Deployment Guide
RADIUS Servers

Deploying the BIG-IP System v11 with RADIUS Servers

Welcome to the F5 deployment guide for RADIUS servers. This document contains guidance on configuring the BIG-IP system version 11 for intelligent traffic management for RADIUS servers, resulting in a secure, fast, and available deployment.

BIG-IP version 11.0 introduces iApp™ Application templates, an extremely easy way to accurately configure the BIG-IP system for your RADIUS servers.

Why F5?

The BIG-IP system provides a number of ways to accelerate, optimize, and scale RADIUS server deployments. The BIG-IP LTM uses an advanced health monitor that logs on to an RADIUS server to ensure traffic is only sent to available RADIUS servers.

To provide feedback on this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com.*

Products and versions tested

Product	Version
BIG-IP LTM	v11.0 - 11.3.x

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/radius-iapp-dg.pdf.*

What is F5 iApp™?

New to BIG-IP version 11, F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp template for RADIUS acts as the single-point interface for building, managing, and monitoring your RADIUS deployment.

For more information on iApp, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network: http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf.*

Document Version

1.2

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

➤ For this deployment guide, the BIG-IP LTM system ***must*** be running version 11.0 - 11.3.x. If you are using a previous or later version of the BIG-IP LTM system, see the Deployment Guide index on F5.com. The configuration described in this guide does not apply to previous or later versions. There is an updated iApp and guide for 11.4 and later.

This document provides guidance for using the iApp for RADIUS found in version 11.0 - 11.3.x. For advanced users extremely familiar with the BIG-IP, there are manual configuration tables at the end of this guide. However, we strongly recommend using the iApp template.

➤ The BIG-IP health monitor created by the iApp requires an RADIUS user account. To check the health of the servers, the monitor uses this account to log in to RADIUS to verify server health. We recommend creating a new RADIUS user account for this health monitor.

➤ The RADIUS server must be configured to accept connections from BIG-IP Self IP address. Consult your RADIUS documentation for specific instructions.
In our example, we are using FreeRADIUS, so we add the BIG-IP address to the clients file, found in **/etc/freeradius/clients** with the following command syntax:

```
client 192.168.12.230 {
    secret = testing123
    shortname = bigip0
}
```

➤ By default, the iApp configures Datagram load balancing. MSCHAPv2 (and other challenge/response authentication mechanisms) do not work with Datagram load balancing, due to multiple RADIUS packets per session. All packets in the conversation need to be delivered to the same server in order for this authentication mechanism to function correctly. If you are using MSCHAPv2 or another challenge/response authentication mechanism, see *Optional: Modifying the iApp configuration if using MSCHAPv2 on page 8.*

➤ See *Appendix B: Test environment configuration information on page 12* and *Verifying successful RADIUS authN on page 13* for additional information.

Configuration example

In this deployment guide, the BIG-IP system is optimally configured to optimize and direct traffic to RADIUS servers. This diagram shows a logical configuration example with a redundant pair of BIG-IP LTM devices in front of a group of RADIUS servers.
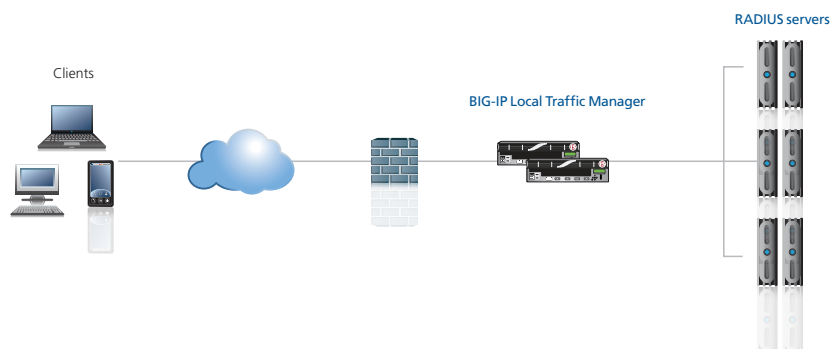
Preparation Worksheet

In order to use the iApp for RADIUS, you need to gather some information, such as server IP addresses and domain information. Use the following worksheet to gather the information you will need while running the template. The worksheet does not contain every question in the template, but rather includes the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages.

