

IMPORTANT: This guide has been archived. While the content in this guide is still valid for the products and version listed in the document, it is no longer being updated and may refer to F5 or 3rd party products or versions that have reached end-of-life or end-of-support. See <https://support.f5.com/csp/article/K11163> for more information.



Configuring the BIG-IP System for NIST SP-800-53r4 Compliance

Welcome to the F5 Configuring BIG-IP for NIST SP-800-53r4 Compliance deployment guide. This document provides guidance on using the F5 iApp for NIST SP-800-53r4 to configure a BIG-IP device to support security controls according to the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53 (Revision 4): Security and Privacy Controls for Federal Information Systems and Organizations (updated 01-02-2015).

NIST SP-800-53r4 is a complex document. Only some of the controls (that is, policies plus supporting technical measures) that organizations adopt to comply with SP-800-53r4 relate to the BIG-IP configuration. This deployment guide discusses the security controls in Appendix F of NIST SP-800-53r4 most applicable to BIG-IP configuration and shows how to support them.

This guide is about configuring the management features of the BIG-IP system rather than the network-traffic-processing modules of system such as BIG-IP Local Traffic Manager. In other words, this deployment guide helps you manage the BIG-IP system as an entity responsive to your SP-800-53r4 controls. Using BIG-IP as a tool to help control other entities like network-based applications is beyond the scope of this document.

For more information on the F5 BIG-IP platform, see <http://www.f5.com/products/big-ip>.

For more information on the F5 BIG-IP Traffic Management Shell (tmsh), see https://support.f5.com/kb/en-us/products/big-ip_tm/manuals/product/bigip-tmsh-reference-12-0-0.html.

For information on NIST, see <http://csrc.nist.gov/>

Products and applicable versions

Product	Version
BIG-IP	11.5.3 - 12.1.2
NIST	SP-800-53r5
iApp Template Version	f5.nist_sp800-53.v1.0.0 and v1.0.1rc5
Deployment Guide version	2.1 (see <i>Document Revision History on page 24</i>)
Last updated	01-31-2019

Important: Make sure you are using the most recent version of this deployment guide, available at <http://www.f5.com/pdf/deployment-guides/nist-sp-800-53-r4-dg.pdf>.

If you are looking for older versions of this or other deployment guides, check the Deployment Guide Archive tab at: <https://f5.com/solutions/deployment-guides/archive-608>

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

Contents

What is F5 iApp™?	3
Prerequisites and configuration notes	3
Before Creating the Application Service from the iApp Template	4
Configuring the BIG-IP system using the iApp template	4
Downloading and importing the iApp template	4
Starting the iApp template	4
Template Options	4
Security Controls	6
User Authentication/Directory Service — AC-6, IA-2	6
External Authentication/Directory Server(s) — IA-2, IA-3	7
Remote Roles — AC-3(7), CM-5	11
Password Strength Policy — IA-5(1)	12
Usage banner — AC-8	12
Display Last Access — AC-9 (Advice-only block)	13
Maximum Failed Login Attempts — AC-7	13
Idle Timeouts for Management Access — AC-2(5), SC-10	13
Concurrent Management GUI Access — AC-10	13
Session Locking and Termination — AC-11, AC-12 (Advice-only block)	13
Management Access IP Addresses — SC-7	14
SNMP Access IP Addresses — SC-7	14
Self IP Lockdown — AC-4, SC-7	14
NTP Configuration — AU-8(1,2)	15
Auditing — AU-2, CM-5	15
Syslog Configuration — AU-8, AU-9(2), AU-12(2)	16
Finished	16
NIST SP-800-53r4 Security Controls Review	17
Access Control Family	17
Awareness and Training	18
Audit and Accountability	18
CA Family of Controls	19
Contingency Planning	20
Identification and Authentication	20
Incident Response	20
Maintenance	20
Physical and Environmental Protection	21
Planning	21
Personnel Security	21
Risk Assessment Policy and Procedures	21
System and Services Acquisition	21
System and Communications Protection	21
System and Information Integrity	21
Appendix: User roles	22
Document Revision History	23

What is F5 iApp™?

Introduced in BIG-IP version 11.0, F5 iApp is a set of features in the BIG-IP system that provides a new way to manage BIG-IP configurations. An iApp template brings together configuration elements, architectural rules, and a management view used to deliver an application reliably and efficiently. 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>.

Prerequisites and configuration notes

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

General prerequisites and notes

- This Deployment Guide and the iApp template are intended to help you achieve compliance to a policy which includes a collection of security controls. Therefore, this document tries to explain clearly how the NIST iApp functions and what you should be aware of to avoid a false sense of compliance.
- NIST Special Publication 800-53r4 defines security and privacy controls for all U.S. Federal information systems and organizations. Many non-governmental organizations also draw guidance from SP-800-53r4. Since SP-800-53r4 is used by a wide audience inside and outside government the F5 NIST iApp template should be useful to many organizations.
- The BIG-IP system must be running v11.6 or later. While this iApp may work on earlier versions, they have not been tested and therefore cannot be supported.
- Depending on the external authentication/directory service you are using, you may need to import SSL/TLS certificates and keys onto the BIG-IP system. See *External Authentication/Directory Server(s) — IA-2, IA-3 on page 7* for more information. Importing certificates and keys is not a part of this guide. See **System > File Management > SSL Certificate List** or the BIG-IP documentation for specific instructions.
- Because this iApp template is not application-specific like most other F5 iApps, and the purpose of the iApp is to group and manage a number of BIG-IP management plane settings, this guide does not provide manual configuration instructions.

