Common Criteria Supplement
EAL2
F5 Networks
BIG-IP® Local Traffic Manager 6400
High Availability pair (qty 2)

Release Date: March 30, 2007
Document ID: 05-948-R-0134
Version: 1.3

Prepared By: M. McAlister
InfoGard Laboratories, Inc.

Prepared For: F5 Networks
401 Elliott Avenue West
Seattle, WA 98119
# Table of Contents

1  PURPOSE .................................................................................................................................................................. 5
   1.1  DEFINITIONS ....................................................................................................................................................... 5
      1.1.1 Acronyms ....................................................................................................................................................... 6

2  F5 BIG–IP INSTALLATION GUIDE SUPPLEMENT ................................................................................................. 8
   2.1  RECEIPT AND PREPARATION OF TOE AND ENVIRONMENT PRIOR TO INSTALLATION .................................. 8
   2.2  VERIFICATION OF COMMON CRITERIA EVALUATED CONFIGURATION ............................................................ 10
      2.2.1 Common Criteria Excluded Aspects .................................................................................................................. 10
      2.2.2 Verification of Common Criteria components .................................................................................................. 11
   2.3  ESTABLISHING ADMINISTRATOR PASSWORD .............................................................................................. 12
      2.3.1 Set Administrator Username/Password .............................................................................................................. 12
      2.3.2 Set Redundancy mode ...................................................................................................................................... 13
      2.3.3 Setup SSH Access ............................................................................................................................................ 13
   2.4  CONFIGURATION SYNCHRONIZATION ............................................................................................................... 13
   2.5  APPLY HOTFIX CR69440 ................................................................................................................................. 14
   2.6  FINAL INSTALLATION NOTE: .......................................................................................................................... 14

3  F5 BIG–IP ADMINISTRATION GUIDE SUPPLEMENT ............................................................................................... 16
   3.1  GENERAL ............................................................................................................................................................... 16
      3.1.1 Administrator Browser Based GUI sessions ....................................................................................................... 17
   3.2  ESTABLISHING LOCAL USERS AND ROLES .................................................................................................... 17
      3.2.1 Changing Default User Role ............................................................................................................................. 18
      3.2.2 Removing or modifying User Access .................................................................................................................. 18
      3.2.3 Deleting an explicit user-role designation ......................................................................................................... 20
      3.2.4 Expired Password Request for update ............................................................................................................... 20
   3.3  VLAN SETTINGS ..................................................................................................................................................... 21
   3.4  CONFIGURING REDUNDANCY SETTINGS ........................................................................................................... 22
      3.4.1 Failover settings ............................................................................................................................................... 22
      3.4.2 Establishing a gateway pool .............................................................................................................................. 23
      3.4.3 VLAN fail-safe settings .................................................................................................................................... 24
3.4.4 Gateway fail safe trigger settings................................................................. 25
3.4.5 System fail safe parameters ................................................................. 26
3.4.6 Configuration synchronization............................................................... 26
3.4.7 Connection Mirroring ........................................................................... 27
3.5 CONFIGURING ALERT/ALARM LOGGING SETTINGS .......................... 28
3.5.1 Enable Local Traffic Events Logging............................................... 29
3.5.2 Enable Audit Events Logging............................................................... 30
3.5.3 Disable Audit Events Logging............................................................. 30
3.5.4 Setting Log Levels ............................................................................... 30
3.5.5 Log Function Verification .................................................................... 31
3.5.6 Review of Audit Log Resource settings ............................................. 32
3.6 SECURITY SETTINGS .................................................................................. 33
3.6.1 SynCheck threshold activation ......................................................... 33
3.6.2 Reaper high water mark/low water mark............................................. 33
3.6.3 Re-encrypting traffic for routing to Clients (where applicable) ....... 33
3.6.4 Access levels to administrator functions for security settings .......... 34
3.6.5 Port Lockdown for Self-IPs ............................................................... 34
3.6.6 Use of Encryption option for Saving of Configuration Data .......... 34
3.6.7 Disabling of front panel controls ...................................................... 35
3.7 TRAFFIC MANAGEMENT SETTINGS ....................................................... 35
3.7.1 Traffic Management Information Flow Security Function Policy ....... 35
3.8 AUTHENTICATION SERVERS SETTINGS .............................................. 36
3.8.1 LDAP Settings ................................................................................... 36
3.8.2 RADIUS Settings............................................................................... 36
3.9 COOKIE SETTINGS .................................................................................. 37
3.9.1 Cookie Persistence Settings ............................................................... 37
3.9.2 Cookie Encryption Settings ............................................................... 37

4 APPENDIX A: REFERENCE DOCUMENTS .................................................. 38
List of Tables

Table 1: Secure values for a VLAN ................................................................. 22
1 Purpose

The purpose of this document/assurance measure is to supplement the existing Target of Evaluation (TOE) documentation for the BIG-IP system. Conformance with this supplemental instruction in addition to the applicable sections of the primary documentation is intended to result in deployment and configuration of the TOE consistent with the Common Criteria\(^1\) evaluated configuration identified in the F5 BIG-IP Security Target.

1.1 Definitions

Administrative Users This term connotes within this document an administrative user of the BIG-IP appliance. Members of this grouping term include: Administrator, Operator and Guest.

Administrator Role applied to user with full access to all aspects of the BIG-IP appliance. Member of Administrative Users definition.

Authenticated Traffic User This term connotes a user of the traffic which traverses the BIG IP appliance but not a direct user of the appliance itself which is required to authenticate with through the TSF prior to access backend server resources. This is a role within the BIG-IP appliance and is a member of the traffic users grouping term.

Guest Role applied to user with read-only access to TSF resources.

iRules™ An iRule is a user-written script that controls the behavior of a connection passing through the LTM system. iRules™ are an F5 Networks feature and are frequently used to direct certain connections to a non-default load balancing pool. However, iRules can perform other tasks, such as implementing secure network address translation and enabling session persistence. iRules can define criteria for pool-member selection, as well as perform content transformations, logging, custom protocol support.

