BIG-IP® System: User Account Administration

Version 12.0

Table of Contents

Legal Notices

Legal notices

Publication Date

This document was published on April 25, 2018.

Publication Number

MAN-0540-01

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, AskF5, ASM, BIG-IP, BIG-IP EDGE GATEWAY, BIG-IQ, Cloud Extender, Cloud Manager, CloudFucious, Clustered Multiprocessing, CMP, COHESION, Data Manager, DDoS Frontline, DDoS SWAT, Defense.Net, defense.net [DESIGN], DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Mobile, Edge Mobility, Edge Portal, ELEVATE, EM, ENGAGE, Enterprise Manager, F5, F5 [DESIGN], F5 Agility, F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FCINCO, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, iCall, iControl, iHealth, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, LineRate, LineRate Point, LineRate Precision, LineRate Systems [DESIGN], Local Traffic Manager, LROS, LTM, Message Security Manager, MobileSafe, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Ready Defense, Real Traffic Policy Builder, SalesXchange, ScaleN, SDAS (except in Japan), SDC, Signalling Delivery Controller, Solutions for an application world, Software Designed Application Services, Silverline, SSL Acceleration, SSL Everywhere, StrongBox, SuperVIP, SYN Check, SYNTHESIS, TCP Express, TDR, TechXchange, TMOS, TotALL, TDR, TMOS, Traffic Management Operating System, Traffix, Traffix [DESIGN], Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*

Link Controller Availability

This product is not currently available in the United States.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Introduction to User Account Management

Purpose of BIG-IP user accounts

An important part of managing the BIG-IP® system is creating and managing user accounts for BIG-IP system administrators. By creating user accounts for system administrators, you provide additional layers of security. User accounts ensure that the system:

- Verifies the identity of users logging into the system
- Controls user access to system resources

User access components

To control user authentication and authorization, you assign passwords, user roles, administrative partition access, and user roles to the BIG-IP® system user accounts:

- *Passwords* allow you to authenticate your users when they attempt to log in to the BIG-IP system.
- *User roles* and *partitions access* allow you to control user access to BIG-IP system resources.
- *Terminal access* controls whether or not a user can access any command line interfaces on the system.

Types of user accounts

The types of user accounts on the BIG-IP® system are:

The root account

Every BIG-IP system has an account named `root`. A user who logs in to the system using the `root` account has full access to all BIG-IP system resources, including all administrative partitions and command line interfaces.

The admin account

Every BIG-IP system has an account named `admin`. A user who logs in to the system using the `admin` account has the Administrator role, which grants the user full access to all BIG-IP system resources, including all administrative partitions on the system. By default, the `admin` user account has access to the BIG-IP Configuration utility only. However, users logged in with this account can grant themselves access to both `tmsh` and the advanced shell. Although the BIG-IP system creates this account automatically, you must still assign a password to the account before you can use it. To initially set the password for the admin account, you must run the Setup utility. To change its password later, you use the BIG-IP Configuration utility's Users screens.

Local accounts

A BIG-IP user with the correct user role can create other local user accounts for BIG-IP system administration. Each local user account on the BIG-IP system has one or more user roles assigned to the account (one per partition), as well as permissions related to `tmsh` and Bash shell access.

Remote accounts

If your organization stores user accounts on a remote authentication server (such as an Active Directory server), you can configure the BIG-IP system to control access to BIG-IP configuration objects for all BIG-IP user accounts stored on the remote server. In this case, the remote server authenticates each BIG-IP user at login time, while the BIG-IP system itself grants the specified access control permissions.

Note: *You are not required to have any user accounts on the BIG-IP system other than the* `root` *and* `admin` *accounts. However, F5 Networks® recommends that you create other user accounts, as a way to intelligently control administrator access to system resources.*

Changing the root and admin account passwords

If you have an Administrator user role, you can use the BIG-IP® Configuration utility to change the passwords of the `root` and `admin` accounts.

1. On the Main tab, expand **System**, and click **Platform**.
2. For the **Root Account** setting, type a new password in the **Password** box, and re-type the new password in the **Confirm** box.
3. For the **Admin Account** setting, type a new password in the **Password** box, and re-type the new password in the **Confirm** box.
4. Click the **Update** button.

Administrative Partitions

What is an administrative partition?

An *administrative partition* is a logical container that you create, containing a defined set of BIG-IP® system objects. If you have the Administrator or User Manager user role assigned to your BIG-IP system user account, you can create administrative partitions to control other users' access to BIG-IP objects. More specifically, when a specific set of objects resides in a partition, you can give certain users the authority to view and manage the objects in that partition only, rather than to all objects on the BIG-IP system. This gives a finer granularity of administrative control. For example, a user that is assigned access to partition `A` with the role of Operator on that partition can mark nodes up or down, but only in that partition. You assign user access to partitions when you configure BIG-IP system user accounts.

The following illustration shows an example of user objects within partitions on the BIG-IP system.

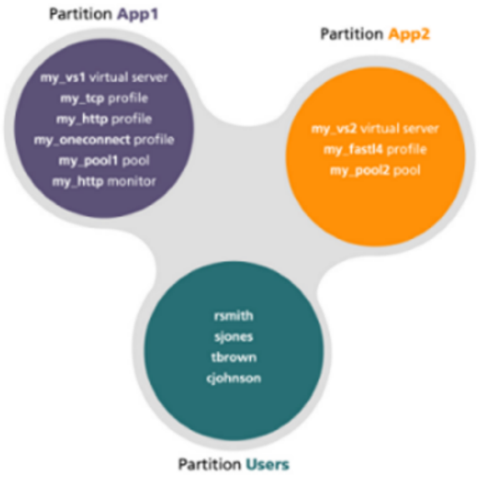


Figure 1: Sample administrative partitions on the BIG-IP system

For every administrative partition on the BIG-IP system, the system creates an equivalent high-level folder with an equivalent name.

Creating an administrative partition

You perform this task to create an administrative partition. An *administrative partition* creates an access control boundary for users and applications.

1. On the Main tab, expand **System** and click **Users**.
   The Users List screen opens.
2. On the menu bar, click **Partition List**.
3. Click **Create**.

The New Partition screen opens.

4. In the **Partition Name** field, type a unique name for the partition.
   An example of a partition name is `Spanned_VIP`.
5. Type a description of the partition in the **Description** field.
   This field is optional.
6. For the **Device Group** setting, choose an action:

Action	Result
Retain the default value.	Choose this option if you want the folder corresponding to this partition to inherit the value of the device group attribute from folder `root`.
Clear the check box and select the name of a device group.	Choose this option if you do not want the folder corresponding to this partition to inherit the value of the device group attribute from folder `root`.

7. For the **Traffic Group** setting, choose an action:

Action	Result
Retain the default value.	Choose this option if you want the folder corresponding to this partition to inherit the value of the traffic group attribute from folder `root`.
Clear the check box and select the name of a traffic group.	Choose this option if you do not want the folder corresponding to this partition to inherit the value of the traffic group attribute from folder `root`.

8. Click **Finished**.

The new partition appears in the partition list.

Relationship of partitions to user accounts

Partitions have a special relationship to user accounts. With respect to partitions and user accounts, you can:

Assign partition access to user accounts

You can configure a user account to grant the user access to one or more partitions, and you can assign a different user role to a user for each partition. Moreover, you can grant an individual user access to all partitions instead of to specific partitions only. Note that assigning partition access to a user does not necessarily give the user full access to all objects in the partition; the user role assigned to the user determines the type of access that the user has to each type of object in the partition.

Create user accounts as partitioned objects

Like other types of objects on the system, user account objects also reside in partitions. Placing user account objects into partitions controls other users' administrative access to those user accounts. Also, like other object types, a BIG-IP® system user account cannot reside in more than one partition simultaneously. When you first install the BIG-IP system, every existing user account (`root` and `admin`) resides in partition `Common`.

Important: *The partition in which a user account object resides does not affect the partition or partitions to which that user is granted access to manage other BIG-IP objects.*

About partition Common

During BIG-IP® system installation, the system automatically creates a partition named `Common`. At a minimum, this partition contains all of the BIG-IP objects that the system creates as part of the installation process. Until you create other partitions on the system, all objects that you or other users create or manage automatically reside in partition `Common`.

With respect to permissions, all users on the system except those with a user role of No Access have read access to objects in partition `Common`. When a user displays a list of a particular type of configuration object, the system displays not only the objects of that type within the user's current partition, but also the same type of object in `Common`. For example, if a user lists all virtual servers within the user's current partition (such as partition `A`), the list also shows the virtual servers in `Common`. In this case, unless the user has write access to `Common`, the virtual servers in `Common` are read-only for that user.

Some users, such as those with the user role of Administrator, can also create, update, and delete objects in partition `Common`. No user can delete partition `Common` itself.

About the current partition

The *current partition* is the specific partition to which the system is currently set for a logged-in user.

A user who has been granted access to one or more partitions, as well as all partitions, can actively select the current partition, that is, the specific partition he or she wants to view or manage. For example:

- If user `jsmith` has access to multiple partitions on the system, then before creating or managing any object on the BIG-IP® system, she must select the partition that she wants to be the current partition. After setting the current partition, any object that she creates resides in that partition, and she can modify or delete only the objects that reside in that partition until she sets the current partition to a different partition. Also, regardless of the current partition that jsmith selects, she also has read access to objects in partition `Common`.
- Conversely, if user `rjones` has access to partition `A` only, then any object that he creates while logged in to the BIG-IP system resides in partition `A`. Although he can view objects in partition `Common`, he cannot select `Common` as his current partition because he has read access only. For user `rjones`, partition `A` is automatically his current partition when he logs in to the system, and he cannot change the current partition to create objects in another partition.