Important configuration notes concerning how this iApp template is different than other F5 iApp templates

- **Configuration folders**
As of version 11, BIG-IP TMOS supports “folders” within the configuration as a means to group and control configuration objects (each Administrative Partition has a folder). By default, objects are placed in the /Common folder, and this iApp operates on objects in /Common. However, BIG-IP administrators may place objects into other folders explicitly, or implicitly by using another iApp (most iApps create subfolders to hold configuration objects for the application services they manage). The objects managed by this iApp are nearly always kept in /Common so subfolders do not pose a problem. However, be aware of the possibility that this iApp could fail to update an object of interest (most likely a Self IP) created by another iApp outside of /Common.
- **iApp Strict Updates**
In general, most objects created by any particular iApp will be owned by that iApp, and attempts to modify those objects outside of the originating iApp fail (unless the Strict Updates feature has been disabled). This NIST iApp can create some objects that will be unmodifiable outside of it, which is generally desirable because this iApp is security-relevant and you would not want uncoordinated changes.

However, this iApp also manages many objects which exist on every BIG-IP system. This iApp does not create those objects but rather uses modify commands to update them without gaining ownership. If this iApp tries to manage some object that happens to have been created by another iApp, its modify commands may fail and you may have to visit the other iApp to make any required changes.
- **Modifications outside the NIST iApp**
When possible this iApp takes initial values for various options from the current system configuration. However, as described above, this iApp does not own most of the configuration items it manages so many can still be changed outside of it. When that occurs, revisiting the configuration of this iApp will not show “outside” changes and saving the configuration of this iApp will overwrite those changes.

Before Creating the Application Service from the iApp Template

The f5.nist_sp800-53 iApp template (also referred to as the "NIST iApp" for simplicity in this guide) lets you configure an external directory service to authenticate BIG-IP management users. If you might use Microsoft Active Directory, an LDAP directory, or a directory service accessed via BIG-IP Access Policy Manager (APM) for user authentication you may wish to import PKI certificates and private keys, and/or create a BIG-IP APM System Authentication Profile and Access Policy before you create the Application Service from the iApp Template. See the discussion of authentication and external directory services in *User Authentication/Directory Service — AC-6, IA-2 on page 6* and *External Authentication/Directory Server(s) — IA-2, IA-3 on page 7*.

Configuring the BIG-IP system using the iApp template

Use the following guidance to use the iApp template for configuring the BIG-IP system.

Downloading and importing the iApp template

The first task is to download and import the NIST iApp template.

To download and import the iApp

1. Open a web browser and go to downloads.f5.com.
2. Click **Find a Download**, and then in the **BIG-IP F5 Product Family** section, click **iApp-Templates**.
3. Accept the EULA, and then download the iapps zip file to a location accessible from your BIG-IP system.
4. Extract (unzip) the **f5.nist_sp800-53.v<latest version>.tmpl** file. For this release, the latest is in the root directory of the zip file.
5. Log on to the BIG-IP system web-based Configuration utility.
6. On the Main tab, expand **iApp**, and then click **Templates**.
7. Click the **Import** button on the right side of the screen.
8. Click a check in the **Overwrite Existing Templates** box.
9. Click the **Browse** button, and then browse to the location you saved the iApp file.
10. Click the **Upload** button. The iApp is now available for use.

Starting the iApp template

To begin the iApp Template, use the following procedure.

To start the iApp template

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 **NIST-**.
5. From the **Template** list, select **f5.nist_sp800-53.v1.0.0** (or newer if applicable).

Template Options

This section of the iApp template asks general questions about the deployment and iApp options.

1. ***Do you want to see inline help***

Select whether you want to see informational and help messages inline throughout the template. If you are unsure, we recommend leaving the default, **Yes, show inline help text**.

Important and critical notes are always shown, no matter which selection you make.

- **Yes, show inline help text**

Select this option to show inline help for most questions in the template.

- **No, do not show inline help text**

Select this option if you do not want to see inline help. If you are familiar with this iApp template, or with the BIG-IP system in general, select this option to hide the inline help text.

2. ***Should the iApp show blocks containing only advice?***

BIG-IP configuration settings in the iApp template are organized in blocks you can match to the catalog of security controls in Appendix F of NIST SP-800-53r4. For some security controls, the iApp template can offer information to help a BIG-IP administrator with compliance even though there are no specific BIG-IP configuration settings available to change.

- **Yes, show advice-only blocks**

Select this option if you want to see the information-only blocks.

- **No, do not show advice-only blocks**

Select this option if you do not want the system to show these information-only blocks. You can always re-enter the template at another time to change your answer.

3. ***Do you want to see the option to revert to pre-iApp configuration?***

This question only appears when re-entering an already configured NIST iApp Application Service using the Reconfigure option.