You might find it useful to print this table and then enter the information.

➲ **Note:** *Although we show space for 7 pool members, you may have more or fewer members in each pool.*

IP Addresses/FQDN	Sync/Failover Groups*	RADIUS services
IP address you will use for the LTM virtual server:	If using the Advanced feature of Sync/Failover Groups, you must already have a Device Group and a Traffic Group Device Group name: Traffic Group name:	The template can configure the BIG-IP system for RADIUS Authentication and Authorization, and Accounting. You must configure the template for Authentication and Authorization, and/or Accounting.

Authentication and Authorization		
Virtual Server port	**Pool Members**	**Health monitor**
You must chose whether the virtual server listens on Port 1645, 1812, or both. 1645 1812 Both ports	RADIUS server IP addresses: 1: 2: 3: 4: 5: 6: 7: Port: 1645 or 1812	The health monitor requires a RADIUS user account. We recommend creating new account for this monitor. User name Associated Password: Secret: Network Access Server (NAS) IP address:

Accounting		
Virtual Server port	**Pool Members**	**Health monitor**
You must chose whether the virtual server listens on Port 1646, 1813, or both. 1646 1813 Both ports	RADIUS server IP addresses: 1: 2: 3: 4: 5: 6: 7: Port: 1646 or 1813	The health monitor requires a RADIUS user account. We recommend creating new account for this monitor. User name Secret: Network Access Server (NAS) IP address:

* Optional

Configuring the BIG-IP iApp for RADIUS

Use the following guidance to help you configure the BIG-IP system for RADIUS servers using the BIG-IP iApp template.

Getting Started with the iApp for RADIUS

To begin the RADIUS iApp Template, use the following procedure.

1. Log on to the BIG-IP system.

2. On the Main tab, expand **iApp**, and then click **Application Services**.

3. Click **Create**. The Template Selection page opens.

4. In the **Name** box, type a name. In our example, we use **RADIUS_**.

5. From the **Template** list, select **f5.radius**.
    The RADIUS template opens.

Advanced options

If you select Advanced from the Template Selection list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. For more information on Device Management, see the Online Help or product documentation.

1. **Configure Sync/Failover?**
    If you want to configure the Application for Sync or failover groups, select **Yes** from the list.

    a. **Device Group**
        If you select Yes from the question above, the Device Group and Traffic Group options appear. If necessary, uncheck the Device Group box and then select the appropriate Device Group from the list.

    b. **Traffic Group**
        If necessary, uncheck the Traffic Group box and then select the appropriate Traffic Group from the list.

Virtual Server Questions

The next section of the template asks questions about the BIG-IP virtual server. A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. Clients send traffic to a virtual server, which then directs the traffic according to your configuration instructions.

1. **IP address for the virtual server**
    This is the address clients use to access the RADIUS servers (or a FQDN will resolve to this address). You need an available IP address to use here.

2. **Routes or secure network address translation**
    If the RADIUS servers do not have a route back for clients through the BIG-IP, i.e. if they do not use the BIG-IP as the default gateway, the BIG-IP uses Secure Network Address Translation (SNAT) Automap (exception in #3) to translate the client's source address to an address configured on the BIG-IP. The servers then use this new source address as the destination address when responding to traffic originating through the BIG-IP.

    If you indicate the RADIUS servers do have a route back to the clients through the BIG-IP, the BIG-IP does not translate the client's source address; in this case, you must make sure that the

BIG-IP is configured as the gateway to the client networks (usually the default gateway) on the RADIUS servers.

We recommend choosing **No** from the list because it is secure and does not require you to configure routing manually.

If you are configuring your BIG-IP LTM in a "one-armed" configuration with your RADIUS servers -- where the BIG-IP virtual server(s) and the RADIUS servers have IP addresses on the same subnet – you must choose No.

3. **More than 64,000 simultaneous connections**
   If you do not expect more than 64,000 simultaneous connections, leave this answer set to **No** and continue with the next section.

   If you have a large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need one IP address for each 64,000 connections you expect. Select **Yes** from the list. A new row appears with an IP address field. In the **Address** box, type an IP address and then click **Add**. Repeat for any additional IP addresses.

