP server. If you configure group access, those settings override the default access setting in the platform settings policy.

Similarly, if you assign a user to specific user role lists in a RADIUS authentication object, the user receives all assigned roles, unless one or more of those roles are mutually incompatible. If a user is on the lists for two mutually incompatible roles, the user receives the role that has the highest level of access.

If the user does not belong to any lists and you have configured a default access role in the authentication object, the user receives that role. If you configure default access in the authentication object, those settings override the default access setting in the platform settings policy.

In a multidomain deployment, you can assign users roles in multiple domains. For example, you can assign a user read-only privileges in the Global domain, but Administrator privileges in a subdomain.

[Predefined User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000750)

[Custom User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000007cb)

[User Account Privileges](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000007ef)

[Managing User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00001384)

[User Role Escalation](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000015e9)

Predefined User Roles

The Firepower System includes ten predefined user roles that provide a range of access privilege sets to meet the needs of your organization. Note that 7000 and 8000 Series devices have access to only three of the ten predefined user roles: Administrator, Maintenance User, and Security Analyst.

Although you cannot edit predefined user roles, you can use their access privilege sets as the basis for custom user roles. In addition, you cannot configure them to escalate to another user role.

The following table briefly describes the predefined roles available to you.

Access Admin

Provides access to access control policy and associated features in the Policies menu. Access Admins cannot deploy policies.

Administrator

Administrators have access to all functionality; their sessions present a higher security risk if compromised, so you cannot make them exempt from login session timeouts.

You should limit use of the Administrator role for security reasons.

Discovery Admin

Provides access to network discovery, application detection, and correlation features in the Policies menu. Discovery Admins cannot deploy policies.

External Database User

Provides read-only access to the Firepower System database using an application that supports JDBC SSL connections. For the third-party application to authenticate to the Firepower System appliance, you must enable database access in the system settings. On the web interface, External Database Users have access only to online help-related options in the Help menu. Because this role’s function does not involve the web interface, access is provided only for ease of support and password changes.

Intrusion Admin

Provides access to all intrusion policy, intrusion rule, and network analysis policy features in the Policies and Objects menus. Intrusion Admins cannot deploy policies.

Maintenance User

Provides access to monitoring and maintenance features. Maintenance Users have access to maintenance-related options in the Health and System menus.

Network Admin

Provides access to access control, SSL inspection, DNS policy, and identity policy features in the Policies menu, as well as device configuration features in the Devices menus. Network Admins can deploy configuration changes to devices.

Security Analyst

Provides access to security event analysis features, and read-only access to health events, in the Overview, Analysis, Health, and System menus.

Security Analyst (Read Only)

Provides read-only access to security event analysis features and health event features in the Overview, Analysis, Health, and System menus.

Security Approver

Provides limited access to access control and associated policies and network discovery policies in the Policies menu. Security Approvers can view and deploy these policies, but cannot make policy changes.

Externally authenticated users, if assigned no other roles, have minimum access rights based on the settings in LDAP or RADIUS authentication objects and in platform settings. You can assign additional rights to these users, but to remove or change minimum access rights, you must perform the following tasks:

Move the user from one list to another in the authentication object or change the user's attribute value or group membership on the external authentication server.

Update platform settings.

Use the User Management page to remove the access from that user account.

Related Concepts
[User Account Privileges](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000007ef)

Custom User Roles

In addition to the predefined user roles, you can also create custom user roles with specialized access privileges. Custom user roles can have any set of menu-based and system permissions, and may be completely original or based on a predefined user role. Like predefined user roles, custom roles can serve as the default role for externally authenticated users. Unlike predefined roles, you can modify and delete custom roles.

Selectable permissions are hierarchical, and are based on the Firepower System menu layout. Permissions are expandable if they have sub-pages or if they have more fine-grained permissions available beyond simple page access. In that case, the parent permission grants page view access and the children granular access to related features of that page. Permissions that contain the word “Manage” grant the ability to edit and delete information that other users create.

|  |  |
| --- | --- |
| Tip | For pages or features not included in the menu structure, privileges are granted by parent or related pages. For example, the Modify Intrusion Policy privilege also allows you to modify network analysis policies.  |

You can apply restricted searches to a custom user role. These constrain the data a user may see in the event viewer. You can configure a restricted search by first creating a private saved search and selecting it from the Restricted Search drop-down menu under the appropriate menu-based permission.