Setting the current partition

Before you perform this task, confirm that your user account grants you permission to access more than one partition on the BIG-IP system.

You perform this task to change the current administrative partition on the BIG-IP® system. You change the partition when you want to create or manage BIG-IP configuration objects in a different partition than the current partition. For example, if the current partition is set to `Common`, but you have access to partition `A` and want to create a load balancing pool and virtual server in that partition, you must change the current partition to partition `A` before creating those objects.

1. Access the BIG-IP ®Configuration utility.

2. Locate the **Partition** list in the upper right corner of the BIG-IP Configuration utility screen, to the left of the **Log out** button.
3. From the **Partition** list, select the partition in which you want to create or manage objects.

After you perform this task, any configuration objects that you create or manage reside in the selected partition. Any objects that you can view reside in the selected partition or partition `Common`. Also, each screen of the BIG-IP Configuration utility displays the role currently assigned to the user, based on the current partition.

Object referencing between partitions

Certain BIG-IP® system objects, such as virtual servers, can reference other objects. Examples of objects that a virtual server can reference are pools, profiles, and iRules®. On the BIG-IP system, there are rules for object referencing with respect to the administrative partitions in which those objects reside.

Valid object referencing

The rules for valid object referencing are:

- An object and the object that it references can reside in the same partition.
- An object can reside in a user-created partition, such as partition `A`, while the object it references resides in partition **Common**.
- An iRule can reference any object, regardless of the partition in which the referenced object resides. For example, an iRule that resides in partition `A` can contain a pool statement that specifies a pool residing in partition `B`. Neither object is required to reside in `Common`.

Invalid object referencing

Object referencing is restricted in these ways:

- An object cannot reside in partition `Common`, while the object that it references resides in a different partition. For example, you cannot have a virtual server residing in `Common` while the pool that the virtual server references resides in partition `A`.
- An object cannot reside in one user-created partition, while the object that it references resides in another user-created partition. For example, you cannot have a virtual server residing in `A` while the pool that the virtual server references resides in partition `B`.

User Roles

What is a user role?

A *User role* is a property of a BIG-IP® administrative user account. For each BIG-IP user account, you can assign a different user role to each administrative partition to which you the user has access. This allows you to assign multiple user roles to each user account on the system.

A user role controls the following:

The types of resources that the user can manage

User roles define the types of resources, or objects, that a user can manage. For example, a user with the role of Operator can enable or disable nodes and pool members only. By contrast, a user with the Guest role cannot manage any BIG-IP system resources.

The tasks that a user can perform

For example, a user with the role of Operator can enable or disable nodes and pool members, but cannot create, modify, or delete them. Conversely, a user with the Manager role can perform all tasks related to objects within a partition, except for tasks related to user accounts.

The BIG-IP system offers several different user roles that you can choose from when assigning roles to a user account. Each user role grants a different level and type of permissions to the user.

***Note:** You must have an Administrator or User Manager user role to assign user roles to a BIG-IP user account.*

Assigning roles to a user account

Before performing this task, ensure that you have a user role of Administrator or that you have a role of User Manager for the relevant partition.

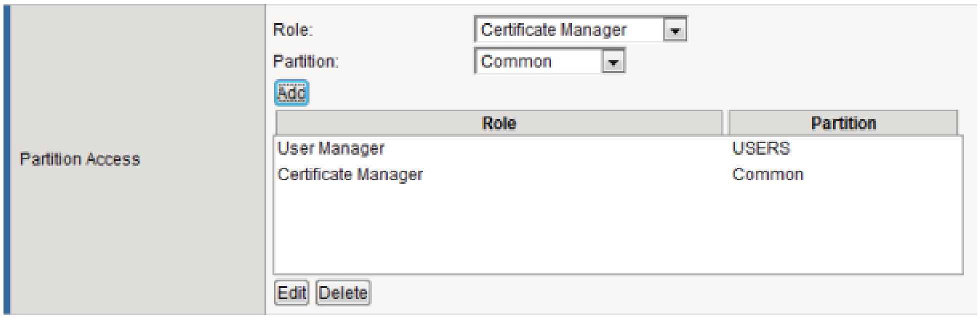
You perform this task to change the user roles that are assigned to a user account. You can assign a different role for each partition to which the user has access. By default, the user role that the BIG-IP® system assigns to a user account on each partition is No Access.

***Important:** If you are performing this task while the user is logged into the system through `tmsh`, the BIG-IP system terminates the user's `tmsh` session when the user subsequently issues another `tmsh` command. This behavior ensures that the user is notified of the change in permissions and that data integrity is maintained.*

1. Access the BIG-IP ® Configuration utility.
2. In the upper-left corner of the screen, confirm that the **Partition** list is set to the partition in which the user account that you want to modify resides.
3. On the Main tab, click **System** > **Users**.

   The BIG-IP system displays the list of user accounts that reside in the current partition and in partition `Common`. Note that all users except those with a user role of No Access have at least read access to partition `Common`.

4. In the User Name column, click the user account name.
5. For the **Partition Access** setting:
   a) From the **Role** list to select a user role.
   b) From the **Partition** list, select a partition name.
   c) Click the **Add** button.
   A user role pertaining to a partition now appears in the box.
   d) Repeat these steps for each partition to which you want to assign a role for this user.



Partition Access

Role: Certificate Manager

Partition: Common

Role	Partition
User Manager	USERS
Certificate Manager	Common

Figure 2: Granting partition access to a BIG-IP user account

After you configure this setting, one or more role-partition combinations are specified for assignment to this user account.

6. Click the **Update** button.

User roles and administrative partitions

As a BIG-IP® user with an Administrator or User Manager user role, you can assign user roles to other BIG-IP user accounts. Specifically, for each BIG-IP user account, you can assign a specific user role to each administrative partition to which you grant the user access. In this way, you can control the BIG-IP configuration objects that the user can manage, as well as the types of actions the user can perform on those objects.

Important: *When a local user with multiple roles logs in to the system, the system applies the most powerful of those roles to the user and sets the current partition to the partition associated with that role. This role remains in effect until the user changes the current partition or the user logs off the system.*

About universal access

When you create a BIG-IP administrative user account, you can grant the user access to all administrative partitions on the system, instead of to specific partitions only. This type of access is known as *universal access*. When you grant universal access to a user, you can assign only one user role, which applies to all partitions on the system for that user.

For example, if you create a user account and assign the role of Operator with the partition access set to **All**, the user has Operator permissions within all partitions on the system. You cannot assign any other user roles to that user account.

You can assign universal access to any user role except No Access. Moreover, certain user roles on the system automatically provide a user with universal access, and you cannot change this. The user roles that automatically and permanently provide universal access are:

- Administrator
- Resource Administrator
- Application Security Administrator
- Auditor

Note: *When you assign the user role No Access to a user account, the role always applies to all partitions on the system.*

User roles on the BIG-IP system

This table lists and describes the various user roles that you can assign to a BIG-IP® user account.

User role	Description	Partition scope
Administrator	This is the most powerful user role on the system and grants users complete access to all objects on the system. Users with this role cannot have other user roles on the system.	All partitions (mandatory)
Resource Administrator	This role grants a user access to all objects on the system except BIG-IP user accounts. With respect to user accounts, a user with this role can view a list of all user accounts on the system but cannot view or change user account properties except for their own user account. Users with this role cannot have other user roles on the system.	All partitions (mandatory)
User Manager	This role grants a user permission to manage BIG-IP user accounts. When granted terminal access, a user with this role has access to TMSH only.	Specific partitions or all partitions (optional)
Manager	This role grants a user permission to manage a subset of local traffic objects. When granted terminal access, a user with this role has access to TMSH only.	Specific partitions or all partitions (optional)
Certificate Manager	This role grants a user permission to manage digital certificates and keys, as well as perform Federal Information Processing Standard (FIPS) operations. When granted terminal access, a user with this role has access to TMSH only.	Specific partitions or all partitions (optional)
iRule Manager	This role grants a user permission to create, modify, view, and delete iRules. Users with this role cannot affect the way that an iRule is deployed. For example, a user with this role can create an iRule but cannot assign the iRule to a virtual server or move the iRule from one virtual server to another. When granted terminal access, a user with this role has access to TMSH only.	Specific partitions or all partitions (optional)
Application Editor	This role grants a user permission to modify a subset of local traffic objects. When granted terminal access, a user with this role has access to TMSH only.	Specific partitions or all partitions (optional)
Acceleration Policy Editor	This role grants a user permission to manage BIG-IP Application Acceleration Manager™ policies. Users with this role cannot have other user roles on the system.	All partitions (mandatory)

User role	Description	Partition scope
Firewall Manager	This role grants a user permission to manage all firewall rules and supporting objects. Notably, the Firewall Manager role has no permission to create, update, or delete non-network firewall configurations, including Application Security or Protocol Security policies.	All partitions or a single partition
Application Security Administrator	This role grants a user permission to manage BIG-IP Application Security Manager™ (ASM®) configuration objects. This role is similar to the Administrator role but for ASM only. You can assign this role only when the BIG-IP system includes the ASM module. Users with this role cannot have other user roles on the system. When granted terminal access, a user with this role has access to TMSH only.	All partitions (mandatory)
Application Security Editor	This role grants a user permission to manage most parts of ASM. You can assign this role only when the BIG-IP system includes the ASM module. When granted terminal access, a user with this role has access to TMSH only.	Specific partitions or all partitions (optional)
Fraud Protection Manager	This role grants a user permission to configure the BIG-IP Fraud Protection Service (FPS) module. When granted terminal access, a user with this role has access to TMSH only.	Specific partitions or all partitions (optional)
Operator	This role grants a user permission to enable or disable nodes and pool members. When granted terminal access, a user with this role has access to TMSH only.	Specific partitions or all partitions (optional)
Auditor	This is a powerful role that grants read-only access to all configuration data on the system, except for ARP data, archives, and support tools. Users with this role cannot have other user roles on the system but can change their own user account password. When granted terminal access, a user with this role has access to TMSH only.	All partitions (mandatory)
Guest	This is the least powerful role on the system other than No Access. This role grants read-only access to all objects in the user's assigned partitions plus Common, except for: ARP data, archives, logs, support tools, SNMP configurations displayed in the BIG-IP Configuration utility, and other users' user accounts. A user with this role has write access to their own user account password. When granted terminal access, a user with this role has access to TMSH only.	Specific partitions or all partitions (optional)
No Access	This role blocks read and write access to any configuration objects and data on the BIG-IP system.	None

User role permissions

This table describes the permissions associated with each BIG-IP user role.