Authentication and Authorization Server Pool and Load Balancing questions

In this section, if you have enabled Authentication and Authorization on the RADIUS servers, you configure the health monitor and pool for Authentication and Authorization. If Authentication and Authorization are not enabled, continue with the following section. Note you must choose at least one (Authentication and Authorization and/or Accounting) for this template.

1. **Authentication and Authorization enabled?**
   If you have enabled Authentication and Authorization on the RADIUS servers, select Yes from the list.

   If you have *not* enabled Authentication and Authorization, you must have enabled Accounting to use the template. See *Accounting Server Pool and Load Balancing Questions on page 6.*

2. **Virtual Server Port**
   You can configure the BIG-IP virtual server to listen on port 1645, 1812, or both ports. Chose the appropriate option from the list.

3. **New Pool**
   Choose **Create New Pool** unless you have already made a pool on the LTM for the RADIUS devices.

4. **Load balancing method**
   While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (member)**.

5. **Address/Port of the RADIUS servers**
   Type the IP Address of each RADIUS server, and then select the appropriate port from the list (1645 or 1812). You can optionally add a Connection Limit. Click **Add** to add additional servers to the pool.

6. **Health Monitor**
   Choose **Create New Monitor** unless you have already made a health monitor on the LTM for the RADIUS devices.

7. **User Name**
The health monitor requires an RADIUS user account, which the BIG-IP uses to log on to the server. Type the user name.

Warning: The user name cannot contain a hash (#) character.

8. **Password**
Type the password for the user name you entered above.

Warning: The Password cannot contain a hash (#) character.

9. **Secret**
Type the RADIUS secret used to verify the RADIUS messages.

Warning: The Secret cannot contain a hash (#) character.

10. **NAS IP address**
Type the IP address of the Network Access Server.

Accounting Server Pool and Load Balancing Questions

In this section, if you have enabled Accounting on the RADIUS servers, you configure the health monitor and pool for Accounting. If Accounting is not enabled, continue with the following section. Note you must choose at least one (Authentication and Authorization and/or Accounting) for this template.

1. **Accounting enabled?**
If you have enabled Accounting on the RADIUS servers, select Yes from the list.

If you have *not* enabled Accounting, you must have enabled Authentication and Authorization to use the template. See *Authentication and Authorization Server Pool and Load Balancing questions on page 5*.

2. **Virtual Server Port**
You can configure the BIG-IP virtual server to listen on port 1646, 1813, or both ports. Chose the appropriate option from the list.

3. **New Pool**
Choose **Create New Pool** unless you have already made a pool on the LTM for the RADIUS devices.

4. **Load balancing method**
While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (member)**.

5. **Address/Port of the RADIUS servers**
Type the IP Address of each RADIUS server, and then select the appropriate port from the list (1646 or 1813). You can optionally add a Connection Limit. Click **Add** to add additional servers to the pool.

6. **Health Monitor**
Choose **Create New Monitor** unless you have already made a health monitor on the LTM for the RADIUS devices.

7. **User Name**
The health monitor requires an RADIUS user account, which the BIG-IP uses to log on to the server. Type the user name.

Warning: The user name cannot contain a hash (#) character.

8. **Secret**
   Type the RADIUS secret used to verify the RADIUS messages.

   Warning: The Secret cannot contain a hash (#) character.

9. **NAS IP address**
   Type the IP address of the Network Access Server.

Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects for the RADIUS implementation.

Optional: Modifying the iApp configuration if using MSCHAPv2

If you are using MSCHAPv2 or another challenge/response authentication mechanism, you must disable Datagram load balancing (currently configured by the iApp by default). To modify the Datagram load balancing setting, you must first disable the Strict Updates feature on the iApp.

Disabling the Strict Updates feature

Before modifying the configuration produced by the iApp, you must turn off the Strict Updates feature. By turning off Strict Updates, if you re-enter the iApp template and modify the configuration within the iApp, you will have to make all of the following changes again manually. A future version of the template will contain these modifications.

To turn off Strict Updates

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your RADIUS Application service from the list.
3. From the **Application Service** list, select **Advanced**.
4. In the **Strict Updates** row, clear the check from the box to disable Strict Updates.
5. Click the **Update** button.

Modifying the Datagram load balancing setting

The next task is to modify the UDP profile created by the iApp to disable Datagram load balancing.