When you configure a custom user role on a Firepower Management Center, all menu-based permissions are available for you to grant. When you configure a custom user role on a managed device, only some permissions are available — those relevant to device functions.

The selectable options under System Permissions allow you to create a user role that can make queries to the external database or escalate to the permissions of a target user role.

Optionally, instead of creating a new custom user role, you can export a custom user role from another appliance, then import it onto your appliance. You can then edit the imported role to suit your needs before you apply it.

[Example: Custom User Roles and Access Control](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2176-00000155)

Related Concepts
[User Account Privileges](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000007ef)[External Database Access Settings](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Management_Center_System_Configuration.html#ID-2241-000002b8)

Example: Custom User Roles and Access Control

You can create custom user roles for access control-related features to designate whether Firepower System users can view and modify access control and associated policies.

The following table lists custom roles that you could create and user permissions granted for each example. The table lists the privileges required for each custom role. In this example, Policy Approvers can view (but not modify) access control and intrusion policies. They can also deploy configuration changes to devices.

| Table 1 Example Access Control Custom Roles |
| --- |
| Custom Role Permission  | Example: Access Control Editor  | Example: Intrusion & Network Analysis Editor  | Example: Policy Approver  |
| Access Control  | yes  | no  | yes  |
| Access Control Policy  | yes  | no  | yes  |
| Modify Access Control Policy  | yes  | no  | no  |
| Intrusion Policy  | no  | yes  | yes  |
| Modify Intrusion Policy  | no  | yes  | no  |
| Deploy Configuration to Devices  | no  | no  | yes  |

User Account Privileges

The following sections provide a list of the configurable user permissions in the Firepower System and the predefined user roles that can access them. Not all permissions are available on managed devices; permissions available only on the Firepower Management Center are marked accordingly.

[Overview Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000803)

[Analysis Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000981)

[Policies Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000dbe)

[Devices Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-0000107f)

[Object Manager Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000010ef)

[Cisco AMP](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00001102)

[Deploy Configuration to Devices](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#reference_A30E167F2A8142B3BC3BF55814523235)

[System Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-0000117a)

[Help Menu](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-0000136b)

Overview Menu

The following table lists, in order, the user role privileges required to access each option in the Overview menu and whether the user role has access to the sub-permissions within. The Security Approver, Discovery Admin, Intrusion Admin, Access Admin, Network Admin, and External Database User roles have no permissions in the Overview menu.

| Table 2 Overview Menu |
| --- |
| Permission  | Admin  | Maint User  | Security Analyst  | Security Analyst (RO)  |
| Dashboards  | yes  | yes  | yes  | yes  |
| Manage Dashboards  | yes  | no  | no  | no  |
| Appliance Information Widget  | yes  | yes  | yes  | yes  |
| Appliance Status Widget (Management Center only)  | yes  | yes  | yes  | yes  |
| Correlation Events Widget  | yes  | no  | yes  | yes  |
| Current Interface Status Widget  | yes  | yes  | yes  | yes  |
| Current Sessions Widget  | yes  | no  | no  | no  |
| Custom Analysis Widget (Management Center only)  | yes  | no  | yes  | yes  |
| Disk Usage Widget  | yes  | yes  | yes  | yes  |
| Interface Traffic Widget  | yes  | yes  | yes  | yes  |
| Intrusion Events Widget (Management Centeronly)  | yes  | no  | yes  | yes  |
| Network Correlation Widget (Management Center only)  | yes  | no  | yes  | yes  |
| Product Licensing Widget (Management Center only)  | yes  | yes  | no  | no  |
| Product Updates Widget  | yes  | yes  | no  | no  |
| RSS Feed Widget  | yes  | yes  | yes  | yes  |
| System Load Widget  | yes  | yes  | yes  | yes  |
| System Time Widget  | yes  | yes  | yes  | yes  |
| White List Events Widget (Management Center only)  | yes  | no  | yes  | yes  |
| Reporting (Management Center only)  | yes  | no  | yes  | yes  |
| Manage Report Templates (Management Center only)  | yes  | no  | yes  | yes  |
| Summary  | yes  | no  | yes  | yes  |
| Intrusion Event Statistics (Management Center only)  | yes  | no  | yes  | yes  |
| Intrusion Event Performance  | yes  | no  | no  | no  |
| Intrusion Event Graphs (Management Center only)  | yes  | no  | yes  | yes  |
| Discovery Statistics (Management Center only)  | yes  | no  | yes  | yes  |
| Discovery Performance (Management Centeronly)  | yes  | no  | no  | no  |
| Connection Summary (Management Center only)  | yes  | no  | yes  | yes  |