\(^1\) Common Criteria is an Information Technology Security Evaluation program adopted by the National Information Assurance Partnership (NIAP). NIAP is collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). NIAP has established the Common Criteria Evaluation Validated Scheme (CCEVS) to validate IT products. Common Criteria is also referred to as ISO 15408.
Node  An application client server within the BIG-IP® managed environment

Operator  Role applied to user with limited access to the appliance. This role has read only access to TSF and beyond that may only enable/disable Nodes. Member of Administrative Users definition.

Pool  A grouping of Nodes or application server clients

Self-IP  A Self-IP is an IP address that the TM/OS takes for itself on a VLAN. You can use a Self-IP to access the GUI.

Unauthenticated traffic user  Role within the BIG-IP appliance to indicate a user of traffic flowing through the TOE to backend servers which does not require authentication support from the BIG-IP appliance.

1.1.1 Acronyms

CC  Common Criteria
DoS  Denial of Service
FIPS  Federal Information Processing Standard
FTP  File Transfer Protocol
GTM  Global Traffic Management
GUI  Graphical User Interface
HTTP  Hypertext Transport Protocol
HTTPS  Hypertext Transport Protocol (Secure)
LDAP  Lightweight Directory Access Protocol
LTM  Local Traffic Management
OpenSSH  Open Secure Shell
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TOE</td>
<td>Target of Evaluation</td>
</tr>
<tr>
<td>Self-IP</td>
<td>Self IP address</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>SFP</td>
<td>Security Function Policy</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface</td>
</tr>
<tr>
<td>VLANs</td>
<td>Virtual Local Area Networks</td>
</tr>
<tr>
<td>VNIC</td>
<td>Virtual Network Interface Card (driver)</td>
</tr>
</tbody>
</table>
2 F5 BIG–IP Installation Guide supplement

This section supplements the Installation, Licensing, and Upgrades for BIG-IP® Systems version 9.2. This reference and release applies to the TOE Common Criteria Evaluated version 9.2.3 + Hotfix CR69440, therefore, any reference within the document stating BIG-IP Traffic Manager version 9.2 can be assumed to be referring to version 9.2.3 + Hotfix CR69440.

Note: All references as listed in Appendix A are applicable to the Common Criteria Evaluated Configuration of 9.2.3 + Hotfix CR69440

Before you begin: The Administrators of the BIG-IP appliance must review all associated documentation and guidance, prior to proceeding with installation and administration of the device. Administration of the BIG-IP appliance requires a base of knowledge in networking and traffic management. The user is responsible to ensure that qualified personnel complete all tasks described herein and in references.

2.1 Receipt and preparation of TOE and Environment prior to installation

Receipt

Verify all components are included per the packing list and are undamaged.

Assure that tamper seals are intact on BIG-IP chassis.

The Common Criteria evaluated configuration requires that the system be installed in a redundant pair configuration where two identical units are required. As specified in Section 1 of the System Management Guide, the “Failover” process assures that traffic is uninterrupted when the TOE is installed in the redundant configuration as required. The CC Evaluated configuration requires that the units be in the “active/standby” mode where the standby unit is available for redundancy and high availability.

Environment preparation

The BIG-IP system must be installed in a secure location that provides physical protection. Access should be limited only to Administrator personnel as defined in the ST. The level of security provided should be commensurate with the BIG-IP system and Environment secured assets.
Prior to installation

Assure that there are no general purpose computing or storage repository capabilities available on the BIG-IP system. The BIG-IP system should be dedicated to its primary functionality.

Assure that the TOE Environment includes provisions for access control mechanisms that will protect TOE Security Function data to include:

- Proper establishment of authentication servers (LDAP, RADIUS) (as required)
- Appropriate Firewall for WAN access (as required)

Assure that networks and domains are secure, separate, dedicated, available and established for the following:

- Authentication Server Local Area Network*
- Dedicated Client Server Local Area Network
- Wide Area Network (Internet) Access
- Provision for Remote Administrator Access via Administrator Management Port*

*Note: Administrator management networks and authentication networks may be combined to allow for redundant administrator access paths.

Step 1: Consult the Quick Start Instructions PUB-0089-03 1205 that is packaged with the BIG-IP System. Complete items #1-#4

Step 2: Review Password Setup instructions in Section 2.3 of this document

Step 3: Complete Items #5 - #6 of Quick Start Instructions PUB-0089-03 1205.

Step 4 Switchboot to latest version

After machine power-up, the default installation with be an older version of the software, 9.1.1. The machine needs to be rebooted into version 9.2.3. To do this, login at the console as root (default username: admin, default password: admin) and run `switchboot`. You will be shown a list of 2 versions of software, select version 9.2.3. After selecting, type `reboot`. When the machine has rebooted, you will be in version 9.2.3. Note: Software installation as referenced in Installation, Licensing, and Upgrades for BIG-IP® Systems version 9.2: Chapter 1 is NOT required for the Common Criteria Evaluated Configuration.

Step 5: Verify system contents per below to assure configuration
2.2 Verification of Common Criteria Evaluated Configuration

2.2.1 Common Criteria Excluded Aspects
The follow features and usage types are excluded from the Common Criteria Evaluated Configuration, therefore, must not be activated or used following deployment in order to retain the CC Evaluated Configuration.

   “Support” Account type for F5 use in supporting the appliance (disabled by default)
   Use of Active Directory Authentication servers

The following aspects of BIG-IP functionality/protocols are not included in the Common Criteria Evaluated Configuration:

1. Application Security Module (incl. related iRules)
2. Use of the CLI (via console or SSH) for any purpose other than initial IP configuration during installation
3. Authentication of traffic users on the appliance incl. Authentication iRules.
4. Support Account type for F5 use in supporting the appliance (disabled by default)
5. Use of Active Directory Authentication servers
6. The following aspects of BIG-IP functionality/protocols are not included in the Evaluated Configuration:
   ■ SNMP (Remote Management of BIG-IP): administrative use of SNMP
   ■ Trunk (link aggregation)
   ■ Packet Filter configuration & administrator usage (audit events are allowed)
   ■ Archives (relating to Backup Configurations)

Note that the following aspects of operation were not evaluated as part of the Common Criteria Evaluated configuration:

   Optimization of network and application traffic
   HTTP compression
   Caching
Aggregation of client requests
Routing around slower or degraded routes
Selective data compression
The use of an OCSP server in the IT Environment.