This iApp template is rather unique in that it adjusts BIG-IP management configuration settings rather than BIG-IP traffic handling configuration. Generally when you remove an Application Service created by an iApp, all of its configuration objects and changes are removed automatically. However, the NIST iApp template may make configuration changes which you can only revert by making an explicit choice inside the iApp template before you remove the Application Service.

Use this question to revert to the BIG-IP configuration that existed before you ran this iApp template.

- **No, do not show the option to revert the configuration**

Select this option if you do not want the iApp to show the option to revert the iApp configuration. This question reduces the chance of reverting the settings by accident.

- **Yes, show the option to revert the configuration**

Select this option if you want the system to show the option to revert the configuration to its pre-iApp state. This does not revert the configuration, but exposes the option to revert.

- a. ***Date and Time the configuration was saved***

This field shows the date and time the configuration was saved. This corresponds to the configuration settings that existed before the first time you submitted the template.

- b. ***Do you want to revert to the pre-iApp configuration?***

Choose whether you want to revert to the pre-iApp configuration at this time, or if you want to configure the system using the iApp template.

- **No, use the settings configured in this iApp template**

Select this option to configure the system for NIST using the iApp and do not want to revert the configuration.

- **Yes, revert to the pre-iApp configuration when I click Finished**

Select this option if you want to revert the configuration back to the way it was before you ever configured the iApp template. This reverts any changes made by the NIST iApp, even if you adjusted it more than once, and may remove manual changes made outside this iApp.

i Important Remember, this iApp does not own most of the configuration items it manages, so many of the settings can still be changed outside of it. When that occurs, revisiting the configuration of this iApp will not reflect these manual changes you made outside the iApp template. If you use the Reconfigure option to make changes within the iApp template, saving the iApp configuration overwrites any outside manual changes to the configuration objects managed by the iApp.

Security Controls

The following sections of the template are marked with the key security controls to which they relate. Because many NIST SP-800-53 security controls are synergistic, each section may relate to more than one control. A more general discussion of applying NIST SP-800-53 security controls to BIG-IP appears in Section *NIST SP-800-53r4 Security Controls Review on page 18*.

User Authentication/Directory Service — AC-6, IA-2

In this section, you can enable an external directory service to authenticate BIG-IP management users. The directory service may also store RBAC roles for users. (Even when you enable an external directory service, the BIG-IP system continues to support local user accounts.)

1. Which authentication/directory service do you want to use?

Choose which authentication or directory service you are using.

- **Local to the BIG-IP system**

Select this option if the authentication is local to the BIG-IP system. No further information is needed. Continue now with *Password Strength Policy — IA-5(1) on page 12*.

- **Active Directory (with LDAP) or,**

- **LDAP**

Select one of these options if appropriate. The configuration for Active Directory (with LDAP) and LDAP is similar because the BIG-IP management authentication service uses LDAP protocol to talk to both Microsoft Active Directory and generic LDAP directory servers. (If you want to use the Kerberos protocol with Active Directory, you must configure BIG-IP Access Policy Manager authentication—see the next bullet). Continue with Step 2.

- **BIG-IP Access Policy Manager**

Select this option if you want to use the BIG-IP APM. To enable this option you must provision the BIG-IP APM module and configure an APM System Authentication Profile with a suitable Access Policy outside this iApp. The details are beyond the scope of this document. This option only appears when at least one APM System Authentication Profile is available.

- **RADIUS**

Select this option if you are using RADIUS authentication. Continue with Step 2.

- **TACACS+**

Select this option if you are using TACACS+ authentication.

2. What is the default role for users without local accounts?

Choose which BIG-IP management role an authenticated external user should have by default (that is, when not assigned a specific role by the directory service). If unsure, leave this at the default, **No Access**. For a description of the different user roles, see *Appendix: User roles on page 23*.

i Important *Anyone having credentials the external directory will accept is an “authenticated user” even if the user is not authorized to manage the BIG-IP system at all. For example, when using Active Directory authentication, any network user with a domain logon account who can connect to the BIG-IP system may be recognized as an “authenticated user.” Unless you maintain a separate, segregated directory server to authenticate BIG-IP management users, we recommend you leave the external-user default role as “No Access.”*

- **No Access (forbid access even if authenticated)**

Select this option if you do not want to grant access to the BIG-IP system to an authenticated external user who has no BIG-IP account or role. This is the default and enables the highest level of security.

- **Select a BIG-IP management role**

Select a BIG-IP management role from the list. See *Appendix: User roles on page 23* for a description of the roles.

3. Should users without local accounts be able access the TMSH console?

This controls whether external users may access TMSH in addition to the BIG-IP management Configuration utility (GUI). If unsure, leave this at the default, “No, remote users may access only the management GUI.”

- **No, remote users may access only the management GUI**

Select this option if you do not want remote users to have access to the TMSH command line console.

- **Yes, remote users may access the TMSH console**

Select this option if you want your external users to be able to access the TMSH command line console. These users will be able to execute TMSH commands. See the Traffic Management Shell (tmsh) Reference Guide for specific information on TMSH and the available commands.

External Authentication/Directory Server(s) — IA-2, IA-3

This section appears when you choose to use an external directory to authenticate BIG-IP management users. The contents of this section vary by the type of external directory you use.