Analysis Menu

The following table lists, in order, the user role privileges required to access each option in the Analysis menu and whether the user role has access to the sub-permissions within. Permissions that appear multiple times under different headings will be listed on the table only where they first appear, except to indicate submenu headings. The Security Approver, Intrusion Admin, Access Admin, Network Admin, and External Database User roles have no permissions in the Analysis menu. The Analysis menu is only available on the Firepower Management Center.

| Table 3 Analysis Menu |
| --- |
| Menu  | Admin  | Discovery Admin  | Maint User  | Security Analyst  | Security Analyst (RO)  |
| Context Explorer  | yes  | no  | no  | yes  | yes  |
| Connection Events  | yes  | no  | no  | yes  | yes  |
| Modify Connection Events  | yes  | no  | no  | yes  | no  |
| Connection Summary Events  | yes  | no  | no  | yes  | yes  |
| Modify Connection Summary Events  | yes  | no  | no  | yes  | no  |
| Security Intelligence Events  | yes  | no  | no  | yes  | yes  |
| Modify Security Intelligence Events  | yes  | no  | no  | yes  | no  |
| Intrusion  | yes  | no  | no  | yes  | yes  |
| Intrusion Events  | yes  | no  | no  | yes  | yes  |
| Modify Intrusion Events  | yes  | no  | no  | yes  | no  |
| View Local Rules  | yes  | no  | no  | yes  | yes  |
| Reviewed Events  | yes  | no  | no  | yes  | yes  |
| Clipboard  | yes  | no  | no  | yes  | yes  |
| Incidents  | yes  | no  | no  | yes  | yes  |
| Modify Incidents  | yes  | no  | no  | yes  | no  |
| Files  | yes  | no  | no  | yes  | yes  |
| Malware Events  | yes  | no  | no  | yes  | yes  |
| Modify Malware Events  | yes  | no  | no  | yes  | no  |
| File Events  | yes  | no  | no  | yes  | yes  |
| Modify File Events  | yes  | no  | no  | yes  | no  |
| Captured Files  | yes  | no  | no  | yes  | yes  |
| Modify Captured Files  | yes  | no  | no  | yes  | no  |
| File Trajectory  | yes  | no  | no  | yes  | yes  |
| File Download  | yes  | no  | no  | yes  | yes  |
| Dynamic File Analysis  | yes  | no  | no  | yes  | no  |
| Hosts  | yes  | no  | no  | yes  | yes  |
| Network Map  | yes  | no  | no  | yes  | yes  |
| Hosts  | yes  | no  | no  | yes  | yes  |
| Modify Hosts  | yes  | no  | no  | yes  | no  |
| Indications of Compromise  | yes  | no  | no  | yes  | yes  |
| Modify Indications of Compromise  | yes  | no  | no  | yes  | no  |
| Servers  | yes  | no  | no  | yes  | yes  |
| Modify Servers  | yes  | no  | no  | yes  | no  |
| Vulnerabilities  | yes  | no  | no  | yes  | yes  |
| Modify Vulnerabilities  | yes  | no  | no  | yes  | no  |
| Host Attributes  | yes  | no  | no  | yes  | yes  |