2.2.2 Verification of Common Criteria components
The following are authorized components for the Common Criteria Evaluated configuration.

Hardware Components:
- BIG-IP Hardware 2 processor 6400 series appliance (redundant pair qty 2)
- Authentication Server applicable Auth. Server (LDAP, RADIUS)
- Application Servers Node application servers – Web Servers
- Remote CPU Remote PC or Laptop for remote admin access
- Network Switch(s) Switch between TOE and Application Servers

Software Components:
- Appliance software revision 9.2.3 + Hotfix CR69440 (aka build 142.0)
  (contains the following:)
  - TM/O.S. (Linux 2.4.21) Operating System with F5 Kernel changes
  - Traffic Manager MicroKernel (v1.0)
  - VNIC (v1.0) Virtual Network Card software
  - Pluggable Authentication module (v.75)
  - Authentication Server OS

Remote Computer for GUI Access:
- Microsoft Windows XP, Server 2003 (or) Unix/Linux any versions that support browsers
  - Microsoft®Internet Explorer™, version 6.x and later (or)
  - Netscape® Navigator™, version 7.1, Mozilla™, Firefox™, and Camino™.
2.3 Establishing Administrator Password

Execute the Setup utility from a supported web browser. The Setup utility prompts you to enter the basic system information including a root password, administrator password, and the IP addresses that will be assigned to the management port as detailed in Chapter 2 of the Installation, Licensing, and Upgrades for BIG-IP® Systems.

2.3.1 Set Administrator Username/Password

(Reference BIG-IP Installation Guide p. 3-3 Platform Management Configuration screen)

The following allows the user to establish a secure username and password. The default settings of the BIG-IP Appliance enforce that only 3 logon attempts are allowed prior to failure of the logon process and presentation of a failed login dialog.

When choosing a username/password do not use any default values for your personal username/password. For the Common Criteria Evaluated configuration, conformance with the following BIG-IP Password Policy is required as follows:

2.3.1.1 Password Policy

Verify that the BIG-IP has the secure password policy is implemented by following the steps listed in 3.2.2.

The minimum password policy enforced by BIG-IP for all users except for the Administrator role requires at least 8 characters, and at least one from capital letters, lowercase letters, numbers, and punctuation. It is mandatory that the Administrator also adhere to this policy, although, the TOE appliance will not enforce a password policy for the Administrator role. The following is the set of available characters for password selection:

This set includes:

- 52 alphabetic characters (26 upper and 26 lower)
- 10 digits
- 10 punctuation marks from the shifted digits
- 22 more punctuation marks from other keys

For a total of 94 characters.

After each failed authentication, there is a delay of 2 seconds to confound intruders.

Users must change their password every 90 days.

Complete the installation process by following the guidance in the Installation, Licensing, and Upgrades for BIG-IP® Systems manual.
Chapter 2 - Connecting a Management Workstation or Network
Chapter 3 - Licensing and Configuring the BIG-IP System

Upon completion of these steps complete the remaining items below to assure configuration settings are suitable for the Common Criteria Evaluated Configuration. Use the Configuration Worksheet (PUB-0090-02 0905) as you create the system configuration to keep track of assigned IP numbers and settings for future reference.

2.3.2 Set Redundancy mode

(Reference BIG-IP Installation Guide p. 3-3 Platform Management Configuration screen)

Select the “Redundant Pair” option in the Platform settings screen to place the BIG-IP system in a high availability mode consistent with the CC Evaluated configuration.

2.3.3 Setup SSH Access

(Reference Installation Guide p. 3-3 Platform Management Configuration screen) Administrative remote access to the BIG-IP must be established using the approved SSH protocol. This assures a higher level of security than non-SSH connections.

Establish the SSH protocol by checking the Enabled box in the Platform settings screen. Command Line Interface (CLI) usage for the Common Criteria Evaluated configuration is limited to the initial IP configuration of the appliance during installation. Therefore, it is recommended that following the installation and setup process, that CLI access is not used.

SSH IP allow range - After SSH access is enabled, you must specify the IP address or address range that other entities use to communicate with the BIG-IP. For security reasons, it is not allowed to specify the “all addresses option” as this would allow potentially unauthorized users to access resources. To specify a range, select Specify Range, and then type an address or address range in the box to restrict SSH access to a block of IP addresses. For example, to restrict access to only systems on the 192.168.0.0 network, type 192.168.0.0.

2.4 Configuration Synchronization

Following the successful initial configuration of the primary BIG-IP appliance, the preceding steps should be repeated on the standby or secondary unit to assure proper configuration. Alternatively, utilizing the Configuration Synchronization feature, the appliance configuration settings can be duplicated a BIG-IP system’s configuration data
onto its peer unit in a redundant system. Follow the steps contained in Chapter 13 (Setting up a Redundant System) in the Network System Management Guide under “Synchronizing configuration data”. Section 3.4.6 of this document, also has details regarding Configuration Synchronization. These steps will results in having identical configuration settings on both units. Be sure to maintain the “Active-Standby” status of the redundant pair configuration.