User role	Write access	Read-only access	No access
Administrator	All objects on the system	All objects on the system	Not applicable

User role	Write access	Read-only access	No access
Resource Administrator	All objects on the system except user accounts	All objects on the system	Not applicable
User Manager	User accounts in assigned partitions	Objects in assigned partitions plus `Common`	ARP entries, archives, SNMP configurations, logs, and support tools
Manager	Virtual servers, pool members, nodes, profiles, monitors, and iRules® in assigned partitions.	Objects in assigned partitions plus `Common`	ARP entries, archives, SNMP configurations, logs, and support tools
Certificate Manager	All digital certificates and FIPS operations in assigned partitions	Objects in assigned partitions plus `Common`	ARP entries, archives, SNMP configurations, logs, and support tools
iRule Manager	iRules in assigned partitions	Objects in assigned partitions plus `Common`	ARP entries, archives, SNMP configurations, logs, and support tools
Application Editor	Nodes, pools, pool members, and monitors in assigned partitions	Objects in assigned partitions plus `Common`	ARP entries, archives, SNMP configurations, logs, and support tools
Acceleration Policy Editor	All Application Acceleration Manager™ policy objects and profiles on the system	Most objects on the system	ARP entries, archives, SNMP configurations, logs, and support tools
Firewall Manager	All firewall rules and supporting objects in assigned partitions. To modify global and management port rules, Firewall Managers must have partition `Common` assigned to their accounts.	Objects in assigned partitions plus `Common`	ARP entries, archives, SNMP configurations, logs, and support tools
Application Security Administrator	All Application Security Manager™ security policy objects on the system	Objects in assigned partitions plus `Common`	ARP entries, archives, SNMP configurations, logs, and support tools
Application Security Editor	Application Security Manager™ objects in assigned partitions	Objects in assigned partitions plus `Common`	ARP entries, archives, SNMP configurations, logs, and support tools
Fraud Protection Manager	Fraud Protection Service objects in assigned partitions	Objects in assigned partitions plus `Common`	ARP entries, archives, SNMP configurations, logs, and support tools
Operator	Nodes and pool members in assigned partitions (enable and disable only)	Objects in assigned partitions plus `Common`	ARP entries, archives, SNMP configurations, logs, and support tools
Auditor	None	Most objects on the system	ARP entries, SSL keys, archives, and user passwords
Guest	None	Objects in assigned partitions plus `Common`	ARP entries, archives, SNMP configurations, logs, and support tools

User role	Write access	Read-only access	No access
No Access	None	None	None

About the User Manager user role

If a user with this role has permission to manage user accounts in partition A, then this user can view most BIG-IP objects in Common and partition. The objects that the User Manager cannot view are: ARP entries, system archives, SNMP configurations, logs (by default), and support information (through QKView and TCP Dump).

A user with a User Manager role on all partitions (that is, with universal access) can manage user accounts in these ways:

- Create a user account in any partition and assign roles for that user on any partition.
- Modify a user account in any partition and change the existing roles for that user on any partitions.
- View all user accounts.
- Modify the password on any user account.
- Enable or disable terminal access for any user account.
- Change his or her own password.

A user with a User Manager role on a specific partition can manage user accounts in the same way as above except that all actions are restricted to the specific partition to which the user manager has access. Therefore the user manager cannot change any user's role that is associated with another partition. For example, suppose that:

- User `mjones` has the User Manager role for partition `A` only.
- User account `rsmith` resides in Partition `A`.
- User `rsmith` has the role of Certificate Manager on Partition `A`.
- User `rsmith` has the role of Operator on Partition `B`.

In this case, user `mjones` can view, change, or delete `rsmith`'s Certificate Manager role for partition `A`. User `mjones` can view `rsmith`'s Operator role for partition **B** but cannot change or delete that role.

With respect to deleting user accounts in partition `A`, user `mjones` cannot delete the `rsmith` account because user `rsmith` has access to a partition other than `A`.

About the Firewall Manager user role

A user with the role of Firewall Manager can manage firewall rules and other supporting objects, including:

- Firewall rules in all contexts
- Address lists
- Port lists
- Schedules
- Security logging profiles and supporting objects, including log publishers and destinations
- IP intelligence and DoS profiles association rights for all of the above security profiles to virtual servers
- DoS Device Configuration (the L2 through L4 DoS protection configuration)

***Note:** To modify global and management port rules, Firewall Managers must have partition `Common` assigned to their user accounts.*

Summary of user role considerations

When managing user roles for BIG-IP® user accounts, it is helpful to understand these system behaviors and restrictions. Some apply to all user accounts, while others apply to remote accounts only.

All user accounts

This section summarizes some high-level concepts about configuring access control for all BIG-IP user accounts, whether stored locally on the BIG-IP system or on a remote authentication server:

- A user account can have only one user role for each administrative partition on the BIG-IP system.
- If a user has multiple roles on the system, the user's most powerful role is applied on first login.
- If you have an Administrator role, you can grant universal access to any user, except those that have a role of No Access.
- A user with the role of Administrator, Resource Administrator, Application Security Administrator, or Auditor always has universal partition access (that is, access to all partitions). For these users, you cannot change this universal access.
- A user with universal access can have only one role on the system, and the role applies to all partitions. On initial login, the user's current partition is set to `Common`.
- During a user's login session, the role for the current partition is continually displayed in the upper left area of each screen of the BIG-IP Configuration utility.
- If you change a role on a user account while the user is logged into the system through `tmsh`, the BIG-IP system terminates the user's `tmsh` session when the user subsequently issues another `tmsh` command.

Remote user accounts

This section summarizes some high-level concepts about configuring access control for remotely-stored BIG-IP user accounts. Specific BIG-IP system behavior with respect to granting permissions depends on the type of remote authentication server. For more detailed information, see the section titled Remote User Account Management.

- When assigning user role-partition combinations to a single remote user group, you can specify multiple combinations to the group (that is, for the same attribute string). However, for a single user group, you cannot specify multiple roles for the same partition. Within one remote group, the BIG-IP system disallows any attempt to assign multiple roles to the same partition.
- For a user with multi-group membership, if you assign more than one role to the same partition, the BIG-IP system chooses a role and partition for the user at login time, based primarily on the line order that you specified in the remote role configuration on the BIG-IP system.
- If you attempt to assign multiple role-partition combinations to a user, and one of those combinations grants universal access (that is, access to all partitions), then the BIG-IP system will either disallow the universal access assignment (if configuring one user group only), or, depending on configured line order, grant universal access to the user and ignore all other role assignments for individual partitions.
- If you are logged in to the BIG-IP system as a member of the account `Other External Users` ,and you modify the role of that account to a lesser role, the system modifies the user role of your own account to the lesser role also. The change occurs when you log out and log in again to the BIG-IP system.

Local User Account Management

About local user accounts

Managing local user accounts refers to the tasks of creating, viewing, modifying, and deleting user accounts that reside on the BIG-IP® system.

The BIG-IP system stores local user accounts (including user names, passwords, and user roles) in a local user-account database. When a user logs into the BIG-IP system using one of these locally-stored accounts, the BIG-IP system checks the account to determine the user role assigned to that user account for each partition to which the user has access.

For example, suppose you grant local user `jsmith` access to partitions `A` and `B`, and in the process, assign her a role of Manager for partition `A` and a role of Operator for partition `B`. This means that user `jsmith` can create, modify, and delete several types of local traffic objects that reside in partition `A`, but in partition `B`, she is restricted to enabling and disabling nodes, pool members, virtual servers, and virtual addresses.

For user `rjones`, you can grant him access to the same partitions `A` and `B`, but assign him the roles of Certificate Manager and Guest, respectively. For user `rjones`, this means that with respect to partition `A`, he can fully manage digital certificates that reside in that partition, but he has no permission to manage other types of objects in the partition. For objects in partition `B`, he has read access only.

Displaying a list of local user accounts

Before performing this task, ensure that you have a role of Administrator or that you have a role of User Manager for the relevant partition.