| Modify Host Attributes  | yes  | no  | no  | yes  | no  |
| Applications  | yes  | no  | no  | yes  | yes  |
| Application Details  | yes  | no  | no  | yes  | yes  |
| Modify Application Details  | yes  | no  | no  | yes  | no  |
| Host Attribute Management  | yes  | no  | no  | no  | no  |
| Discovery Events  | yes  | no  | no  | yes  | yes  |
| Modify Discovery Events  | yes  | no  | no  | yes  | no  |
| Users  | yes  | yes  | no  | yes  | yes  |
| User Activity  | yes  | yes  | no  | yes  | yes  |
| Modify User Activity Events  | yes  | yes  | no  | yes  | no  |
| Users  | yes  | yes  | no  | yes  | yes  |
| Modify Users  | yes  | yes  | no  | yes  | no  |
| Vulnerabilities  | yes  | no  | no  | yes  | yes  |
| Third-party Vulnerabilities  | yes  | no  | no  | yes  | yes  |
| Modify Third-party Vulnerabilities  | yes  | no  | no  | yes  | no  |
| Correlation  | yes  | yes  | no  | yes  | yes  |
| Correlation Events  | yes  | yes  | no  | yes  | yes  |
| Modify Correlation Events  | yes  | yes  | no  | yes  | no  |
| White List Events  | yes  | yes  | no  | yes  | yes  |
| Modify White List Events  | yes  | yes  | no  | yes  | no  |
| White List Violations  | yes  | yes  | no  | yes  | yes  |
| Remediation Status  | yes  | yes  | no  | no  | no  |
| Modify Remediation Status  | yes  | yes  | no  | no  | no  |
| Custom  | yes  | no  | no  | yes  | yes  |
| Custom Workflows  | yes  | no  | no  | yes  | yes  |
| Manage Custom Workflows  | yes  | no  | no  | yes  | yes  |
| Custom Tables  | yes  | no  | no  | yes  | yes  |
| Manage Custom Tables  | yes  | no  | no  | yes  | yes  |
| Search  | yes  | no  | yes  | yes  | yes  |
| Manage Search  | yes  | no  | no  | no  | no  |
| Bookmarks  | yes  | no  | no  | yes  | yes  |
| Manage Bookmarks  | yes  | no  | no  | yes  | yes  |
| Application Statistics  | yes  | no  | no  | yes  | yes  |
| Geolocation Statistics  | yes  | no  | no  | yes  | yes  |
| User Statistics  | yes  | no  | no  | yes  | yes  |
| URL Category Statistics  | yes  | no  | no  | yes  | yes  |
| URL Reputation Statistics  | yes  | no  | no  | yes  | yes  |
| DNS Queries by Record Types  | yes  | no  | no  | yes  | yes  |
| SSL Statistics  | yes  | no  | no  | yes  | yes  |
| Intrusion Event Statistics by Application  | yes  | no  | no  | yes  | yes  |
| Intrusion Event Statistics by User  | yes  | no  | no  | yes  | yes  |
| Security Intelligence Category Statistics  | yes  | no  | no  | yes  | yes  |
| File Storage Statistics by Disposition  | yes  | no  | no  | yes  | yes  |
| File Storage Statistics by Type  | yes  | no  | no  | yes  | yes  |
| Dynamic File Analysis Statistics  | yes  | no  | no  | yes  | yes  |