- If you chose "Local to the BIG-IP system" as the authentication/directory service you are using, continue with *Password Strength Policy — IA-5(1) on page 12*.
- If you selected RADIUS, go to *RADIUS on page 9*.
- If you selected TACACS+, go to *TACACS+ on page 9*.
- If you selected BIG-IP Access Policy Manager, go to *BIG-IP Access Policy Manager on page 11*.

- **Active Directory (using LDAP) or LDAP**

If you selected Active Directory (with LDAP) or LDAP from the list in Step 1 in the previous section, you must complete the following.

- a. **What is the name of the login attribute?**

Type the name of the login attribute in your configuration. The login attribute is an attribute of user objects in the directory. The value stored in the login attribute is the user's login username.

- b. **What is the DN of the Search Base?**

The search base defines the location in the directory from which the LDAP search for the user object begins. The search looks for a user object whose login-attribute value matches the user name entered at the BIG-IP management UI, SSH, or console login prompt.

Type the appropriate search base, such as `dc=prefix,dc=example,dc=com`.

- c. **What Search Scope do you want to use?**

A search scope defines how deep to search within the search base. Choose the appropriate search scope from the list. If you are unsure, select **Subtree**.

- **Base**

Base, or zero level, indicates a search of the base object only.

- **OneLevel**

OneLevel indicates a search of objects immediately subordinate to the base object, but does not include the base object itself.

- **Subtree**

Subtree causes a search of the whole subtree rooted at the Search Base, including that object and all its descendants.

- d. **Do directory user objects include group-membership attributes (like memberOf)?**

This question only appears if you selected "LDAP", because Active Directory supports memberOf

You may define one or more remote roles (see *Remote Roles — AC-3(7), CM-5 on page 11*) based on user membership in a group. For each remote role you specify a directory attribute (like `memberOf`) and a value (like the DN of a security group object). Users having that attribute with that value may be assigned that role. Select one of the following to indicate whether your LDAP directory attaches **memberOf** (or similar) attributes to each user object listing the groups to which the user belongs.

- **Yes. User objects list groups to which user belongs (preferred)**

Many directories support `memberOf` (or similar) attributes on user objects (each `memberOf` attribute holds the DN of one group). This is very efficient because the BIG-IP device makes just one query to learn which groups the user belongs to.

- **No. Query each group to check whether user belongs to it**

Some directories do not support `memberOf`, so the BIG-IP device must query each group separately to discover whether a user belongs to it. In this case you may specify one of {`memberOf`, `uniqueMemberOf`, `memberUidOf`} as the remote-role's attribute and give the DN of a security group object as its value. Then for each remote role, the BIG-IP device will check if the user belongs to the specified group by querying whether the group object lists the user's DN (as `member` or `uniqueMember` for `memberOf` or `uniqueMemberOf`, respectively) or login-name (as `memberUid` for `memberUidOf`).

- e. **What is the DN of the Search Account?**

Type the DN of a search account on the directory server that the BIG-IP system can use for read-only access to the DIT (directory information tree). This 'Search Account' should have READ-ONLY privileges (no write privileges) and may be shared. For Microsoft Active Directory you may type the UPN of the Search Account rather than its DN.

f. What is the Search Account secret (passphrase)?

Type the secret (or passphrase) for the search account.

g. Confirm the Search Account secret (passphrase)

Re-type the secret.

h. Do you want to secure authentication queries with TLS (SSL)?

Choose whether or not you want to use TLS to secure authentication queries. Use of LDAP without TLS is supported but not recommended. If you neglect to configure TLS, user passwords are sent across the network in cleartext.

- **No, disable TLS (not recommended)**

Select this option if you want to use LDAP without TLS.

 **Warning** If you choose to disable TLS, user passwords are sent across the network in cleartext.

- a. Which unsecure LDAP port do you want to use?

Choose which unsecure LDAP port (389 or 3268) you want to use. Port 3268 is the MS Active Directory Global Catalog service.

- **Yes, use TLS to protect authentication queries**

Select this option if you want to enable TLS. When you enable TLS you may optionally specify a CA certificate to validate the LDAPS server certificate and/or a certificate/private-key pair the BIG-IP system should use to authenticate itself to the directory server. You must acquire and then upload any required certificates and keys before you are able to choose them in the iApp. See the BIG-IP documentation or **System > File Management > SSL Certificate List** for specific instructions and information on importing certificates and keys.

- a. Which secure LDAP port do you want to use?

Choose which secure LDAP port (636 or 3269) you want to use. Port 3269 is the MS Active Directory Global Catalog service.

- b. Which CA certificate is used to validate directory servers?

If you want the BIG-IP to validate TLS certificates presented by directory servers (which means refusing to connect to directory servers that do not present valid certificates) select the Certificate Authority (CA) certificate or bundle to be used to validate directory server TLS certificates. To import a CA certificate, see System > File Management > SSL Certificate List

- c. Which TLS (SSL) client certificate should the BIG-IP use?