2.5 Apply Hotfix CR69440

Note: Before installing the Hotfix review the general instructions for installing a Hotfix at the following URL location:
https://tech.f5.com/home/bigip-next/releasenotes/hotfix_uninstall.html

Perform the following steps to download and install the Hotfix to the TOE appliance:

1. Open a browser session and navigate to the Hotfix web page:

   Save this file and associated readme files to the local drive

2. Place the file listed above in the following directory on the BIG-IP appliance:
   /var/tmp

3. Enter the following Bigpipe (CLI) command from the BIG-IP appliance command line:
   [im /var/tmp/ Hotfix-BIG-IP-9.2.3-CR69440.im]

4. The Hotfix is installed and the TOE is now updated to version 9.2.3 + Hotfix CR69440 (aka build 142.0)

2.6 Final Installation note:

Upgrading the TOE as referred to in the Installation, Licensing, and Upgrades for BIG-IP® Systems version 9.2 manual does not apply to the Common Criteria Evaluated
Configuration and may result in a non-compliant state. Any re-loading of software necessitates repeat of all listed configuration steps listed herein to assure compliance to the Evaluated Configuration.

Since Command Line Interface (CLI) usage is restricted for the Common Criteria Evaluated configuration to initial IP address configuration during installation it is recommended that, following the installation process, CLI access through the Administrator Management Port be disabled for SSH based Ethernet access by restrict availability of SSH access to IP subnets.

When these steps are completed progress to the next section to complete remaining Administrator settings and complete the deployment process.
3 F5 BIG-IP Administration Guide supplement

This section supplements the BIG-IP® Network and System Management Guide. Note: All references listed in Appendix A are applicable to the Common Criteria Evaluated Configuration of 9.2.3+ Hotfix CR69440. In some cases the major revision of 9.2 may be referred to in some documents and is analogous to the TOE revision 9.2.3 + Hotfix CR69440.

3.1 General

Administrator settings that follow will ensure the preservation of a secure state in the event of:

- Operational failure of a Server Node
- Loss of sufficient availability in a given Pool or Server Node
- Operational failure of the network switch hardware
- Operational failure of a single TOE hardware device

Environment Guidelines and Assumptions related to Common Criteria deployment:

In accordance with the applicable Security Target (F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Security Target)

A.USE The BIG-IP Appliance is dedicated to its primary function and does not provide any general purpose computing or storage capabilities.

Instructions:
The TOE does not contain any general purpose software or storage facility. This assumption is met as long and the TOE resource is not used for any purpose beyond what is detailed in this document and references. No verification is necessary beyond assuring that only authorized software is installed as specified herein and that access is limited to administrator personnel.

A.ADMIN The administrators are appropriately trained, not careless, not willfully negligent, non hostile and follow and abide by the instructions provided in the guidance documentation.

Instructions:
The Administrators of the BIG-IP appliance must review all associated documentation and guidance prior to proceeding with installation and administration of the device. Administration of the BIG-IP appliance requires a base of knowledge in networking and traffic management. The user is responsible to ensure that qualified personnel complete all tasks described herein and in references.
3.1.1 Administrator Browser Based GUI sessions

It should be noted that browser based GUI sessions use the Internet Explorer Web browser and, during the login process, Administrative User credentials are entered through the browser and are cached within the browser. In order to prevent unauthorized access using these credentials, the browser application should be closed following the Administrative User session.

The following sections should be consulted during the deployment process to assure that secure settings and installation environment is configured in accordance with the Common Criteria Evaluated Configuration.

3.2 Establishing local users and roles

Consult page 14-1 of the BIG-IP® Network and System Management Guide and review the User Account Types available on the BIG-IP appliance.

Refer to Table 14-2 for information regarding Users Roles and associated access

Configure the administrative accounts using the guidelines listed on page 14-4 of the BIG-IP® Network and System Management Guide. A step by step instruction for establishing User level accounts is provided on page 14-5 and is listed below (note that “user” in this case is a user of the BIG-IP appliance itself (role: administrator, operator, guest) and is therefore a Trusted Administrator per the ST):

- Configuring the admin account – p.14-4
  - The Primary or Root Administrator account is automatically configured for full access.
- Creating (administrator) user accounts –see below:

To create a user account:

1. On the Main tab of the navigation pane, expand System, and click Users.
   The User List screen opens, displaying a list of all Web UI accounts.

2. In the upper right corner of the screen, click Create.
   The New User screen opens.

3. In the User Name box, type a name for the user account.

4. For the Authentication setting, type and confirm a password for the account.
   For more information on user account passwords, see Managing remote user accounts, on page 14-8.
5. To grant the appropriate access level*, use the Web User Role setting and select one of these options:
   • Administrator
   • Operator
   • Guest

6. Click Finished.

*by default, when new users are created the access level is “no access” meaning no access to the appliance, therefore it is always necessary to select the appropriate role in order to access the appliance.

Details regarding access levels granted to various User Roles is detailed in Table 14.2 - User roles for user accounts on p. 14-3 of the BIG-IP® Network and System Management Guide.

3.2.1 Changing Default User Role

The BIG-IP appliance establishes a default setting of “No Access” for new users created. This is to ensure that the Administrator consciously determines and specifies the access level and role so as to avoid the potential for higher level access being granted to a new user than is appropriate. The Common Criteria Evaluated Configuration requires that this default value is not changed for maximum security.

3.2.2 Removing or modifying User Access


You use the Configuration utility to modify the properties of any existing Local user account, other than the root account. Only users who have been granted the Administrator role can modify user accounts other than their own.

Note: Administrator/Root accounts may not be deleted as they would result is loss of access to the appliance.

When you modify account properties, Administrators can:

   • Change the password
   • Change the user role
   • Allow console access (that is, using SSH) if the account has a user role of Administrator*

Note: The Allow Console Access check box shall not be checked for the Common Criteria evaluated configuration for any user as CLI usage is prohibited except for initial appliance IP configuration.

Users with roles of Operator or Guest can change their own passwords only. Users with an Administrator role can change their own
passwords as well as other users’ passwords.
To change properties of a user account other than root

1. On the Main tab of the navigation pane, expand System, and click Users.

The User List screen opens, displaying a list of all Web UI accounts.