Policies Menu

The following table lists, in order, the user role privileges required to access each option in the Policies menu and whether the user roles has access to the sub-permissions within. The External Database User, Maintenance User, Security Analyst, and Security Analyst (Read Only) roles have no permissions in the Policies menu. The Policies menu is only available on the Firepower Management Center.

Note that the Intrusion Policy and Modify Intrusion Policy privileges also allow you to create and modify network analysis policies.

| Table 4 Policies Menu |
| --- |
| Menu  | Access Admin  | Admin  | Discovery Admin  | Intrusion Admin  | Network Admin  | Security Approver  |
| Access Control  | yes  | yes  | no  | no  | yes  | yes  |
| Access Control Policy  | yes  | yes  | no  | no  | yes  | yes  |
| Modify Access Control Policy  | yes  | yes  | no  | no  | yes  | no  |
| Modify Administrator Rules  | yes  | yes  | no  | no  | yes  | no  |
| Modify Root Rules  | yes  | yes  | no  | no  | yes  | no  |
| Intrusion Policy  | no  | yes  | no  | yes  | no  | yes  |
| Modify Intrusion Policy  | no  | yes  | no  | yes  | no  | no  |
| Malware & File Policy  | yes  | yes  | no  | no  | no  | yes  |
| Modify Malware & File Policy  | yes  | yes  | no  | no  | no  | no  |
| DNS Policy  | yes  | yes  | no  | no  | yes  | yes  |
| Modify DNS Policy  | yes  | yes  | no  | no  | yes  | no  |
| Identity Policy  | yes  | yes  | no  | no  | yes  | no  |
| Modify Identity Policy  | yes  | yes  | no  | no  | yes  | no  |
| Modify Administrator Rules  | yes  | yes  | no  | no  | yes  | no  |
| Modify Root Rules  | yes  | yes  | no  | no  | yes  | no  |
| SSL Policy  | yes  | yes  | no  | no  | yes  | yes  |
| Modify SSL Policy  | yes  | yes  | no  | no  | yes  | no  |
| Modify Administrator Rules  | yes  | yes  | no  | no  | yes  | no  |
| Modify Root Rules  | yes  | yes  | no  | no  | yes  | no  |
| Network Discovery  | no  | yes  | yes  | no  | no  | yes  |
| Custom Fingerprinting  | no  | yes  | yes  | no  | no  | no  |
| Modify Custom Fingerprinting  | no  | yes  | yes | no  | no  | no  |
| Custom Topology  | no  | yes  | yes  | no  | no  | no  |
| Modify Custom Topology  | no  | yes  | no  | no  | no  | no  |
| Modify Network Discovery  | no  | yes  | yes  | no  | no  | no  |
| Application Detectors  | no  | yes  | yes  | no  | no  | no  |
| Modify Application Detectors  | no  | yes  | yes  | no  | no  | no  |
| User 3rd Party Mappings  | no  | yes  | yes  | no  | no  | no  |
| Modify User 3rd Party Mappings  | no  | yes  | no  | no  | no  | no  |
| Custom Product Mappings  | no  | yes  | yes  | no  | no  | no  |
| Modify Custom Product Mappings  | no  | yes  | no  | no  | no  | no  |
| Correlation  | no  | yes  | no  | no  | no  | no  |
| Policy Management  | no  | yes  | no  | no  | no  | no  |
| Modify Policy Management  | no  | yes  | yes  | no  | no  | no  |
| Rule Management  | no  | yes  | no  | no  | no  | no  |
| Modify Rule Management  | no  | yes  | yes  | no  | no  | no  |
| White List  | no  | yes  | no  | no  | no  | no  |
| Modify White List  | no  | yes  | yes  | no  | no  | no  |
| Traffic Profiles  | no  | yes  | no  | no  | no  | no  |
| Modify Traffic Profiles  | no  | yes  | yes  | no  | no  | no  |
| Actions  | no  | yes  | yes  | no  | no  | yes  |
| Alerts  | no  | yes  | yes  | no  | no  | yes  |
| Impact Flag Alerts  | no  | yes  | yes  | no  | no  | no  |
| Modify Impact Flag Alerts  | no  | yes  | yes  | no  | no  | no  |
| Discovery Event Alerts  | no  | yes  | yes  | no  | no  | no  |
| Modify Discovery Event Alerts  | no  | yes  | yes  | no  | no  | no  |
| Email  | no  | yes  | no  | yes  | no  | no  |
| Modify Email  | no  | yes  | no  | yes  | no  | no  |
| Modify Alerts  | no  | yes  | yes  | no  | no  | no  |
| Scanners  | no  | yes  | yes  | no  | no  | no  |
| Scan Results  | no  | yes  | yes  | no  | no  | no  |
| Modify Scan Results  | no  | yes  | yes  | no  | no  | no  |
| Modify Scanners  | no  | yes  | yes  | no  | no  | no  |
| Groups  | no  | yes  | no  | no  | no  | no  |
| Modify Groups  | no  | yes  | yes  | no  | no  | no  |
| Modules  | no  | yes  | no  | no  | no  | no  |
| Modify Modules  | no  | yes  | yes  | no  | no  | no  |
| Instances  | no  | yes  | no  | no  | no  | no  |
| Modify Instances  | no  | yes  | yes  | no  | no  | no  |

Devices Menu

The Devices menu table lists, in order, the user role privileges required to access each option in the Devices menu and the sub-permissions within. The Discovery Admin, External Database User, Intrusion Admin, Maintenance User, Security Analyst, and Security Analyst (Read Only) have no permissions in the Devices menu. The Devices menu is only available on the Firepower Management Center.

| Table 5 Devices Menu |
| --- |
| Menu  | Access Admin  | Admin  | Network Admin  | Security Approver  |
| Device Management  | no  | yes  | yes  | yes  |
| Modify Devices  | no  | yes  | yes  | no  |
| NAT  | yes  | yes  | yes  | yes  |
| NAT List  | yes  | yes  | yes  | yes  |
| Modify NAT Policy  | yes  | yes  | yes  | no  |
| VPN  | no  | yes  | yes  | yes  |
| Modify VPN  | no  | yes  | yes  | no  |
| Device Management  | no  | yes  | yes  | no  |
| Modify Devices  | no  | yes  | yes  | no  |