Using the BIG-IP® Configuration utility, you can display a list of existing local user accounts. If the user role assigned to your account is Administrator, you can view any user account on the BIG-IP® system, in any partition. If the user role assigned to your account is User Manager, you can view any user account in any partition to which you have access on the BIG-IP system.

1. On the Main tab, click **System** > **Users**.
2. From the **Partition** list in the upper-left corner of the screen, set the current partition to the partition in which the relevant user accounts reside.
3. View the list of user accounts.

Creating a local user account

To perform this task, you must have the Administrator or User Manager user role assigned to your user account. Note that if the user role assigned to your account is User Manager, you can only create a user account in the partitions to which you have access.

You perform this task to create a local user account for BIG-IP ®administrative users.

***Note:** User accounts on the BIG-IP® system are case-sensitive. Thus, the system treats user accounts such as `JONES` and `Jones` as two separate user accounts. Note, however, that certain user names, such as `admin`,* *are reserved, and are therefore exempt from case-sensitivity. For example, you cannot create a user account named `Admin`, `aDmin`, or `ADMIN`.*

---

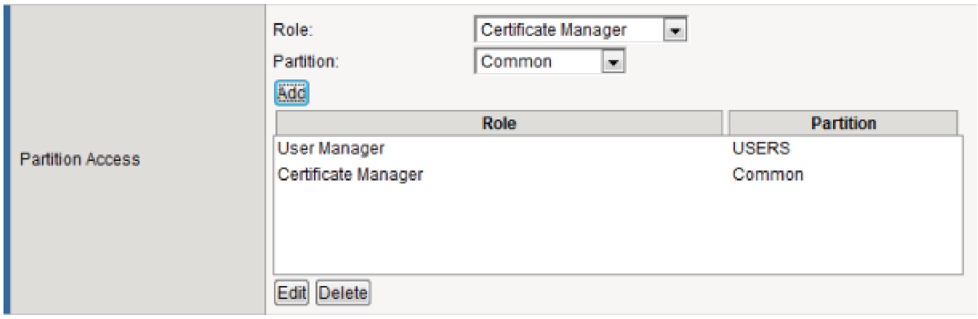
1. Access the BIG-IP ® Configuration utility.
2. On the Main tab, click **System** > **Users**.

   The BIG-IP system displays the list of user accounts that reside in the current partition and in partition `Common`. Note that all users except those with a user role of No Access have at least read access to partition `Common`.
3. From the **Partition** list in the upper-left corner of the screen, set the current partition to the partition in which you want the user account to reside.

   Important: *The partition you select in this step is not the partition to which you want the user account to have access.*

   ---
4. Click the **Create** button.

   If the **Create** button is unavailable, you do not have permission to create a local user account. You must have the Administrator or User Manager role assigned to your user account in order to create a local user account.
5. For the **Password** setting:
   a) In the **New** field, type a password for the user account.
   b) In the **Confirm** field, type the password again.
   If the two passwords match, the BIG-IP system assigns the password to the user account. The user can log in to the system later and change this password.
6. For the **Partition Access** setting:
   a) From the **Role** list to select a user role.
   b) From the **Partition** list, select a partition name.
   c) Click the **Add** button.
   A user role pertaining to a partition now appears in the box.
   d) Repeat these steps for each partition to which you want to assign a role for this user.



Partition Access

Role: Certificate Manager

Partition: Common

Role	Partition
User Manager	USERS
Certificate Manager	Common

Figure 3: Granting partition access to a BIG-IP user account

   After you configure this setting, one or more role-partition combinations are specified for assignment to this user account.
7. If you want to allow user access to the command line interface, then from the **Terminal Access** list, select a level of access.

   Note: *The advanced shell is only available for accounts with the Administrator or Resource Administrator user role.*

   ---

8. Click the **Finished** button.

After you perform this task, a user account exists on the BIG-IP system that assigns one or more roles, each corresponding to a partition on the system. The task also grants some level of terminal access, either `tmsh` or Bash shell access.

Viewing the properties of a local user account

Before performing this task, ensure that you have a user role of Administrator or that you have a role of User Manager for the relevant partition.

Using the BIG-IP® Configuration utility, you can view the properties of an individual account.

1. On the Main tab, click **System** > **Users**.
2. From the **Partition** list in the upper-left corner of the screen, set the current partition to the partition in which the relevant user accounts reside.
3. In the user-account list, find the user account you want to view and click the account name. This displays the properties of that user account.

Modifying the properties of a local user account

Before performing this task, ensure that you have a user role of Administrator or that you have a role of User Manager for the relevant partition.

Using the BIG-IP® Configuration utility, you can modify the properties of an existing local user account, other than the `root` account.

Warning: *If you change a role on a user account while the user is logged into the system through the Traffic Management Shell (*`tmsh`*), the BIG-IP system terminates the user's* `tmsh` *session when the user subsequently issues another* `tmsh` *command.*

1. On the Main tab, click **System** > **Users**.
2. From the **Partition** list in the upper-left corner of the screen, set the current partition to the partition in which the relevant user accounts reside.
3. In the user account list, find the user account you want to view and click the account name. This displays the properties of that user account.
4. To change the user's password, locate the **Password** setting and replace the existing password in the **New** and **Confirm** fields with the new password.
5. To modify a user's role and partition access, do any of the following:
   a) To add a role for a partition, from the **Role** list select a role, and from the **Partition** list, select a partition. Then click the **Add** button.
   The new role-partition entry appears in the **Partitian Access** box.
   b) To modify a role or partition, in the **Partition Access** box, select the role-partition entry you want to modify, and click the **Edit** button. Then from the **Role** or **Partition** list, select a new role or partition. Then click the **Add** button.
   c) To delete a role-partition entry, in the **Partition Access** box, select the role-partition entry you want to delete, and click the **Delete** button.

   You can add, modify, or delete only those role-partition entries that you are authorized to manage based on your own user role and partition access.

6. If you want to change the user's access to the command line interface, then from the **Terminal Access** list, select a level of access.

   Note: *The advanced shell is only available for accounts with the Administrator or Resource Administrator user role.*

7. Click the **Update** button.

Deleting a local user account

Before performing this task, ensure that you have a user role of Administrator or that you have a role of User Manager for the relevant partition.

When you delete a local user account, you remove it permanently from the local user-account database on the BIG-IP system. If the account you are using has the Administrator or User Manager user role, you can delete other local user accounts. A user with the Administrator role can delete any user account on the BIG-IP® system in any partition. A user with the User Manager role can delete user accounts on the BIG-IP system in only those partitions to which she has access.

Note: *You cannot delete the* `admin` *user account, nor can you delete the user account with which you are logged in.*

Warning: *The Administrator user role provides access to the BIG-IP system prompt. If another user with the Administrator user role is currently logged in to the system and you delete the user account, the user can still run commands at the BIG-IP system command prompt until he or she logs off of the system.*

1. On the Main tab, click **System** > **Users**.
2. In the user-account list, locate the name of the account you want to delete and select the check box to the left of the account name.
3. Click the **Delete** button.
4. Click **Delete** again.

Properties of a local BIG-IP system user account

This table lists and describes the properties that define a local BIG-IP user account.

Property	Description	Default Value
User Name	Specifies the name of the user account. The BIG-IP system is case-sensitive, which means that names such as JONES and Jones are treated as separate user accounts.	No default value
Partition	When viewing the properties of an existing user account, displays the name of the partition in which the user account object resides. All partitionable BIG-IP system objects (including user account objects) have the **Partition** property. Note that you cannot edit the value of this setting.	No default value
Password	Specifies a password that the user will use to log in to the BIG-IP system.	No default value
Partition Access	Specifies a user role for each partition to which the user has access when logged on to the BIG-IP system. When you assign the user role of Administrator,	All

Property	Description	Default Value
	Resource Administrator, or Auditor, the list of partitions to choose from becomes unavailable. (Accounts with these roles always have universal partition access, that is, access to all partitions.)	
Terminal Access	Specifies the level of access to the BIG-IP system command line interface. Possible values are: **Disabled** and **Advanced shell**. Users with the **Administrator** or **Resource Administrator** role assigned to their accounts can have advanced shell access, that is, permission to use all BIG-IP system command line utilities, as well as any Linux commands.	Disabled

About secure password policy configuration

The BIG-IP® system includes an optional administrative feature: a security policy for creating passwords for local BIG-IP system user accounts. A secure password policy ensures that BIG-IP system users who have local user accounts create and maintain passwords that are as secure as possible.

The secure password policy feature includes two distinct types of password restrictions:

Enforcement restrictions

These are, specifically, character restrictions that you can enable or disable. They consist of the minimum password length and the required character types (numeric, uppercase, lowercase, and other kinds of characters). When enabled, the BIG-IP system never enforces restrictions on user accounts that have the Administrator role assigned to them. Consequently, a user with Administrator permissions does not need to adhere to these restrictions when either changing his or her own password, or changing the passwords of other user accounts.

Policy restrictions

These restrictions represent the minimum and maximum lengths of time that passwords can be in effect. Also included in this type of policy restriction are the number of days prior to password expiration that users are warned, and the number of previous passwords that the BIG-IP system should store, to prevent users from re-using former passwords. These restrictions are always enabled, although using the default values provides a minimal amount of restriction.

Passwords for remotely-stored user accounts are not subject to this password policy, but might be subject to a separate password policy defined on the remote system.

Configuration settings for a secure password policy

This table lists and describes the settings for a password policy.