2. In the user-account list, click a user account name. This displays the properties of that account.

3. Change the password, or choose a new user role for the account, or both. If the user account has the Administrator role assigned to it, or you are changing the user role to Administrator.

4. Query, Modify, Delete (Disable)

1. On the Main tab on the navigation pane, expand System, and click Users.
   The Users screen opens.
2. From the menu bar, click Authentication. This displays the screen for implementing a password policy (see Figure 1).

Within this screen the authorized administrator may query, modify, change or disable the password policy.

Note: These settings represent the secure password policy restrictions, which apply to all user accounts, regardless of user role. Password policy mechanisms, however, are not enforced against admin, root or remote accounts therefore password policy is enforced procedurally for these users.

3. Click Finished.
3.2.3 **Deleting an explicit user-role designation**


When you use the Configuration utility to delete a remote user account, you are not actually deleting the account from the remote server. Instead, you are removing the explicit user-role designation that you previously assigned the account.

Removing an explicit user-role designation from a remote user account causes the BIG-IP system to assign the default user role to the account.

To delete an explicit user role designation

1. On the Main tab of the navigation pane, expand System, and click Users. This opens the User List screen, displaying a list of all Web UI accounts.
2. Locate an account name in the list and click the corresponding Select box.
3. Click Delete. A confirmation page appears.
4. Click Delete.

3.2.4 **Expired Password Request for update**

If the current user's password is about to expire, the UI will display a warning on the properties page for that user's account (System >> Users >> username).

Additionally, when navigating to the base address of system (where the browser is redirected to the preferred start page), if the password is about to expire, the GUI will redirect the browser to their user account properties page where the password expiration warning will be displayed. In
both cases, the phrase "about to expire" indicates that the user's password will expire in less than or equal to the number of days specified by the Expiration Warning field under the System >> Users >> Authentication tab referenced above (Figure 1).

Figure 2: Updated Password Screen (after redirect)

3.3 VLAN settings
Consult page 5-3 in the BIG-IP Network and System Management Guide for guidance on set up of the Virtual LAN (VLAN) Environments. Below are the secure settings to be used in lieu of those represented in Table 5 of the Network and System Management Guide.

It is recommended that when considering Virtual Network Design, that you isolate Hosts that must transmit sensitive data. See the Network and System Management Guide, Chapter 7.0.

The following table specifies preferred settings for VLAN configuration.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a unique name for the VLAN. This value is required.</td>
<td>No default value</td>
</tr>
<tr>
<td>Tag</td>
<td>Specifies the VLAN ID. If you do not specify a VLAN ID, the BIG-IP system assigns an ID automatically. The value of a VLAN tag can be between 1 and 4094.</td>
<td>No default value</td>
</tr>
</tbody>
</table>
### Interfaces
Specifies any tagged or untagged interfaces that you want to associate with the VLAN.

### Source Check
Causes the BIG-IP system to verify that the return path of an initial packet is through the same VLAN from which the packet originated.

### MTU
Specifies the maximum transmission unit for the VLAN.

### MAC Masquerade
Sets up a media access control (MAC) address that is shared by a redundant system.

### Fail-safe
Triggers fail-over in a redundant system when certain VLAN-related events occur.

<table>
<thead>
<tr>
<th>Table 1: Secure values for a VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>* indicates values changed from default values (ref: Table 5.1 Network Sys. Mgmt. Guide Configuration settings for a VLAN)</td>
</tr>
</tbody>
</table>

### 3.4 Configuring Redundancy Settings

When configuring the BIG-IP units for the Common Criteria Evaluated Configuration they are required to be set in the Active-Standby configuration.

Consult Chapter 13 in the Network System and Management Guide: Setting up a Redundant System – and utilize the below settings in establishing the required High Availability, Redundant Pair Configuration.

#### 3.4.1 Failover settings

– Access setting from Main tab of the navigation pane in the Graphic User Interface (GUI)

(Reference Chapter 13 in Network and System Management Guide)

**Must be set to “Active – Standby” configuration**

**To initiate failback for an active/standby system**

1) On the Main tab of the navigation pane, expand **System**, and click **High Availability**.

2) The Redundancy Properties screen opens.
   a. At the bottom of the screen, select the **Force to Standby** button. You can also use the **FailOver.ManFailBack** bigdb database key.
3.4.2 Establishing a gateway pool

(Reference Chapter 4 in the Configuration Guide for Local Traffic Management)

This section is identical to that include in Chapter 4 of the Configuration Guide for Local Traffic Management – it is provided here as a convenience in Setting up the gateway pool.

A gateway pool is established to designate a group of members in a load balancing pool for monitoring as a basis for redundancy switchover. The pool is created by:

**To create a load balancing pool**

1. On the Main tab, expand **Local Traffic**.
2. Click **Pools**.
   The Pools screen opens.
3. In the upper-right corner of the screen, click **Create**.
   The New Pool screen opens.
4. From the Configuration list, select **Advanced**.
5. For the **Name** setting, type a name for the pool.
6. Specify, retain, or change each of the other settings.
   For information on pool settings, see *Configuring pool settings*, on page 4-5, or refer to the online help for this screen.
7. Click **Finished**.

**To implement a load balancing pool**

(Reference Chapter 4 in the Configuration Guide for Local Traffic Management – this section is a direct, unchanged excerpt)

1. On the Main tab, click **Virtual Servers**.
   The Virtual Servers screen opens.
2. Click the name of the appropriate virtual server.
   This displays the settings for that virtual server.
3. On the menu bar, click Resources.
4. In the **Default Pool** list, select the name of your newly-created pool.
5. Click **Update**.