If you want the BIG-IP system to use a TLS client certificate to authenticate itself to the directory servers, select the TLS (SSL) client certificate and the corresponding key you imported onto the BIG-IP system. Importing certificates and keys is not a part of the iApp template, and to select a certificate from this list, it must already be present on the BIG-IP system. See **System > File Management > SSL Certificate List** for more information or to import certificates and keys.

- d. What is the private key for the BIG-IP's client certificate?

Select the associated key you imported onto the BIG-IP system for this implementation.

i. What is the IP address or FQDN of the primary directory server?

Type the IP address or FQDN of your primary LDAP/Active Directory directory server. This is a required field and you must add a value here or you will not be able to submit the template.

j. What is the IP address or FQDN of the first alternate directory server?

If you have other LDAP/Active Directory servers to add, type the first alternate server in this field. Alternate servers are optional but recommended. Once you have entered your first alternate server, if you have additional servers to add, press the Tab key or simply click any other field. The following question appears.

- a. Which additional directory servers do you want to add?

Once you enter the first alternate server, this question appears asking for additional directory servers. If you have more directory servers you want to add to the list, type the IP address or FQDN in the box. Click the **Add** button to include more servers. Use the Remove button (x) if you accidentally include an extra row.

k. Do you want to enable LDAP debugging?

Choose whether or not you want to enable LDAP debugging. This can be useful for troubleshooting. Debugging information is written to the system Audit log.

- **No, do not enable LDAP debugging**

Select this option if you do not want to enable LDAP debugging.

- **Yes, enable LDAP debugging (rarely needed)**
Select this option if you want to enable LDAP debugging. This is rarely needed and should not be left running by default because user typing errors may leave passwords in the log.

Continue with *Remote Roles* — AC-3(7), CM-5 on page 11.

- **RADIUS**

If you selected RADIUS from the list in Step 1 in the previous section, you must complete the following.

 **Warning** RADIUS encryption of passwords is very weak.

a. What is the IP address or FQDN of the primary RADIUS server?

Type the IP address or fully-qualified domain name of the primary RADIUS server.

b. What is the primary RADIUS server secret?

Type the RADIUS secret shared by the primary RADIUS server and this BIG-IP device.

c. Confirm the RADIUS secret

Confirm the secret you just typed.

d. Which port does the primary RADIUS server use?

Type the port the primary RADIUS server uses (port 1812 is standard).

e. What is the IP address or FQDN of the first alternate RADIUS server?

If you have an alternate RADIUS servers to add, type the first alternate server in this field. Alternate servers are optional but recommended. Once you have entered your first alternate server, if you have additional servers to add, press the Tab key or simply click any other field. You can add a maximum of 10 RADIUS servers. The following question appears.

a. What is the first alternate RADIUS server secret?

Once you enter the first alternate server, this question appears asking for the secret for the alternate server. Type the RADIUS secret shared by the alternate server and the BIG-IP system.

b. Which port does the alternate RADIUS server use?

If your RADIUS server uses a port other than 1812, type it in the list.

c. Which additional RADIUS servers do you want to add?

If you have more RADIUS servers you want to add to the list, type the following information:

- **Server**

Type the IP address or FQDN of the RADIUS server in the box.

- **Secret**

Type the RADIUS secret shared by the additional RADIUS server and the BIG-IP system.

- **Confirm**

Confirm the secret you just typed.

- **Port**

If your RADIUS server uses a port other than 1812, type it in the list.

Click the **Add** button to include more servers. Use the Remove button (x) if you accidentally include an extra row.

f. Do you want to enable RADIUS debugging?

Choose whether or not you want to enable RADIUS debugging. This can be useful for troubleshooting. Debugging information is written to the system Audit log.

- **No, do not enable RADIUS debugging**

Select this option if you do not want to enable RADIUS debugging.

- **Yes, enable RADIUS debugging (rarely needed)**

Select this option if you want to enable RADIUS debugging. This is rarely needed and should not be left running by default because user typing errors may leave passwords in the log.

Continue with *Remote Roles* — AC-3(7), CM-5 on page 11.

- **TACACS+**

If you selected TACACS+ from the list in Step 1 in the previous section, you must complete the following questions. For detailed explanations of TACACS+ parameters, see <https://support.f5.com/kb/en-us/solutions/public/8000/800/sol8808.html>.

a. What is the TACACS+ service name?

The service name specifies the name of the service that the user who is requesting to be authorized will use. Identifying the service name enables the TACACS+ server to behave differently for different types of authorization requests. This setting is required. Type the service name in the field, for example: **shell**.

b. What is the TACACS+ protocol name?

Specifies the protocol associated with the value specified in Service Name, which is a subset of the associated service being used for client authorization or system accounting. Type the protocol name in the field (this is typically **http**).

c. What is the TACACS+ secret

Type the TACACS+ secret for this implementation. The TACACS+ secret is the key to encrypt passwords in the TACACS+ protocol. The same key must be set at the TACACS+ server(s).

 **Warning** The secret must NOT contain a pound sign (#) or BIG-IP management authentication will fail. For details, see <https://support.f5.com/kb/en-us/solutions/public/12000/300/sol12304.html>.

d. Confirm the TACACS+ secret

Type the secret again to confirm it.

e. Do you want to secure authentication queries with TACACS+ encryption?