To modify the UDP profile

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your RADIUS Application service from the list.
3. On the Menu bar, click **Components**. The BIG-IP objects for the iApp appear.
4. From the list, click the name of the UDP profile that was created by the iApp. This profile is preceded by the name you gave the iApp, followed by **_udp_monitor**. This is not actually a monitor, but the UDP profile.
5. Click to clear check from the **Datagram LB Enabled** box.
6. Click the **Update** button.
7. *Optional*: After modifying the template, we recommend turning Strict Updates back on. However, if you modify the iApp in the future, you must modify the UDP profile again. To turn on Strict Updates, use the procedure above for turning off Strict Updates, but in Step 4, click a check in the box to Enable Strict Updates.

For more information on the UDP profile, see
http://support.f5.com/kb/en-us/solutions/public/7000/500/sol7535.html

For more information on Datagram load balancing, see
http://support.f5.com/kb/en-us/solutions/public/3000/600/sol3605.html

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the RADIUS service you just created. To see the list of all the configuration objects created to support RADIUS, on the Menu bar, click **Components**. The complete list of all RADIUS related objects opens. You can click individual objects to see the settings.

Once the objects have been created, you are ready to use the new deployment.

Modifying DNS settings to use the BIG-IP virtual server address

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for the RADIUS implementation to point to the BIG-IP system's virtual server address.

Modifying the iApp configuration

The iApp application service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). As a safer option, the iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your RADIUS Application Service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the RADIUS configuration objects created by the iApp template.

Object-level statistics
Use the following procedure to view object-level statistics.

To view object-level statics

1. On the Main tab, expand **Overview**, and then click **Statistics**.
2. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers.
3. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.
4. To see Networking statistics in a graphical format, click **Dashboard**.

For more information on viewing statistics on the BIG-IP system, see the online help or product documentation.

Appendix A: Manual configuration table

We strongly recommend using the iApp template to configure the BIG-IP system for nPath. Advanced users familiar with the BIG-IP system can use the following table to manually configure the system.

The following table contains a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

There are two tables below, one for RADIUS Authentication and Authorization, and one for RADIUS Accounting. Use the the table applicable for your configuration. If you are using both services, use both tables.

RADIUS Authentication and Authorization configuration table

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	*Name*	Type a unique name	
	Type	**RADiUS**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
	User Name	Type the User Name of a RADIUS user. **Warning:** *The user name cannot contain a hash (#) character*	
	Password	Type the associated password. **Warning:** *The password cannot contain a hash (#) character*	
	Secret	Type the RADIUS secret. **Warning:** *The secret cannot contain a hash (#) character*	
	NAS IP Address	Type the IP address of the Network Access Server	
Pool (*Main tab-->Local Traffic -->Pools*)	*Name*	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We use the default **Round Robin**	
	Address	Type the IP Address of the RADIUS nodes	
	Service Port	Either **1645** or **1812** as applicable (you can optionally create an addition pool, one for each service port). Click **Add** to repeat Address and Service Port for all nodes	
	Additional Pool (optional)	If your configuration requires a separate pool for both service ports (1645 and 1812), create an additional pool using the settings above. Use whichever service port you did not use above (either 1645 or 1812). Be sure to give this second pool a unique name)	
Profiles (*Main tab-->Local Traffic -->Profiles*)	*UDP* (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**UDP**
		Datagram LB	**Enabled** (If using MSCHAPv2, leave Datagram LB Disabled. see *Optional: Modifying the iApp configuration if using MSCHAPv2 on page 8 for more information*)
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	*Name*	Type a unique name	
	Address	Type the IP Address for the virtual server	
	Service Port	Either **1645** or **1812** as applicable (you can optionally create an addition virtual server, one for each service port)	
	Protocol	**UDP**	
	Protocol Profile (client)[1]	Select the UDP profile you created above	
	SNAT Pool [2]	**Automap** (optional; see footnote [2])	
	Default Pool	Select the pool you created above	
	Additional virtual server (optional)	If you configured an additional pool above, create an additional virtual server using the settings above. Use the service port you did not use above (either 1645 or 1812). Be sure to give this second pool a unique name).	