Object Manager Menu

The Object Manager menu table lists, in order, the user role privileges required to access each option in the Object Manager menu and the sub-permission within. The Discovery Admin, Security Approver, Maintenance User, External Database User, Security Analyst, and Security Analyst (Read Only) have no permissions in the Object Manager menu. The Object Manager menu is available only on theFirepower Management Center.

| Table 6 Object Manager Menu |
| --- |
| Menu  | Access Admin  | Admin  | Intrusion Admin  | Network Admin  |
| Object Manager  | yes  | yes  | no  | yes  |
| Rule Editor  | no  | yes  | yes  | no  |
| Modify Rule Editor  | no  | yes  | yes  | no  |
| NAT List  | yes  | yes  | no  | yes  |
| Modify Object Manager  | no  | yes  | no  | no  |

Cisco AMP

The Cisco AMP permission is available only to the Administrator user role. This permission is available only on the Firepower Management Center.

Deploy Configuration to Devices

The Deploy Configuration to Devices permission is available to the Administrator, Network Admin, and Security Approver roles. This permission is available only on the Firepower Management Center.

System Menu

The following table lists, in order, the user role privileges required to access each option in the System menu and whether the user role has access to the sub-permissions within. The External Database User role has no permissions in the System Menu.

| Table 7 System Menu |
| --- |
| Menu  | Access Admin  | Admin  | Discovery Admin  | Intrusion Admin  | Maint User  | Network Admin  | Security Approver  | Security Analyst  | Security Analyst (RO)  |
| Configuration  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Domains  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Integration  | no  | yes  | no  | no  | no  | yes  | yes  | no  | no  |
| Cisco CSI  | yes  | yes  | no  | no  | no  | yes  | yes  | no  | no  |
| Identity Realms (Management Center only)  | yes  | yes  | no  | no  | no  | yes  | yes  | no  | no  |
| Modify Identity Realms (Management Center only)  | yes  | yes  | no  | no  | no  | yes  | no  | no  | no  |
| Identity Sources (Management Center only)  | yes  | yes  | no  | no  | no  | yes  | yes  | no  | no  |
| Modify Identity Sources (Management Center only)  | yes  | yes  | no  | no  | no  | yes  | no  | no  | no  |
| eStreamer  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Host Input Client (Management Center only)  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Smart Software Satellite (Management Center only)  | yes  | yes  | no  | no  | no  | yes  | yes  | no  | no  |
| Modify Smart Software Satellite (Management Center only)  | yes  | yes  | no  | no  | no  | yes  | no  | no  | no  |
| User Management  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Users  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| User Roles  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| External Authentication (Management Center only)  | no  | yes  | yes  | no  | no  | no  | no  | no  | no  |
| Updates  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Rule Updates (Management Center only)  | no  | yes  | no  | yes  | no  | no  | no  | no  | no  |
| Rule Update Import Log (Management Center only)  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Licenses  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Smart Licences  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Modify Smart Licenses  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Classic Licenses  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Health (Management Center only)  | no  | yes  | no  | no  | yes  | no  | no  | yes  | yes  |
| Health Policy (Management Center only)  | no  | yes  | no  | no  | yes  | no  | no  | yes  | no  |
| Modify Health Policy (Management Center only)  | no  | yes  | no  | no  | yes  | no  | no  | yes  | no  |
| Apply Health Policy (Management Center only)  | no  | yes  | no  | no  | yes  | no  | no  | yes  | no  |
| Health Events (Management Center only)  | no  | yes  | no  | no  | yes  | no  | no  | yes  | yes  |
| Modify Health Events (Management Center only)  | no  | yes  | no  | no  | yes  | no  | no  | yes  | no  |
| Monitoring  | no  | yes  | no  | no  | yes  | yes  | yes  | yes  | no  |
| Audit  | no  | yes  | no  | no  | yes  | no  | no  | no  | no  |
| Modify Audit Log  | no  | yes  | no  | no  | yes  | no  | no  | no  | no  |
| Syslog  | no  | yes  | no  | no  | yes  | no  | no  | no  | no  |
| Statistics  | no  | yes  | no  | no  | yes  | no  | no  | no  | no  |
| Tools  | no  | yes  | no  | no  | yes  | no  | no  | yes  | no  |
| Backup Management  | no  | yes  | no  | no  | yes  | no  | no  | no  | no  |
| Restore Backup  | no  | yes  | no  | no  | yes  | no  | no  | no  | no  |
| Scheduling  | no  | yes  | no  | no  | yes  | no  | no  | no  | no  |
| Delete Other Users’ Scheduled Tasks  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Import/Export  | no  | yes  | no  | no  | no  | no  | no  | no  | no  |
| Discovery Data Purge (Management Center only)  | no  | yes  | no  | no  | no  | no  | no  | yes  | no  |
| Whois (Management Center only)  | no  | yes  | no  | no  | yes  | no  | no  | yes  | yes  |