Setting	Description	Default value
Secure Password Enforcements	Enables or disables character restrictions, that is, a policy for minimum password length and required characters. When you enable this setting, the BIG-IP Configuration utility displays the **Minimum Length** and **Required Characters** settings.	Disabled
Minimum Length	Specifies the minimum number of characters required for a password, and the allowed range of values is **6** to **255**. This setting appears only when you enable the **Secure Password Enforcement** setting.	6

Setting	Description	Default value
Required Characters	Specifies the number of numeric, uppercase, lowercase, and other characters required for a password. The allowed range of values is **0** to **127**. This setting appears only when you enable the **Secure Password Enforcement** setting.	0
Password Memory	Specifies, for each user account, the number of former passwords that the BIG-IP system retains to prevent the user from re-using a recent password. The range of allowed values is **0** to **127**.	0
Minimum Duration	Specifies the minimum number of days before a user can change a password. The range of allowed values is **0** to **255**.	0
Maximum Duration	Specifies the maximum number of days that a user's password can be valid. The range of allowed values is **1** to **99999**. This setting applies to all user accounts.	99999
Expiration Warning	Specifies the number of days prior to password expiration that the system sends a warning message to a user. The range of allowed values is **1** to **255**. This setting applies to all user accounts.	7
Maximum Login Failures	Denies access to a user after the specified number of failed authentication attempts. The administrator can then reset the lock to re-enable access for the user.	0

Configuring a password policy for administrative users

Use this procedure to require BIG-IP® system users to create strong passwords and to specify the maximum number of BIG-IP login failures that the system allows before the user is denied access.

Important: *You must have the user role of Administrator assigned to your account to configure this feature.*

1. On the Main tab, click **System** > **Users**.
2. On the menu bar, click **Authentication**.
3. From the **Secure Password Enforcement** list, select **Enabled**.
   Additional settings appear on the screen.
4. For the **Minimum Length** and **Required Characters** settings, configure the default values, according to your organization's internal security requirements.
5. In the **Password Memory** field, type the number of passwords that the user cannot re-use. The valid range is from `0` to `127`.
6. In the **Minimum Duration** field, type the minimum number of days before which users cannot change their passwords. The valid range is from `0` to `255`.
7. In the **Maximum Duration** field, type the maximum number of days that a password is valid. Users must change their passwords before the maximum duration is reached.

   The value of this setting determines when users receive warning messages to change their passwords. If you change the value of this setting, any subsequent warning messages that users receive indicate the previous maximum duration value, rather than the new value. Once a user changes the password, however, subsequent reminder messages show the new value.
8. In the **Expiration Warning** field, type the number of days before the password expires that the user receives a password expiration warning. The valid range is from `1` to `255`.
9. In the **Maximum Login Failures** field, specify a number.

If the user fails to log in the specified number of times, the user is locked out of the system. Therefore, F5 Networks recommends that you specify a value that allows for a reasonable number of login failures before user lockout.

10. Click **Update**.

User authentication lockout

When you configure the password policy restrictions for user accounts, you can configure the number of failed authentication attempts that a user can perform before the user is locked out of the system. If a user becomes locked out, you can remove the lock to re-enable access for the user.

Unlocking a user account

Before performing this task, you must have an Administrator user role or have a User Manager role with access to the partition containing the locked user account.

If a user exceeds the number of failed login attempts that the password policy allows, the BIG-IP® system locks the user account. You can perform this task to unlock the account.

1. Access the BIG-IP ® Configuration utility.
2. On the Main tab, click **System** > **Users** > **User List**.

   The BIG-IP system displays the list of user accounts that reside in the current partition and in partition `Common`. Note that all users except those with a user role of No Access have at least read access to partition `Common`.
3. In the upper-left corner of the screen, from the **Partition** list, select the partition in which the user account that you want to unlock resides.
4. In the user account list, locate the name of the account you want to unlock and select the check box to the left of the account name.
5. Click the **Unlock**button.

After you perform this task, the user can attempt to log in to the BIG-IP system.

Remote User Account Management

About remote user accounts

Each BIG-IP® system requires one or more administrative user accounts. Rather than store these BIG-IP user accounts locally on the BIG-IP system, you can store BIG-IP user accounts on a remote authentication server, either LDAP, Active Directory, RADIUS, or TACACS+. In this case, you create all of your standard BIG-IP user accounts (including user names and passwords) on the remote server, using the mechanism supplied by that server's vendor. The remote server then performs all authentication of those user accounts.

To implement access control for remotely-stored BIG-IP user accounts, you can use the BIG-IP Configuration utility or `tmsh`. You first specify information for the type of remote authentication server, and then you configure these access control properties:

- User role
- Partition access
- Terminal access

To ensure easy management of access control for remote accounts, the BIG-IP system automatically creates a single user account named `Other External Users`. This user account represents all of the remotely-stored BIG-IP user accounts that conform to the access-control properties defined on the BIG-IP system.

Specifying LDAP or Active Directory server information

Before you begin:

- Verify that the BIG-IP® system user accounts have been created on the remote authentication server.
- Verify that the appropriate user groups, if any, are defined on the remote authentication server.
- If you want to verify the certificate of the authentication server, import one or more SSL certificates.

You can configure the BIG-IP system to use an LDAP or Microsoft® Windows® Active Directory ®server for authenticating BIG-IP system user accounts, that is, traffic that passes through the management interface (MGMT).

Important: *The values you specify in this procedure for the **Role**, **Partition Access**, and **Terminal Access** settings do not apply to group-based access control. These values represent the default values that the BIG-IP system applies to any user account that is not part of a remotely-stored user group. Also, for the* `Other External Users` *user account, you can modify the **Role**, **Partition Access**, and **Terminal Access** settings only when your current partition on the BIG-IP system is set to* `Common`*. If you attempt to modify these settings when your current partition is other than* `Common`*, the system displays an error message.*

1. On the Main tab, click **System** > **Users** > **Authentication**.
2. On the menu bar, click **Authentication**.
3. Click **Change**.
4. From the **User Directory** list, select **Remote - LDAP** or **Remote - Active Directory**.
5. In the **Host** field, type the IP address of the remote server.

The route domain to which this address pertains must be route domain `0`.

6. For the **Port** setting, retain the default port number (`389`) or type a new port number.

   This number represents the port number that the BIG-IP system uses to access the remote server.

7. In the **Remote Directory Tree** field, type the file location (tree) of the user authentication database on the LDAP or Active Directory server.

   At minimum, you must specify a domain component (that is, `dc=[value]`).

8. For the **Scope** setting, retain the default value (`Sub`) or select a new value.

   This setting specifies the level of the remote server database that the BIG-IP system should search for user authentication.

9. For the **Bind** setting, specify a user ID login for the remote server:

   a) In the **DN** field, type the distinguished name for the remote user ID.
   b) In the **Password** field, type the password for the remote user ID.
   c) In the **Confirm** field, re-type the password that you typed in the **Password** field.

10. In the **User Template** field, type a string that contains a variable representing the distinguished name of the user, in the format `%s`.

    This field can contain only one `%s` and cannot contain any other format specifiers.

    For example, you can specify a user template such as `%s@siterequest.com` or `uxml:id=%s,ou=people,dc=siterequest,dc=com`.
    The result is that when a user attempts to log on, the system replaces `%s` with the user name specified in the Basic Authentication dialog box, and passes that name as the distinguished name for the bind operation. The system also passes the associated password as the password for the bind operation.

11. For the **Check Member Attribute in Group** setting, select the check box if you want the system to check the user's member attribute in the remote LDAP or AD group.

12. To enable SSL-based authentication, from the **SSL** list select **Enabled** and, if necessary, configure these settings:

    a) From the **SSL CA Certificate** list, select the name of a chain certificate, that is, the third-party CA or self-signed certificate that normally resides on the remote authentication server.
    b) From the **SSL Client Key** list, select the name of the client SSL key.

       Use this setting only when the remote server requires that the client present a certificate.

    c) From the **SSL Client Certificate** list, select the name of the client SSL certificate.

       Use this setting only if the remote server requires that the client present a certificate.

13. In the **Login LDAP Attribute** field, type the account name for the LDAP server.

    The value for this option is normally the user ID. However, if the server is a Microsoft® Windows® Active Directory®server, the value must be the account name `sAMAccountName` (case-sensitive). The default value is none.

14. From the **Client Certificate Name Field** list:

    a) Select either a subject alternate name or the subject name (**Common Name**).
    b) If you select the subject alternate name **Other Name**, then in the **OID** field, type an object identifier (OID).

       The OID indicates the format and semantics of the subject alternate name.

15. From the **Role** list, select the user role that you want the BIG-IP system to assign by default to all BIG-IP system user accounts authenticated on the remote server.

16. From the **Partition Access** list, select the default administrative partition that all remotely-authenticated BIG-IP system user accounts can access.

17. From the **Terminal Access** list, select either of these as the default terminal access option for remotely-authenticated user accounts:

Option	Description
Disabled	Choose this option when you do not want the remotely-stored user accounts to have terminal access to the BIG-IP system.
tmsh	Choose this option when you want the remotely-stored user accounts to have only `tmsh` access to the BIG-IP system.

18. Click **Finished**.

You can now authenticate administrative user accounts that are stored on a remote LDAP or Active Directory server. If you have no need to configure access control for remotely-stored user groups, your configuration tasks are complete.

Specifying client certificate LDAP server information

Verify that the required user accounts for the BIG-IP® system exist on the remote authentication server.