[1] You must select **Advanced** from the **Configuration** list for these options to appear
[2] *If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.*

RADIUS Accounting configuration table

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	*Name*	Type a unique name
	Type	**RADiUS Accounting**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	User Name	Type the User Name of a RADIUS user. **Warning:** *The user name cannot contain a hash (#) character*
	Secret	Type the RADIUS secret. **Warning:** *The secret cannot contain a hash (#) character*
	NAS IP Address	Type the IP address of the Network Access Server
Pool (*Main tab-->Local Traffic -->Pools*)	*Name*	Type a unique name
	Health Monitor	Select the monitor you created above
	Slow Ramp Time[1]	**300**
	Load Balancing Method	Choose a load balancing method. We use the default **Round Robin**
	Address	Type the IP Address of the RADIUS nodes
	Service Port	Either **1646** or **1813** as applicable (you can optionally create an addition pool, one for each service port). Click **Add** to repeat Address and Service Port for all nodes
	Additional Pool (optional)	If your configuration requires a separate pool for both service ports (1646 and 1813), create an additional pool using the settings above. Use whichever service port you did not use above (either 1646 or 1813). Be sure to give this second pool a unique name)
Profiles (*Main tab-->Local Traffic -->Profiles*)	**UDP** (*Profiles-->Protocol*)	Name Type a unique name
		Parent Profile **UDP**
		Datagram LB **Enabled** (If using MSCHAPv2, leave Datagram LB Disabled. see *Optional: Modifying the iApp configuration if using MSCHAPv2 on page 8 for more information*)
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	*Name*	Type a unique name
	Address	Type the IP Address for the virtual server
	Service Port	Either **1646** or **1813** as applicable (you can optionally create an addition virtual server, one for each service port)
	Protocol	**UDP**
	Protocol Profile (client)[1]	Select the UDP profile you created above
	SNAT Pool[2]	**Automap** (optional; see footnote [2])
	Default Pool	Select the pool you created above
	Additional virtual server (optional)	If you configured an additional pool above, create an additional virtual server using the settings above. Use whichever service port you did not use above (either 1646 or 1813). Be sure to give this second pool a unique name).

[1] You must select **Advanced** from the **Configuration** list for these options to appear
[2] If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.

Appendix B: Test environment configuration information

The following information shows the configuration of the non-F5 devices used in our test environment.

Participating Nodes

- FreeRADIUS server listening on: 192.168.12.29/24:1812

- BIG-IP LTM
  - Self IP VLAN 12: 192.168.12.230/24
  - Self IP VLAN 245: 192.168.245.230/24

- Dell 5424 switch
  - VLAN 245 IP 192.168.245.201/24
  - ethernet g21 configured for 802.1X authentication
  - configured to authenticate 802.1X via RADIUS server @ 192.168.245.129:1812

- Linux supplicant host
  Attached directly to switchport g21 via eth3
  using wpa_supplicant to issue 802.1X EAP frames to switchport

Configure FreeRADIUS (Debian Squeeze)

- Add BIG-IP to clients file (/etc/freeradius/clients.conf):
  ```
  client 192.168.12.230 {
     secret = testing123
     shortname = bigip0
   }
  ```

- Add credentials to users file (/etc/freeradius/users)
  proliant0eth3 Cleartext-Password := "testing"
  steve   Cleartext-Password := "testing" # exists in default config

- Start freeradius in debug mode
  - $ sudo /etc/init.d/freeradius stop
  - $ sudo /usr/sbin/freeradius -X

Configure Dell 5424 Switch

- dot1x system-auth-control
  ```
  interface ethernet g21
     dot1x port-control auto
     dot1x re-authentication
     dot1x max-req 10
     dot1x timeout re-authperiod 300
     dot1x timeout quiet-period 1
  exit
  ```

- interface vlan 245
  ```
  ip address 192.168.245.201 255.255.255.0
  exit
  ```

- radius-server host 192.168.245.129 auth-port 1812 key testing123 usage dot1.x

- aaa authentication dot1x default radius

Configure 802.1X supplicant (Debian Squeeze)

- create wpa_supplicant-eth3 (man wpa_supplicant.conf)

```
ctrl_interface=/var/run/wpa_supplicant
 ap_scan=0
 network={
        key_mgmt=IEEE8021X
        eap=MD5
        identity="proliant0eth3"
        password="testing"
        eapol_flags=0
 }
```