Choose whether or not you want to enable TACACS+ encryption on the authentication queries. Not using encryption is supported but not recommended. If you do not enable encryption, user passwords will be exposed on the network.

- **Yes, use TACACS+ encryption to protect authentication queries**
Select this recommended option if you want to enable TACACS+ encryption to secure authentication queries.
- **No, do not use TACACS+ encryption (not recommended)**
Select this option if you do not want to enable TACACS+ encryption on the authentication queries.

 **Warning** If you do not enable encryption, user passwords are sent across the network in cleartext.

f. How should the system attempt authentication?

Choose whether you want the system to try authentication once to the primary server, or try each server.

- **Attempt authentication once to the primary server only**
If you select this option, the BIG-IP system sends authentication requests only to the primary server and authentication fails if the primary server does not respond.
- **Attempt authentication to each server**
If you select this option, the system sends an authentication request to each server in turn until one succeeds or the list of servers is exhausted (in which case authentication fails).

g. Should the system send accounting information to all servers?

Choose whether the BIG-IP system should send accounting data (such as which services users access and how much network resources they consume) only to the first available TACACS+ server, or to all of the servers.

- **Yes, send accounting information to all servers**
Select this option if you want the system to send accounting information to all the TACACS+ servers you will specify in the next question.
- **No, send accounting information only to the first available server**
Select this option if you want the system to send accounting information only to the first available TACACS+ server.

h. What is the IP address or FQDN of the primary TACACS+ server?

Type the IP address or FQDN of your primary TACACS+ server. This field is required; you must supply at least one server.

i. What is the IP address or FQDN of the first alternate TACACS+ server?

If you have another TACACS+ server to add, type the first alternate server in this field. Alternate servers are optional but recommended. Once you have entered your first alternate server, if you have additional servers to add, press the Tab key or simply click any other field. The following question appears.

a. Which additional TACACS+ servers do you want to include?

Once you enter the first alternate server, this question appears asking for additional TACACS+ servers. If you have more servers you want to add to the list, type the IP address or FQDN in the box. Click the **Add** button to include more servers. Use the Remove button (x) if you accidentally include an extra row.

j. Do you want to enable TACACS+ debugging?

Choose whether or not you want to enable TACACS+ debugging. This can be useful for troubleshooting. Debugging information is written to the system Audit log.

- **No, do not enable TACACS+ debugging**

Select this option if you do not want to enable TACACS+ debugging.

- **Yes, enable TACACS+ debugging (rarely needed)**

Select this option if you want to enable TACACS+ debugging. This is rarely needed and should not be left running by default because user typing errors may leave passwords in the log. Continue with *Remote Roles — AC-3(7), CM-5 on page 11*.

- **BIG-IP Access Policy Manager**

If you selected BIG-IP Access Policy Manager from the list in Step 1 in the previous section, you select the policy you created in this section. For this option to even appear, you must have provisioned the BIG-IP APM module and already configured an APM System Authentication Profile with a suitable Access Policy. The specific details on configuring the APM policy are beyond the scope of this document, see the BIG-IP APM documentation for your specific version for information.

a. Which APM system authentication profile do you want to use?

From the list, select the APM Access Policy you created with a Profile Type of System Authentication.

Remote Roles — AC-3(7), CM-5

When you configure an external directory service it may also store Role-Based Access Control (RBAC) roles for users (in addition to the default external-user role configured previously). The iApp template lets you define roles for up to ten groups of users (you can define more outside of the iApp if necessary). For each group, you specify how to recognize its members using directory attribute values. When you define a group you set the “BIG-IP access” field to allow or deny its members access and set each member’s RBAC role when access is allowed.

1. Do you want to add remote roles?

Choose whether you want to add a remote role to assign to users who have a certain attribute set to a particular value.

- **No (users without local accounts get the default role)**

Select this option if you want users without local accounts to be assigned the default external user role. This is the role you selected in 2. *What is the default role for users without local accounts? on page 6*.

- **Yes (assign roles based on user attributes)**

Select this option to assign roles based on user attributes.

One way to define a group is to fill in the **Directory attribute** field with the name of the relevant attribute and fill in the **Value must be** field with the value (a string) that must appear in the directory attribute to indicate group membership. Commonly you then select the *BIG-IP role* for all members of the group.

However, you may leave **Directory attribute** (and **Value must be**) empty and rely on attribute-value insertion to the field **BIG-IP role**. With attribute-value insertion, you identify a directory attribute (such as **f5-role**) that holds a number which matches a BIG-IP role name. Then you put a percent sign (%) followed by the attribute name into the **BIG-IP role** field, for example, **%f5-role**. The directory attribute must contain one of the following numeric values indicating a BIG-IP role: **0** (admin), **20** (resource admin), **40** (user manager), **80** (auditor), **100** (manager), **300** (application editor), **350** (advanced operator), **400** (operator), **450** (firewall manager), **500** (certificate manager), **510** (iRule manager), **700** (guest), **800** (web application security administrator), **810** (web application security editor), **850** (acceleration policy editor), **900** (no-access). TMOS version 11.6 and above also recognizes **480** (fraud protection manager). For each user, if the named attribute is valid, the user is assigned the role listed in the attribute.