For authenticating BIG-IP system user accounts (that is, traffic that passes through the management interface [MGMT]), you can configure the BIG-IP system to authenticate certificates issued by a certificate authority's Online Certificate Status Protocol (OCSP) responder.

Important: *The values you specify in this procedure for the* ***Role***, ***Partition Access***, *and* ***Terminal Access*** *settings do not apply to group-based authorization. These values represent the default values or locally configured user accounts (which override the default role) that the BIG-IP system applies to any user account that is not part of a remote role group.*

1. On the Main tab, click **System** > **Users** > **Authentication**.
2. On the menu bar, click **Authentication**.
3. Click **Change**.
4. From the **User Directory** list, select **Remote - ClientCert LDAP**.
5. In the **Host** field, type the IP address of the remote server.

   The route domain to which this address pertains must be route domain `0`.
6. For the **Port** setting, retain the default port number (`389`) or type a new port number.

   This number represents the port number that the BIG-IP system uses to access the remote server.
7. In the **Remote Directory Tree** field, type the file location (tree) of the user authentication database on the client certificate server.

   At minimum, you must specify a domain component (that is, `dc=[value]`).
8. For the **Scope** setting, retain the default value (`Sub`) or select a new value.

   This setting specifies the level of the remote server database that the BIG-IP system should search for user authentication.
9. For the **Bind** setting, specify a user ID login for the remote server:
   a) In the **DN** field, type the distinguished name for the remote user ID.
   b) In the **Password** field, type the password for the remote user ID.
   c) In the **Confirm** field, re-type the password that you typed in the **Password** field.
10. To enable SSL-based authentication, from the **SSL** list select **Enabled** and, if necessary, configure these settings:

a) From the **SSL CA Certificate** list, select the name of a chain certificate; that is, the third-party CA or self-signed certificate that normally resides on the remote authentication server.
b) From the **SSL Client Key** list, select the name of the client SSL key.

   Use this setting only when the remote server requires that the client present a certificate.
c) From the **SSL Client Certificate** list, select the name of the client SSL certificate.

   Use this setting only if the remote server requires that the client present a certificate.

11. In the **CA Certificate** field, type the absolute folder path of `apache-ssl-cert fileobject` for the CA signing authority.

    The absolute folder path is `/Common/<folder path>/<certificate name>`. To determine the absolute folder path of the `apache-ssl-cert fileobject`, click **System** > **File Management** > **Apache Certificate List** and note the target certificate's partition and path.

    Important: *Apache certificates can only be stored within* `/Common`*.*
12. In the **Login Name** field, type an LDAP search prefix that will contain the distinguished name (DN) from the user certificate, such as `CN`.

    This specifies the LDAP attribute to be used as a login name. The default is disabled.
13. In the **Login LDAP Attribute** field, type the account name for the LDAP server.

    The value for this option is normally the user ID. However, if the server is a Microsoft® Windows® Active Directory®server, the value must be the account name `sAMAccountName` (case-sensitive). The default value is none.
14. In the **Login Filter** field, type the LDAP attribute that contains the short name of the user.

    This specifies the filter to be applied on the common name (CN) of the client certificate and usually this is the user ID or `sAMAccountName`. The filter is a regular expression used to extract required information from the CN of the client certificate that is matched against the LDAP search results. The default is disabled.
15. For the **Depth** setting, retain the default value (`10`) or type a new value for verification depth.
16. From the **Client Certificate Name Field** list:

    a) Select either a subject alternate name or the subject name (**Common Name**).
    b) If you select the subject alternate name **Other Name**, then in the **OID** field, type an object identifier (OID).

       The OID indicates the format and semantics of the subject alternate name.
17. From the **OCSP Override** list, select **On** or **Off** to specify whether the system uses a specified OCSP responder to override the CA certificate to authenticate/authorize logon operations.
18. If the **OCSP Override** is set to **On**, then in the **OCSP Responder** field, retain the default value or type the server name or URL that authenticates/authorizes logon operations.

    The default value is `localhost.localdomain`.
19. From the **Role** list, select the user role that you want the BIG-IP system to assign by default to all BIG-IP system user accounts authenticated on the remote server.
20. From the **Partition Access** list, select the default administrative partition that all remotely-authenticated BIG-IP system user accounts can access.
21. From the **Terminal Access** list, select either of these as the default terminal access option for remotely-authenticated user accounts:

Option	Description
Disabled	Choose this option when you do not want the remotely-stored user accounts to have terminal access to the BIG-IP system.

Option	Description
tmsh	Choose this option when you want the remotely-stored user accounts to have only `tmsh` access to the BIG-IP system.

22. Click **Finished**.

You can now authenticate administrative traffic for user accounts that are stored on a remote client certificate server. If you have no need to configure group-based user authorization, your configuration tasks are complete.

Specifying RADIUS server information

Before you begin:

- Verify that the BIG-IP® system user accounts have been created on the remote authentication server.
- Verify that the appropriate user groups, if any, are defined on the remote authentication server.

You can configure the BIG-IP system to use a RADIUS server for authenticating BIG-IP system user accounts, that is, traffic that passes through the management interface (MGMT).

Important: *The values you specify in this procedure for the* ***Role****,* ***Partition Access****, and* ***Terminal Access*** *settings do not apply to group-based authorization. These values represent the default values that the BIG-IP system applies to any user account that is not part of a role group that is defined on the remote authentication server. Also, for the* `Other External Users` *user account, you can modify the* ***Role****,* ***Partition Access****, and* ***Terminal Access*** *settings only when your current partition on the BIG-IP system is set to* `Common`*. If you attempt to modify these settings when your current partition is other than* `Common`*, the system displays an error message.*

1. On the Main tab, click **System** > **Users** > **Authentication**.
2. On the menu bar, click **Authentication**.
3. Click **Change**.
4. From the **User Directory** list, select **Remote - RADIUS**.
5. For the **Primary** setting:
   a) In the **Host** field, type the name of the primary RADIUS server.
      The route domain with which this host is associated must be route domain `0`.
   b) In the **Secret** field, type the password for access to the primary RADIUS server.
   c) In the **Confirm** field, re-type the RADIUS secret.
6. If you set the **Server Configuration** setting to **Primary and Secondary**, then for the **Secondary** setting:
   a) In the **Host** field, type the name of the secondary RADIUS server.
      The route domain with which this host is associated must be route domain `0`.
   b) In the **Secret** field, type the password for access to the secondary RADIUS server.
   c) In the **Confirm** field, re-type the RADIUS secret.
7. From the **Role** list, select the user role that you want the BIG-IP system to assign by default to all BIG-IP system user accounts authenticated on the remote server.
8. From the **Partition Access** list, select the default administrative partition that all remotely-authenticated BIG-IP system user accounts can access.

9. From the **Terminal Access** list, select either of these as the default terminal access option for remotely-authenticated user accounts:

Option	Description
Disabled	Choose this option when you do not want the remotely-stored user accounts to have terminal access to the BIG-IP system.
tmsh	Choose this option when you want the remotely-stored user accounts to have only `tmsh` access to the BIG-IP system.

10. Click **Finished**.

You can now authenticate administrative traffic for BIG-IP system user accounts that are stored on a remote RADIUS server. If you have no need to configure access control for remotely-stored user groups, your configuration tasks are complete.

Specifying TACACS+ server information

Before you begin:

- Verify that the BIG-IP® system user accounts have been created on the remote authentication server.
- Verify that the appropriate user groups, if any, are defined on the remote authentication server.

You can configure the BIG-IP system to use a TACACS+ server for authenticating BIG-IP system user accounts, that is, traffic that passes through the management interface (MGMT).

Important: *The values you specify in this procedure for the* ***Role****,* ***Partition Access****, and* ***Terminal Access*** *settings do not apply to group-based authorization. These values represent the default values that the BIG-IP system applies to any user account that is not part of a remote role group. Also, for the* `Other External Users` *user account, you can modify the* ***Role****,* ***Partition Access****, and* ***Terminal Access*** *settings only when your current partition on the BIG-IP system is set to* `Common`*. If you attempt to modify these settings when your current partition is other than* `Common`*, the system displays an error message.*

1. On the Main tab, click **System** > **Users** > **Authentication**.
2. On the menu bar, click **Authentication**.
3. Click **Change**.
4. From the **User Directory** list, select **Remote - TACACS+**.
5. For the **Servers** setting, type an IP address for the remote TACACS+ server.

   The route domain to which this address pertains must be route domain `0`.
6. Click **Add**.
   The IP address for the remote TACACS+ server appears in the **Servers** list.
7. In the **Secret** field, type the password for access to the TACACS+ server.

   Warning: *Do not include the symbol* `#` *in the secret. Doing so causes authentication of local user accounts (such as* `root` *and* `admin`*) to fail.*
8. In the **Confirm Secret** field, re-type the TACACS+ secret.
9. From the **Encryption** list, select an encryption option:

Option	Description
Enabled	Specifies that the system encrypts the TACACS+ packets.
Disabled	Specifies that the system sends unencrypted TACACS+ packets.

10. In the **Service Name** field, type the name of the service that the user is requesting to be authenticated to use (usually `ppp`).

    Specifying the service causes the TACACS+ server to behave differently for different types of authentication requests. Examples of service names that you can specify are: `ppp`, `slip`, `arap`, `shell`, `tty-daemon`, `connection`, `system`, and `firewall`.

11. In the **Protocol Name** field, type the name of the protocol associated with the value specified in the **Service Name** field.