Help Menu

The Help menu and its permissions are accessible to all user roles. You cannot restrict Help menu options.

Managing User Roles

| Smart License  | Classic License  | Supported Devices  | Supported Domains  | Access  |
| --- | --- | --- | --- | --- |
| Any  | Any  | Any  | Any  | Admin  |

Each Firepower System user is associated with a user access role or roles. These user roles are assigned permissions that determine access to menus and other options in the system. For example, an analyst needs access to event data to analyze the security of your network, but might not require access to administrative functions for the Firepower System itself. You can grant Security Analyst access to analysts while reserving the Administrator role for the user or users managing the Firepower System.

The Firepower System includes ten predefined user roles designed for a variety of administrators and analysts. These predefined user roles have a set of predetermined access privileges.

You can also create custom user roles with more granular access privileges.

You can also restrict the data that a user role can view in the event viewer by applying a restricted search to that role. To create a custom role with restricted access, you must choose the tables you want to restrict from the Menu Based Permissions list, then choose private saved searches from the Restrictive Search drop-down lists.

You cannot delete predefined user roles, but you can delete custom roles that are no longer necessary. If you want to disable a custom role without removing it entirely, you can deactivate it instead. Note that you cannot delete your own user role or a role that is set as a default user role in a platform settings policy.

Procedure

|  |  |
| --- | --- |
| Step 1    | Choose System > Users.  |
| Step 2    | Click the User Roles tab.  |
| Step 3    | Manage user roles: Activate — Activate or deactivate a predefined user role as described in [Activating and Deactivating User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000013bb). Create — Create custom user roles as described in [Creating Custom User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-000013e0) Copy — Copy an existing user role to create a new custom user role as described in [Copying User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00001413). Edit — Edit a custom user role as described in [Editing Custom User Roles](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#task_9BA004CE32094C40AC6A4CF204D84CFE). Delete — Click the delete icon (https://www.cisco.com/c/dam/en/us/td/i/300001-400000/370001-380000/371001-372000/371631.tif/_jcr_content/renditions/371631.jpg) next to the custom role you want to delete. If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

|  |  |
| --- | --- |
| Note     | If a deleted role is the only role assigned to a given user, that user can log in and access the User Preferences menu, but is otherwise unable to access the Firepower System.  |

 |

Activating and Deactivating User Roles

| Smart License  | Classic License  | Supported Devices  | Supported Domains  | Access  |
| --- | --- | --- | --- | --- |
| Any  | Any  | Any  | Any  | Admin  |

You cannot delete predefined user roles, but you can deactivate them. Deactivating a role removes that role and all associated permissions from any user who is assigned that role.

In a multidomain deployment, the system displays custom user roles created in the current domain, which you can edit. It also displays custom user roles created in ancestor domains, which you cannot edit. To view and edit custom user roles in a lower domain, switch to that domain.

Firepower System User Authentication

When a user logs into the web interface on a Firepower Management Center or a managed device, the appliance looks for a match for the user name and password in the local list of users. This process is called authentication.

There are two types of authentication:

internal authentication — The system checks the list in the local database for the user.

external authentication — The system checks the list in the local database for the user and, if the user is not present on that list, queries an external authentication server for its user list.

The authentication process is illustrated below.



When you create a user account, you specify either internal or external authentication for that user.

[Internal Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000025)

[External Authentication](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.html#ID-2263-00000040)

Internal Authentication

In internal authentication, user credentials are verified against records in the internal Firepower System database. This is the default authentication type.

You set the access rights for internal authentication users when you create the user's account.

|  |  |
| --- | --- |
| https://www.cisco.com/c/dam/en/us/td/i/templates/note.gifNote | When an internally authenticated user is converted to external authentication, you cannot revert to internal authentication.  |