- Start wpa_supplicant in debug mode on interface attached to g21

```
$ sudo apt-get -y install wpasupplicant
$ sudo wpa_supplicant -d -Dwired -ieth3 -c/home/cjac/tmp/wpa_supplicant-
eth3
```

Verifying successful RADIUS authN

The following is the output to the FreeRADIUS debug console during a successful EAP/MD5 authentication request in our example

```
rad_recv: Access-Request packet from host 192.168.12.230 port 49158, id=0, length=91
        NAS-IP-Address = 192.168.245.201
        NAS-Port-Type = Ethernet
        NAS-Port = 21
        User-Name = "proliant0eth3"
        EAP-Message = 0x02b300120170726f6c69616e743065746833
        Message-Authenticator = 0xf2a175759c8f1c09847530924206f050
# Executing section authorize from file /etc/freeradius/sites-enabled/default
+- entering group authorize {...}
++[preprocess] returns ok
++[chap] returns noop
++[mschap] returns noop
++[digest] returns noop
[suffix] No '@' in User-Name = "proliant0eth3", looking up realm NULL
[suffix] No such realm "NULL"
++[suffix] returns noop
[eap] EAP packet type response id 179 length 18
[eap] No EAP Start, assuming it's an on-going EAP conversation
++[eap] returns updated
[files] users: Matched entry proliant0eth3 at line 90
++[files] returns ok
++[expiration] returns noop
++[logintime] returns noop
[pap] WARNING: Auth-Type already set.  Not setting to PAP
++[pap] returns noop
Found Auth-Type = EAP
# Executing group from file /etc/freeradius/sites-enabled/default
+- entering group authenticate {...}
```

```
[eap] EAP Identity
[eap] processing type md5
rlm_eap_md5: Issuing Challenge
++[eap] returns handled
Sending Access-Challenge of id 0 to 192.168.12.230 port 49158
        EAP-Message = 0x01b400160410f4e0d93077f6bee67f014150792e4312
        Message-Authenticator = 0x00000000000000000000000000000000
        State = 0x233c09a423880df339ce99821b06cde4
Finished request 116.
Going to the next request
Waking up in 4.9 seconds.
rad_recv: Access-Request packet from host 192.168.12.230 port 49158, id=0, length=113
# Executing section authorize from file /etc/freeradius/sites-enabled/default
+- entering group authorize {...}
++[preprocess] returns ok
++[chap] returns noop
++[mschap] returns noop
++[digest] returns noop
[suffix] No '@' in User-Name = "proliant0eth3", looking up realm NULL
[suffix] No such realm "NULL"
++[suffix] returns noop
[eap] EAP packet type response id 180 length 22
[eap] No EAP Start, assuming it's an on-going EAP conversation
++[eap] returns updated
[files] users: Matched entry proliant0eth3 at line 90
++[files] returns ok
++[expiration] returns noop
++[logintime] returns noop
[pap] WARNING: Auth-Type already set.  Not setting to PAP
++[pap] returns noop
Found Auth-Type = EAP
# Executing group from file /etc/freeradius/sites-enabled/default
+- entering group authenticate {...}
[eap] Request found, released from the list
[eap] EAP/md5
[eap] processing type md5
[eap] Freeing handler
++[eap] returns ok
# Executing section post-auth from file /etc/freeradius/sites-enabled/default
+- entering group post-auth {...}
++[exec] returns noop
Sending Access-Accept of id 0 to 192.168.12.230 port 49158
        EAP-Message = 0x03b40004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "proliant0eth3"
Finished request 117.
```

Document Revision History

Version	Description	Version
1.0	New Version	N/A
1.1	**-** Added information for disabling Datagram load balancing if using MSCHAPv2 or other challenge/response authentication methods. - Added Appendix B: Test environment configuration information.	11/09/2011
1.2	- Added warnings in the iApp walkthrough and the manual configuration tables about not using hash (#) characters in the RADIUS user account User Name, Password, or Secret you choose for the health monitor. - Added to the note in the prerequisites about the maximum version of the BIG-IP system this guide applies to (11.3.x). An updated version of the iApp template and the deployment guide are available in 11.4 and later.	06/06/2014