    This value is usually `ip`. Examples of protocol names that you can specify are: `ip`, `lcp`, `ipx`, `atalk`, `vines`, `lat`, `xremote`, `tn3270`, `telnet`, `rlogin`, `pad`, `vpdn`, `ftp`, `http`, `deccp`, `osicp`, and `unknown`.

12. From the **Role** list, select the user role that you want the BIG-IP system to assign by default to all BIG-IP system user accounts authenticated on the remote server.
13. From the **Partition Access** list, select the default administrative partition that all remotely-authenticated BIG-IP system user accounts can access.
14. From the **Terminal Access** list, select either of these as the default terminal access option for remotely-authenticated user accounts:

Option	Description
Disabled	Choose this option when you do not want the remotely-stored user accounts to have terminal access to the BIG-IP system.
tmsh	Choose this option when you want the remotely-stored user accounts to have only `tmsh` access to the BIG-IP system.

15. Click **Finished**.

You can now authenticate administrative traffic for BIG-IP system user accounts that are stored on a remote TACACS+ server. If you have no need to configure access control for remotely-stored user groups, your configuration tasks are complete.

Changing the default access control for remote accounts

You perform this task to change the user role, partition access, and terminal access that you want the BIG-IP system to assign by default to all remote users that are members of the user account `Other External Users`.

1. On the Main tab, click **System** > **Users** > **Authentication**.
2. Click **Change**.
3. From the **User Directory** list, select **Remote - Active Directory**, **Remote - LDAP**, **Remote - RADIUS**, or **Remote - TACACS+**.
4. From the **Role** list, select a user role.

   The BIG-IP system assigns this user role to any remote account that is not part of a remote user group to which you have explicitly assigned a user role.

5. From the **Partition Access** list, select a partition name.

   All remote user accounts that are members of the BIG-IP account `Other External Users` can have access to either all partitions or the same individual partition. Individual members of this account cannot have access to different partitions.

6. From the **Terminal Access** list, select **Enabled** or **Disabled**.
7. Click **Update**.

After you perform this task, most BIG-IP user accounts stored on a remote authentication server have the specified user role, as well as partition and console access. Remote accounts that are part of a role group are not subject to these authentication settings.

About remote user groups

On the BIG-IP® system, you can assign access control properties (user role, partition, and terminal access) to any group of BIG-IP user accounts defined on a remote authentication server. You can assign these properties by using either the BIG-IP configuration utility or the Traffic Management Shell (`tmsh`) to specify the appropriate remote attribute string and line-order for each group of BIG-IP users, along with the access control values you want to assign to the group.

You can configure access control for remote groups of BIG-IP user accounts in these ways:

- By specifying on the BIG-IP system the relevant attribute string and the role, partition access, and terminal access that you want to assign to the group.
- By specifying on the BIG-IP system the relevant attribute string and then using variable substitution (`tmsh` only).

Note: *Note that access control for these group-based user accounts is separate from the access control assigned to accounts represented by the BIG-IP user account named* `Other External Users`*.*

Configuration examples

Because some types of remote servers allow a user to be a member of multiple user groups, configuration of user roles and partitions for BIG-IP ®user groups on those servers can result in conflicts. For example, two separate remote user groups might specify different roles on the same administrative partition. For a user that is a member of both groups, this configuration breaks the BIG-IP rule that a user cannot have two roles for any one partition.

In the case of such conflicts, the BIG-IP system must choose one of the conflicting roles for the user at login time. The primary way that the BIG-IP system makes this choice is by using line order. The line order that you specify within each remote role configuration affects how the system ultimately resolves any conflicts.

By contrast, within a single remote user group, no conflicts occur because the BIG-IP system prevents administrators from assigning more than role to the same partition.

Example 1: Conflicting role-partition entries within a group

The following example shows that two user roles Guest and Certificate Manager are associated with the same partition, `A`, for the same remote user group, `BigIPAdminGroup`.

This configuration is invalid because no one user can have more than one role for a specific partition. If an administrative user attempts to implement this configuration, the BIG-IP system disallows the configuration and displays an error message.

```
BigIPAdminGroup
         attribute memberOF=CN=BigIPAdminGroup,OU=BIP,DC=dean,DC=local
         console tmsh
         line-order 30
         role guest
         user-partition A

         attribute memberOF=CN=BigIPAdminGroup,OU=BIP,DC=dean,DC=local
         console tmsh
         line-order 30
         role manager
         user-partition B

         attribute memberOF=CN=BigIPAdminGroup,OU=BIP,DC=dean,DC=local
         console tmsh
         line-order 30
         role certificate manager
         user-partition A
```

Example 2: Conflicting role-partition entries in multiple groups

In the following example, the remote server contains two BIG-IP® user groups `BigIPNetworkGroup` and`BigIPAdminGroup`, and the BIG-IP system has three partitions, `A`, `B`, and `C`.

Suppose that user `jsmith` is a member of both groups. The configuration below shows that on login to the BIG-IP system, user `jsmith` will clearly be assigned the role of Operator for partition `B`, and Manager for partition `C`. But for partition `A`, there is a conflict, because a user can have only one role per partition on the system, and this configuration attempts to assign the roles of both Manager and Guest for that partition.

To resolve the conflict, the BIG-IP system uses line order to determine which of the conflicting roles to assign to `jsmith` for partition `A`. In this case, the system will choose Manager, the role with the lowest line-order number (20).

```
BigIPNetworkGroup
        attribute memberOF=CN=BigIPNetworkGroup,OU=BIP,DC=dean,DC=local
        console tmsh
        line-order 20
        role manager
        user-partition A

        attribute memberOF=CN=BigIPNetworkGroup,OU=BIP,DC=dean,DC=local
        console tmsh
        line-order 10
        role operator
        user-partition B

        attribute memberOF=CN=BigIPNetworkGroup,OU=BIP,DC=dean,DC=local
        console tmsh
        line-order 40
        role manager
        user-partition C

BigIPAdminGroup
         attribute memberOF=CN=BigIPAdminGroup,OU=BIP,DC=dean,DC=local
         console tmsh
         line-order 30
         role guest
         user-partition A
```

Example 3: Conflicting role-partition entries due to universal access

In the following example, suppose that user `jsmith` is a member of three remote user groups: `BigIPGuestGroup`, `BigIPOperatorGroup`, and `BigipAdminGroup`, and the BIG-IP system has three partitions, `A`, `B`, and `C`.

In this configuration, the role specified for `BigIPAdminGroup` creates a conflict, because some entries specify a particular role for each partition, while `BigIPAdminGroup` specifies a role of Administrator for all three partitions. To resolve the conflict, the BIG-IP system uses the configured line order.

Because the line order for `BigIPAdminGroup` is 9 and therefore not the lowest line-order number, the BIG-IP system will ignore the role of Administrator for `jsmith`, leaving her with a role of Guest on partitions `A` and `C`, and Operator on partition `B`.

```
BigIPGuestGroup
            attribute memberOF=CN=BigIPGuestGroup,OU=BIP,DC=dean,DC=local
            console tmsh
            line-order 2
            role guest
            user-partition A

   BigIPOperatorGroup
            attribute memberOF=CN=BigIPOperatorGroup,OU=BIP,DC=dean,DC=local
            console tmsh
            line-order 10
            role operator
            user-partition B

   BigIPAdminGroup
            attribute memberOF=CN=BigIPAdminGroup,OU=BIP,DC=dean,DC=local
            console tmsh
            line-order 9
            role administrator
            user-partition All

   BigIPGuestGroup
            attribute memberOF=CN=BigIPGuestGroup,OU=BIP,DC=dean,DC=local
            console tmsh
            line-order 3
            role guest
            user-partition C
```

Configuring access control for remote user groups

You perform this task to assign a user role, a corresponding administrative partition, and a type of terminal access to a remotely-stored group of user accounts. For a given user group, you can assign as many role-partition combinations as you need, as long as each role is associated with a different partition. If the partition you associate with a role is `All`, this entry might or might not take effect, depending on whether the `All` designation conflicts with other role-partition combinations for that user group. For any conflicts, line order in the configuration is a consideration. To assign multiple role-partition combinations for a user group, you repeat this task for each combination, specifying the same attribute string for each task.

1. On the Main tab, click **System** > **Users**.
2. On the menu bar, click **Remote Role Groups**.
3. Click **Create**.
4. In the **Group Name** field, type the group name that is defined on the remote authentication server.

An example of a group name is **BigIPOperatorsGroup**.

5. In the **Line Order** field, type a number.

   This value specifies the order of this access control configuration in the file `/config/bigip/auth/remoterole` for the named group. The LDAP and Active Directory servers read this file line by line. The order of the information is important; therefore, F5 Networks recommends that you specify a value of `1000` for the first line number. This allows you, in the future, to insert lines before the first line.

6. In the **Attribute String** field, type an attribute.

   An example of an attribute string is `memberOF=cn=BigIPOperatorsGroup,cn=users,dc=dev,dc=net`.

   The BIG-IP system attempts to match this attribute with an attribute on the remote authentication server. On finding a match, the BIG-IP system applies the access control settings defined here to the users in that group. If a match is not found, the system applies the default access control settings to all remotely-stored user accounts (excluding any user account for which access control settings are individually configured).

7. From the **Remote Access** list, select a value.

Option	Description
Enabled	Choose this value if you want to enable remote access for the defined user group.
Disabled	Choose this value if you want to disable remote access for the defined user group. Note that if you configure multiple instances of this remote role group (one instance for each role-partition pair for the attribute string), then choosing a value of **Disabled** disables remote access for all user group members, regardless of the remote role group instance.