When making configuration settings for the pool set the following parameter to the gateway monitor setting (Reference available settings table 4.1 in the Configuration Guide for Local Traffic Management.):
<table>
<thead>
<tr>
<th>Pool Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Monitors</td>
<td>You can associate a health or performance monitor with an entire pool, rather than with individual pool members only. This eases the task of configuring health and performance monitoring for multiple web servers.</td>
<td>(No Default Value) set to: <em>gateway_icmp</em></td>
</tr>
</tbody>
</table>

When you designate a pool as a gateway fail-safe pool, you provide the following information (Reference Section 13 of the Network and System Management Guide):

- Name of the pool
- The unit ID number of the peer on which the gateway pool is configured.
- The minimum number of gateway pool members that must be available to avoid the designated action.
- The action that the BIG-IP system should take when the number of available gateway pool members drops below the designated threshold. Possible actions are **Reboot, Fail Over, and Restart All**. The default value is **Fail Over**.

### 3.4.3 VLAN fail-safe settings
(Reference Chapter 13 in the Network and System Management Guide)

**To configure VLAN fail-safe using the VLANs screen**

1. On the Main tab of the navigation screen, expand **Network**, and click **VLANs**.
   This opens a list of existing VLANs.
2. Click the name of an existing VLAN, or click **Create**.

3. For the **Configuration** heading, select **Advanced**.

4. In the **Fail-safe** setting, check the box.
   This shows additional settings.

5. In the **Fail-safe Timeout** box, specify the period of time during which traffic should be detected on the VLAN, after which the designated action will occur.

   The default value, in seconds, of **30 should be used**.

6. From the **Action** list, select “Fail-Over” as the action that the BIG-IP system should take when the timeout period expires.

7. Click **Update** or **Finished**.

### 3.4.4 Gateway fail safe trigger settings

(Reference Chapter 13 in the Network and System Management Guide)

When establishing the gateway pool, assure the failure safe setting is configured per the instructions below:

**Confirm Fail-Over setting**

*Gateway fail-safe* monitors traffic between the active BIG-IP system and a pool containing a gateway router, thereby protecting the system from a loss of an internet connection by triggering a failover when a gateway router is unreachable for a specified duration.

**To configure gateway fail-safe**

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**. The Redundancy Properties screen opens.

2. From the Fail-safe menu, choose Gateway. The Gateway Fail-safe screen opens.

3. In the upper-right corner of the screen, click **Add**. The Add Gateway Pool screen opens.

4. From the **Gateway Pool** list, select the name of a load balancing Pool created in step 4.3.2 above.

5. From the **Unit ID** list, select a unit ID (1 or 2).for the pool

6. In the **Threshold** box, type the number of pool members that must be available to avoid the action designated in the **Action** setting.
7. From the **Action** list, select an action (**Reboot**, **Fail Over**, or **Restart All**).

8. Click **Finished**.

### 3.4.5 System fail safe parameters

(Reference Chapter 13 Network and System Management Guide)

The following settings are required to assure the Fail-Over processes meet the requirement of the Common Criteria Evaluated configuration:

**System Fail-safe** is the ability of a BIG-IP system to monitor certain aspects of the system or network, detect interruptions, and consequently take some action.

A redundant system can detect a problem and initiate failover to the peer unit. When configuring the fail-safe feature on a BIG-IP system, you are specifying the particular events that invoke the failover feature. The fail-safe feature applies to:

- System services
- Traffic between the BIG-IP system and a gateway router
- Traffic on a VLAN

To ensure redundant-system designation for a unit – the following setting arranges the two redundant appliances to operate in Active-Standby, thus transferring traffic to the standby unit in the event of primary appliance failure.


1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**. The Redundancy Properties screen opens.

2. From the Fail-safe menu, choose System. The System Fail-safe screen opens.

3. From the **Switch Board Failure** list, verify the default setting (**Fail Over**).

4. Click **Update**.

### 3.4.6 Configuration synchronization

(Reference Section 13 from the Network and System Management Guide) – Set **Synchronize** settings based on deployment
These are further settings relating to the redundancy setup procedure for the high availability, redundant pair configuration.

The **Synchronize** setting provides the option to perform configuration synchronization between two units. To synchronize data, click either of the following buttons:

**Synchronize TO Peer**
Use this button when the unit you are currently configuring contains the updated configuration data that is to be shared with the peer unit.

**Synchronize FROM Peer**
Use this button when the peer unit contains updated configuration data that you want to share with the unit you are currently configuring. In either case, the term *peer* refers to the unit with the self IP address that appears in the **ConfigSync Peer** box.

**To synchronize configuration data**
1. On the Main tab of the navigation pane, expand **System**, and choose **High Availability**. The Redundancy Properties screen opens.
2. On the menu bar, click **ConfigSync**. The ConfigSync screen opens.
3. If the user name you are using is other than **admin**:
   a) Find the Configuration heading and choose **Advanced**.
   b) For the **ConfigSync User** setting, select a user name.
   c) In the password box, type a password.
4. For the **Synchronize** setting, click **Synchronize TO Peer** or **Synchronize FROM Peer**.
5. Click **Update**.

### 3.4.7 Connection Mirroring

- (Reference Section 13 in Network and System Management Guide)

These are further settings relating to the redundancy setup procedure for the high availability, redundant pair configuration. The Evaluated Configuration requires that Connection Mirroring be enabled:

– Must be **enabled**

The **connection mirroring** feature on the BIG-IP system duplicates a unit’s state (that is, real-time connection and persistence information) on the peer unit. When connection mirroring is enabled, failover can be so
seamless that file transfers can proceed uninterrupted and servers can generally continue with the services at the time of failover.

**To enable connection mirroring for a virtual server**

1. On the Main tab of the navigation pane, expand Local Traffic, and choose Virtual Servers. This opens the Virtual Servers screen, which displays a list of existing virtual servers.
2. Click the name of a virtual server. This shows the properties for that virtual server.
3. Next to the Configuration heading, select Advanced.
4. Scroll down to the Connection Mirroring setting and check the box.
5. Click Update.

### 3.5 Configuring Alert/Alarm logging settings

The BIG-IP system has provisions for logging:

- System Events*
- Packet Filter Events*
- Local Traffic Events
- Audit Events

*Since Packet Filtering is excluded from the CC Evaluated Configuration, auditing for these events is not configured. System Events are logged through the syslog function within the Operating System and are active by default. No further configuration is necessary.