You can use both the **Directory attribute** field and attribute-value insertion at the same time. If you do, the group membership is checked first and the role assignment done second. This lets you assign roles from different attributes to members of different groups.

Attribute-value insertion also works in the **Console access** and **Partition** fields where you can either specify Disabled/TMSH or an Administrative Partition name respectively, or put in a percent sign and the name of a directory attribute which contains an appropriate value, which is (digit) **0** or **1** to disable or enable console access, or the name of the Administrative Partition.

a. What are the settings for remote role 1?

Configure the following settings for the first remote role. See the description above for additional details.

- **Directory attribute and Value must be**

Type the name and required value of the directory attribute which determines whether to assign an external user the

BIG-IP role specified just below. If the user lacks the attribute, or if its value is different, the user will not be assigned this role (but may be assigned another role, or the default role for external users). You may leave the directory-attribute and value fields blank when you extract role information from attributes using the **%xyz** syntax described below. An example of an attribute name and value (for Active Directory or LDAP) is (attribute name) **memberOf** and (required value, the DN of a security group object) **CN=NetworkManagers,OU=IT,OU=Users,DC=example,DC=com**.

- **BIG-IP access and BIG-IP role**

Indicate whether users having the specified attribute and attribute value are allowed to access BIG-IP management services at all, and if so, which BIG-IP role they should be assigned. You may extract the role from a directory attribute 'xyz' by placing '%xyz' into the BIG-IP role field. For a list of BIG-IP role names, see the f5 Traffic Management Shell (TMSH) Reference Guide.

- **TMSH access and Partition**

For users having the specified attribute and attribute value, indicate whether they are allowed to use the BIG-IP TMSH console. Also indicate which BIG-IP Partition they may access (note that /Common includes all other partitions). You may extract the value of either field from a directory attribute 'xyz' by placing '%xyz' into the field.

b. ***Add another role?***

Choose whether you want to add another role at this time. You can add up to ten roles.

- **No**

Leave this option if you do not want to add any more roles. Continue with the next section.

- **Yes**

Select this option if you want to add another role. The same options described in step a appear. Return to step a if you need additional guidance.

Password Strength Policy — IA-5(1)

The section contains guidance on configuring a local password policy for passwords of BIG-IP local user accounts (external directory services enforce their own password-strength policies).

1. ***Do you want to enforce custom local password policy?***

Choose whether you want the system to enforce a custom password strength policy. This governs local accounts such as **admin** but not accounts in an external user authentication/directory server.

- **No, use the BIG-IP default password policy**

Select this option if you do not want the system to enforce a custom password strength policy. Continue with "*Usage banner — AC-8*" on this page.

- **Yes, enforce a local password policy**

Select this option if you want to set a local policy for password strength, valid life and reuse. You must configure the values in the following questions.

a. ***How many days should pass before the password expires?***

Type the number of days the password should be valid.

b. ***How many changes before reuse?***

Type the number of password changes you want to require before a previously used password can be reused.

c. ***How many characters should be the minimum for each setting?***

For the following settings, type a number of characters at a minimum that should be required for each.

- **Length**

Type the minimum number of characters the password should be in length. This minimum-length restriction does not apply to BIG-IP user accounts with the Administrator role, including the default **admin** and **root** accounts.

- **Lowercase**

Type the minimum number of lowercase letters that should be required. Leave 0 if you do not want to require a minimum number of lowercase characters.

- **Uppercase**

Type the minimum number of uppercase letters that should be required. Leave 0 if you do not want to require a minimum number of uppercase characters.

- **Special chars**

Type the minimum number of special characters that should be required. A special character is defined as anything you can type on a keyboard that is not a number or letter. Leave 0 if you do not want to require a minimum number of special characters.

- **Digits**
Type the minimum number of digits (numbers) that should be required. Leave 0 if you do not want to require a minimum number of digits.

Usage banner — AC-8

In this section, you have the ability to alter the banner messages which appear to users of the management web GUI or the BIG-IP command line. If you do not want to change the banner messages, you can continue with the next section.

1. ***What banner message should appear for the web-based Configuration utility?***

Type the message you want to appear when the user attempts to log in using the BIG-IP web-based Configuration utility (GUI). This field shows the message currently configured by default.

2. ***What banner message should appear for the management console?***

Type the message you want to appear when the user logs into the BIG-IP system from the console. This field shows the message currently configured by default.

Display Last Access — AC-9 (Advice-only block)

This section only appears when you choose to see information-only blocks. There are no options to change here. See the iApp template (must select Show Advice-only blocks) or the NIST specification for details.

Maximum Failed Login Attempts — AC-7

In this section you have the ability to disable a BIG-IP local user account after some number of failed login attempts. Note that an external directory server enforces its own limit.

1. ***Disable account after several failed login attempts?***

Choose whether you want to disable the account after multiple failed login attempts, or if you want to allow an unlimited number of login attempts. For stronger security, we do not recommend allowing unlimited login attempts.

- **No, allow unlimited login attempts (not recommended)**
Select this option if you do not want to limit login attempts. We do not recommend using this option because of the security risk.
- **Yes, limit failed login attempts**
Select this option if you want to limit the number of failed login attempts. You specify the number of attempts in the question that appears.
 - a. ***Allow how many consecutive login failures before disabling the account?***
Type the number of consecutive failed login attempts you want to allow before disabling the account.