8. From the **Assigned Role** list, select a user role for the remote user group.

9. From the **Partition Access** list, select an administrative partition value.

Option	Description
All	Choose this value to give users in the defined group access to their authorized objects in all partitions on the BIG-IP system.
`partition_name`	Choose a specific partition name to give users in the defined group access to that partition only.
Common	Choose this value to give users in the defined group access to partition **Common** only.

10. From the **Terminal Access** list, select the type of command-line access you want to grant users in the group, if any.

11. Click **Finished** or **Repeat**.

After you perform this task, the user group that you specified has the assigned role, partition access, and terminal access properties assigned to it.

About variable substitution

As an alternative to using the BIG-IP™ Configuration utility to specify explicit values for access control properties for remote user groups, you can configure the remote server to return a vendor-specific attribute with variables for role, partition access, and console access. You can then assign values to those variables (numeric or alphabetic), and you can use the tmsh remoterole command to perform variable substitution for those access control properties.

For example, suppose that you configure a remote RADIUS authentication server to return the vendor-specific attribute F5-LTM-User-Info-1 = DC1 , along with three variables and their values:

- F5-LTM-User-Role = 400 (variable)
- F5-LTM-User-Partition = App_C (variable)
- F5-LTM-User-Console = 1 (variable)

Note: *A user role value of 400 signifies the Operator user role.*

The remoterole command can use the attribute F5-LTM-User-Info-1 on which to match. The command can then read the role, user partition, and console values from the three variables, rather than you specifying them explicitly. To do this, you specify each of the three variables on the command line, preceded by the string %, as arguments.

The following shows a sample use of the remoterole command. This sample command matches on the vendor-specific attribute F5-LTM-User-Info-1 and then, using the above variables, assigns a user role of (Operator (400)), access to partition App_C, and tmsh access 1) to any user accounts that are part of Datacenter 1 (DC1):

```
 tmsh auth remote-role role-info add { DC1 { attribute "F5-LTM-User-Info-1=DC1"
console "%F5-LTM-User-Console" role "%F5-LTM-User-Role" user partition
 "%F5-LTM-User-Partition" line order 1 } }
```

Values for remote role variables

This table lists the values for the BIG-IP variable F5-LTM-User-Role that you use for defining a role for a remotely-stored user group. For example, a value of 100 to the variable F5-LTM-User-Role indicates the Manager user role.

User Role	Value
Administrator	0
Resource-Admin	20
User-Manager	40
Auditor	80
Manager	100
App-Editor	300
Operator	400
Firewall Manager	450
Fraud Protection Manager	480
Certificate-Manager	500
Certificate-Manager	510
Guest	700
Application-Security-Admin	800
Application-Security-Editor	810
Application-Policy-Editor	850

User Role	Value
No-Access	900

About terminal access for remote user groups

If you use the Traffic Management Shell (`tmsh`) `remoterole` command to configure console access for a user account within a remote user group, the BIG-IP™ system behavior differs depending on the value of the `console` option:

- If an attribute string for a remote user group has one or more role-partition pairs assigned to that attribute, and you set the value of the `console` option to **tmsh**, then on successful authentication the BIG-IP system grants all users in that user group `tmsh` access to the BIG-IP system.
- If you set the value of the `console` option to `disable` (or you do not configure the `console` option) for all role-partition combinations assigned to the same attribute string, then the BIG-IP system denies all users in that user group `tmsh` access to the BIG-IP system, even on successful authentication. Note that this does not affect user access to the BIG-IP Configuration utility.

Saving access control settings to a file

You can save the running configuration of the system, including all settings for remote user authentication and authorization, in a flat, text file with a specified name and the extension `.scf`.

1. On the BIG-IP® system, access a command-line prompt.
2. At the prompt, open the Traffic Management Shell by typing the command `tmsh`.
3. Type `sys save` *`filename`*.
   `sys save myConfiguration053107` creates the file `myConfiguration053107.scf` in the `var/local/scf` directory.
   `sys save /config/myConfiguration` creates the file `myConfiguration.scf` in the `/config` directory.

You can now import this file onto other BIG-IP devices on the network.

Importing BIG-IP configuration data onto other BIG-IP systems

You can use the `tmsh sys load` command to import a single configuration file (SCF), including access control data, onto other BIG-IP® devices on the network.

Note: *This task is optional.*

1. On the BIG-IP system on which you created the SCF, access a command-line prompt.
2. Copy the SCF that you previously created to a location on your network that you can access from the system that you want to configure.
3. Edit the SCF to reflect the management routing and special passwords of the BIG-IP system that you want to configure:
   a) Open the SCF in an editor.

b) Where necessary, change the values of the management IP address, network mask, management default route, self IP addresses, virtual server IP addresses, routes, default routes, and host name fields to the values for the new system.

c) If necessary, change the passwords for the `root` and `admin` accounts using the command `user` *`name`* `password none newpassword` *`password`*.

> ***Important:*** *When configuring a unit that is part of a redundant system configuration and that is using the SCF from the peer unit, do not modify the* `root` *and* `admin` *accounts. These accounts must be identical on both units of the redundant system.*

d) Save the edited SCF.

4. On the BIG-IP system that you want to configure, open the Traffic Management Shell by typing the command `tmsh`.
5. Type `sys load` *`scf_filename`*.
   `sys load myConfiguration053107.scf` saves a backup of the running configuration in the `/var/local/scf` directory, and then resets the running configuration with the configuration contained in the SCF you are loading.

About viewing remote user accounts

Using the BIG-IP Configuration utility, you can display a list of those remote user accounts to which you explicitly assigned a non-default user role. If a remote user account has the default role assigned to it, you cannot see that account in the user account list.

Any users who have access to a partition in which remote accounts reside can view a list of remote user accounts.

Displaying a list of remote user accounts

You perform this task to display a list of remotely-stored user accounts.

1. On the Main tab, click **System** > **Users**.
2. On the menu bar, click **Authentication**.
3. Verify that the **User Directory** setting specifies a remote authentication server type (Active Directory, LDAP, or RADIUS).
4. On the menu bar, click **User List**.
5. View the list of user accounts. Remote user accounts that are assigned the default user role appear as **Other External Users**.

Viewing access control properties

1. On the Main tab, click **System** > **Users**.
2. On the menu bar, click **Authentication**.
3. Verify that the **User Directory** setting specifies a remote authentication server type (Active Directory, LDAP, or RADIUS).

4. On the menu bar, click **User List**.
5. View the list of user accounts. Remote user accounts that are assigned the default user role appear as **Other External Users**.
6. In the user account list, find the user account you want to view and click the account name. This displays the properties of that user account.

Auditing User Access

About auditing of user access to the BIG-IP system

The BIG-IP® system generates a log message whenever a user or an application attempts to log in to or log out of the system. The system logs both successful and unsuccessful login attempts. The system stores these log messages in the `/var/log/secure` file.

When the system logs an authentication message in the `/var/log/secure` file, the message can contain the following types of information:

- The connecting user's ID
- The IP address or host name of the user's interface
- The time of each login attempt
- Successful login attempts for command line interface sessions only
- Failed login attempts for command line interface, BIG-IP Configuration utility, and iControl® sessions
- The time of the logout for command line interface sessions only

This is an example of log messages for both successful and failed login attempts made by user `jsmith`:

```
May 10 16:25:25 jsmith-dev sshd[13272]: pam_audit: user: jsmith(jsmith) from:
 /dev/pts/10 at jsmith-dev attempts: 1 in:
[Thu May 10 16:25:23 2007 ] out: [Thu May 10 16:25:25 2007 ]
May 10 16:14:56 jsmith-dev sshd[716]: pam_audit: User jsmith from ssh at
jsmith-dev failed to login after 1 attempts
(start: [Thu May 10 16:14:53 2007 ] end: [Thu May 10 16:14:56 2007 ]).
```

About audit logging

Audit logging is an optional feature that logs messages whenever a BIG-IP® system object, such as a virtual server or a load balancing pool, is configured (that is, created, modified, or deleted). The BIG-IP system logs the messages for these auditing events in the file `/var/log/audit`.

There are three ways that objects can be configured:

- By user action
- By system action
- By loading configuration data

Whenever an object is configured in one of these ways, the BIG-IP system logs a message to the audit log.

About enabling and disabling auditing logging

An optional type of logging that you can enable is audit logging. *Audit logging* logs messages that pertain to actions that users or services take with respect to the BIG-IP® system configuration. This type of audit logging is known as *MCP audit logging*. Optionally, you can set up audit logging for any `tmsh` commands that users type on the command line.

For both MCP and `tmsh` audit logging, you can choose a log level. In this case, the log levels do not affect the severity of the log messages; instead, they affect the initiator of the audit event.

The log levels for MCP logging are:

Disable
This turns audit logging off.

Enable
This causes the system to log messages for user-initiated configuration changes only. This is the default value.

Verbose
This causes the system to log messages for user-initiated configuration changes and any loading of configuration data.

Debug
This causes the system to log messages for all user-initiated and system-initiated configuration changes.

The log levels for `tmsh` logging are:

Disable
This turns audit logging off.

Enable
This causes the system to log all `tmsh` commands, including commands that result in no change to the configuration. Note that the system does not generate a log entry when the user types the single command `tmsh` to open the `tmsh` shell. This is the default log level.

Index