Access to Audit log records and maintenance screen must be done exclusively through the Administrator GUI interface. Use of the CLI interface to access these records/functions is excluded from the Common Criteria Evaluated Configuration.

The following steps must be taken to ensure logging levels meet the requirement for the Common Criteria Evaluated Configuration – these settings are not active by default.

The settings listed below in sections 3.5.1 and 3.5.2 will result in conformance to the F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair (qty 2) Security Target FAU_GEN.EXP.1 requirements:

Log-in authentication failure
Log-in identification failure
Modification of security attributes
Modification of security attributes – Pools & VLAN
Modification of TSF values-Delete
Modification of TSF values-Modify
Modification to Admin (security) roles
Use of Security Management functions

Audit Events are not enabled by default and should be activated by the following:

3.5.1 Enable Local Traffic Events Logging
(Reference Network System Management Guide ch.17)
To set a minimum log level for local traffic events
1. On the Main tab of the navigation pane, expand System, and click Logs. This opens the Logs screen.
2. On the menu bar, click Options. This displays the screen for setting minimum log levels on local traffic events.
3. In the Local Traffic Logging area of the screen, locate the event type for which you want to set a minimum log level.
   An example of an event type is HTTP Compression.
4. Select a minimum log level from the list. For the Common Criteria Evaluated Configuration this minimum log level should be set to: **Warning for the following Local Traffic Event types:**
   - ARP/NDP
   - BigDB
   - IP
   - MCP
   - Network
   - SSL

5. Click Update following each selection.
6. This process should be repeated for the following Traffic type with alternative settings (default):
   Traffic Management OS – “ERROR”
Monitors – “ERROR”
Layer 4 – “NOTICE”
iRules – “INFORMATIONAL”
HTTP – “ERROR”
HTTP Compression – “ERROR”

Click Update following each selection.

3.5.2 Enable Audit Events Logging
(Reference Network System Management Guide ch.17)
Assure the Audit logging settings are activated to assure logging of TSF related events.
To enable Audit Logging:
   Using the Administrator Interface navigate to the System/Logs page
   Under the Options tab, enable the Audit Log checkbox to enable logging

3.5.3 Disable Audit Events Logging
The Common Criteria Evaluated Configuration prohibits disabling of audit functions,
however, should it be necessary to temporarily disable the audit function the follow steps
should be followed:

1. On the Main tab of the navigation pane, expand System, and click Logs.
   This opens the Logs screen.
2. On the menu bar, click Options.
   This displays the screen for setting minimum log levels on local traffic events.
3. In the Audit Logging area of the screen, select the “DISABLE” log level from the Audit list.
4. Click Update.

3.5.4 Setting Log Levels
Logging levels can be adjusted based on the severity of the event – see page 17-7 of the
BIG-IP® Network and System Management Guide, which specifies the following selections:

The log levels that you can set on certain types of events, ordered from
highest severity to lowest severity, are:

• Emergency
Various logging levels are available for Local Traffic and Audit events to customize the level of logging produced.

Once enabled, the level assigned must set to the “Warning” level to assure that visibility is maintained to the TOE Administrator for crucial activities.

### 3.5.4.1 Setting Audit Log Levels:

To set a minimum log level for audit events

1. On the Main tab of the navigation pane, expand System, and click Logs.
   This opens the Logs screen.
2. On the menu bar, click Options.
   This displays the screen for setting minimum log levels on local traffic events.
3. In the Audit Logging area of the screen, select the “ENABLED” log level from the Audit list.
4. Click Update.

### 3.5.5 Log Function Verification

Following installation and deployment, conduct the following test and verification steps to assure audit settings are effective in producing required audit records:

During initial deployment and operation verify that logging functions are producing audit records for the following at a minimum:

- Packet Discard Events (packets not meeting protocol standard)
- DoS related Events
- Authentication Failures Failed authentication mechanism
Failed **identification** mechanism

- Modification of security attributes
  - User Account Management/Authentication
  - Initial TOE appliance configuration settings
  - Virtual Server Administration
  - iRules assignments (enable/disable)
  - Password Policy
  - Enable or Disable Virtual Servers
  - Enable or Disable Pool members
  - SSL cert usage settings

- Modification of TSF values
  - User Accounts (create/modify/delete)
  - User Roles
  - Passwords
  - SSL certificate data

- Modification to Administrative User (security) roles
  - Guest, Operator & Administrator

- Modification of Administrator management functions
  - Enabling/Disabling of Audit functions
  - Review of Audit logs
  - User Role Management
  - Virtual LAN/Server Management
  - Password Policy Management
  - Node Configuration (traffic management)
  - Pool configuration (traffic management)
  - Protocol Profile configuration (traffic management)
  - iRules configuration
  - Enable/Disable Nodes

### 3.5.6 Review of Audit Log Resource settings
(Reference Ch. 17 in the Network and Systems Management Guide)
BIG-IP administrators for the Common Criteria Evaluated configuration should assure that audit logs are reviewed on a timely basis to identify security events as when the allocated space within the appliance is reached, audit records will be overwritten in an oldest record first manner.

3.6 Security Settings
The following security related features and settings are crucial to the system performing in the CC Evaluated Configuration. Verify the following settings to assure the appropriate security settings are appropriate:

3.6.1 SynCheck threshold activation
SynCheck specifies the number of new or untrusted TCP connections that can be established before the system activates the SYNCookies authentication method for subsequent TCP connections.

Assure settings support maximum Denial of Service (DoS) protection by selecting:

- SynCheck: “16384”

Administrators should preserve the most secure (default) setting of: 16384

3.6.2 Reaper high water mark/low water mark

Assure settings support maximum DoS protection by selecting:

- Reaper high water mark: “95”
- Reaper low water mark: “85”

Administrators should preserve the most secure (default) settings indicated above.

3.6.3 Re-encrypting traffic for routing to Clients (where applicable)
When required, SSL profiles should be configured to re-encrypt SSL traffic prior to routing through SSL profile configuration options.
**SSL Profile Settings:**
Default settings are acceptable as listed in Table 7.3 (Configurable settings for an SSL profile) in Chapter 7 of the Configuration Guide for Local Traffic Management, however, note allowable ciphers for the Common Criteria Evaluated Configuration include FIPS approved Ciphers: 3DES, AES with a minimum key size of 128 bits.

**3.6.4 Access levels to administrator functions for security settings**
Access levels and roles should adhere to guidelines contained in the Security Target as follows:

Table 8: Security Management Attributes
Table 9: Table of Security Attributes Access

**3.6.5 Port Lockdown for Self-IPs**
The following describes the process of locking down ports not in use for maximum security.

By default, a self IP address accepts traffic from these protocols and services:

Default Setting (**Allow Default**):
- For UDP, the allowed protocols and services are: DNS (53), SNMP (161), RIP (520)
- For TCP, the allowed protocols and services are: SSH (22), DNS (53), SNMP (161), HTTPS (443), 4353 (iQuery)

**Secure Port Lockdown settings:**
The most secure option is to set Port Lockdown to: **Allow None** or **Allow Custom**;
Allow Custom allows you to specify allowed Ports and Services. In general, only Ports that are used or likely to be used should be open; all others should be closed for maximum security.

**3.6.6 Use of Encryption option for Saving of Configuration Data**
(as referenced in Chapter 16 in the Network and System Management Guide)

The use of Archives (Backup Configurations) is not included in the CC Evaluated Configuration, therefore this section should be IGNORED.
3.6.7 Disabling of front panel controls
For maximum security, the front panel of the BIG-IP system may be disabled. The System menu on the LCD front panel can be used to set the management port, IP address, halt or reboot the box.

To turn off this menu, go to the System Menu, General Properties, and disable the check box marked "Display LCD System Menu".

3.7 Traffic Management Settings

3.7.1 Traffic Management Information Flow Security Function Policy

The BIG-IP TOE is configured by default to enforce the unauthenticated/authenticated Traffic Management Information Flow SFP. Administrators shall assure this by verification that the following traffic flow control rules are enforced by the appliance:

Non SSL traffic (unauthenticated traffic management information flow SFP) must be configured to enforce the following rule:

The presumed IP address of the source/destination subject translates to a configured VLAN resource, information security attribute values are unambiguously permitted by the information security policy rules as configured by the Administrator including: iRules based rules permit traffic flow for Pool member, availability rules permit routing to resource in accordance with established configuration, availability/performance metrics and TOE monitor responses indicate destination resources are available, URI and header attributes translate to a backend server resource Pool assignment

SSL traffic (authenticated traffic management information flow SFP) must be configured to enforce the following rule:

The presumed IP address of the source/destination subject translates to a configured VLAN resource, information security attribute values are unambiguously permitted by the information security policy rules as configured by the Administrator including: iRules based rules permit traffic flow for Pool member, availability rules permit routing to resource in accordance with established configuration, availability/performance metrics and TOE monitor responses indicate destination resources are available, URI and header attributes translate to a backend server resource Pool assignment

Successful negotiation of SSL protocol, username/password combination resolves to a valid authenticated user role, required key exchange has
successfully taken place, certificate verification and revocation checks are successful.

### 3.8 Authentication Servers Settings

Two types of remote administration authentication servers are approved for use in the CC Evaluated configuration:

- **LDAP** - Lightweight Directory Access Protocol
- **RADIUS** - Remote Authentication Dial In User Service

#### 3.8.1 LDAP Settings

**Ref. Chapter 14 Network and System Management Guide**

For LDAP configuration objects (as applicable) assure the following security related settings are selected:

- Select Port 636 for SSL enabled communication
- SSL setting: Enabled
- Configure the SSL Client certificate settings to:
  - “Secure” setting is set to “enabled” (SSL required) between the system and LDAP server (default is “disabled”)

#### 3.8.2 RADIUS Settings

**(Reference Chapter 14 Network and System Management Guide)**

The default settings for RADIUS Authentication Servers are acceptable for the CC Evaluated Configuration, however, note that using redundant RADIUS servers is preferred.
3.9 Cookie Settings

3.9.1 Cookie Persistence Settings

(Reference Settings of a cookie persistence Chapter 9 in Local Traffic Management configuration manual table 9.1)

The default Cookie Persistence Settings offer the most secure options, therefore administrators should preserve these settings. Session Cookies provide the most secure option.

3.9.2 Cookie Encryption Settings

If your application uses cookies that could potentially contain authentication information or allow a user to impersonate another user, you should enable cookie encryption and authentication to preserve security. You will have to create an iRule that knows about the cookies and encrypts them for outbound traffic, and decrypts them on requests. Attach the iRule to your virtual server. See Chapter 13 of BIG-IP Configuration Guide for Local Traffic Management for more information.

HTTP::cookie encrypt <name> <pass phrase>
Encrypts the value for the given cookie using a key generated from the pass-phrase. The default key length is 128.

HTTP::cookie decrypt <name> <pass phrase>
Decrypts the value for the given cookie using a key generated from the pass phrase. The default key length is 128.
4 Appendix A: Reference Documents

a) Configuration Guide for Local Traffic Management version 9.2
   MAN-0185-00
b) BIG-IP® Network and System Management Guide version 9.2*
   MAN-0182-00
c) Installation, Licensing and Upgrades for BIG-IP version 9.2
d) BIG-IP® Quick Start Instructions  PUB-0089-03  1205
e) F5 Networks BIG-IP® Local Traffic Manager 6400 High Availability pair
    (qty 2) Security Target 05-948-R-0105
f) Configuration Worksheet PUB-0090-02  0905

*9.2 in this instance applies to the TOE Revision 9.2.3 + Hotfix CR69440