Idle Timeouts for Management Access — AC-2(5), SC-10

In this section, you can adjust the idle timeout intervals for several access methods. The minimum timeout is one minute; if you enter zero, a timeout of 12 hours results.

1. ***How many minutes for each Idle Timeout value?***

For each of the following fields, type the number of minutes of idle time you want to pass before a timeout occurs. Any initial values that appear in the boxes are the current settings on the device.

Remember, a value of **0** sets an idle timeout of 12 hours (**720** minutes).

- **Management GUI**
Type the number of minutes you want to set for the web-based Configuration utility (management GUI) Idle Timeout value.
- **SSH**
Type the number of minutes you want to set for the Idle Timeout value for SSH connections.
- **Console**
Type the number of minutes you want to set for the Idle Timeout value for console connections.

- **TMSH**

Type the number of minutes you want to set for the Idle Timeout value for TMSH connections.

Concurrent Management GUI Access — AC-10

In this section, you have the ability to limit the number of concurrent users of the management web GUI. It is not currently possible to restrict the number of concurrent command-line users.

1. ***How many GUI sessions may be active at once?***

Type the number of concurrent connections you want to allow to the web-based Configuration utility (management GUI). Once the number of connections you specify is reached, any additional connection attempts are refused.

Session Locking and Termination — AC-11, AC-12 (Advice-only block)

This section only appears when you choose to see information-only blocks. There are no options to change here. See the iApp template (must select Show Advice-only blocks) or the NIST specification for details.

Management Access IP Addresses — SC-7

In this section, you have the ability to control from which IP addresses the BIG-IP management network interface accepts connections (to the management web GUI or command line).

1. ***How should the system control BIG-IP management access?***

Choose whether you want to allow all IP addresses access to the web-based Configuration utility (GUI) or the command line, or if you want to restrict access based on IP address. If possible, we recommend restricting access by the source IP addresses or subnets used by administrator workstations (or VPN tunnels).

- **Allow access from any IP address (default)**

Select this option if you do not want to restrict management access to the BIG-IP system by IP address at all.

- **Allow access only from IP addresses I specify**

Select this option if you want to restrict access to the BIG-IP Configuration utility or command line by source IP address.

- a. ***Which IP addresses should be allowed?***

Type a single IP address, or a list of acceptable source IP addresses separated by space characters. Each address may specify a host or a subnet (meaning all the hosts on that subnet) using the form address/mask.

To enable BIG-IP administrators at the command line of one BIG-IP device in a Device Group to access other BIG-IP devices in that group, add the management-port addresses or subnets of all devices in the group to this permitted list.

➡ Note *Leaving this allowed list empty enables access from any IP address. If you really want to disable all network-based management access—which we STRONGLY recommend against—list only the loopback subnet 127.0.0.0/8 (doing so will force you to manage this device through the serial or virtual console).*

SNMP Access IP Addresses — SC-7

In this section, you have the ability to control from which IP addresses the BIG-IP system will accept SNMP connections.

1. ***How should the system control SNMP access?***

Choose how you want the system to control SNMP access. If you use SNMP to monitor or manage the BIG-IP system, you should choose Restrict access by source IP address and enter one or more IP addresses from which SNMP connections should be accepted.

- **Allow SNMP access only locally from this device (default)**

Select this option if you want to restrict SNMP access to internal communication within the BIG-IP system. This allows BIG-IP management plane local tools to work but forbids SNMP access from anywhere else.

- **Forbid all SNMP access**

Select this option if you do not want to allow SNMP access at all, even from the BIG-IP shell command line.

- **Allow SNMP access from IP addresses I specify**

Select this option if you want to restrict SNMP access by source IP address.

a. Which IP addresses should be allowed?

Type a list of IP addresses or subnets that should be permitted SNMP. Each address may specify a host or a subnet (meaning all the hosts on that subnet) using the form address/mask. Separate addresses by space characters.

In nearly all cases you should include **127.0.0.0/8** in the list so local SNMP tools will work.

Self IP Lockdown — AC-4, SC-7

In this section, you have the ability to choose a *self IP access policy* to permit some services (such as DNS, OSPF, HTTPS, etc.) to be accessed on BIG-IP self IP addresses.

 **Tip** *The BIG-IP Advanced Firewall Manager (AFM) module may also be used to control network access to BIG-IP management facilities. For more information consult the F5 BIG-IP Data Center Firewall Deployment Guide (<https://f5.com/solutions/deployment-guides/data-center-firewall-big-ip-v116-ltm>).*

1. What type of self IP access policy do you want to use?

Select the type of self IP access policy you want to use. By default on a new BIG-IP device, no services are permitted. Note that BIG-IP DNS (previously called GTM) will not work properly unless tcp:f5-iquery is permitted.

- **Do not change my current self IP access policy**
Select this option if you have already adjusted the permitted services on self IP addresses outside the NIST iApp, and you want to leave these changes intact.
- **Use the standard BIG-IP list (see SOL 17333)**
Select this option if you want to permit the standard list of services. See <https://support.f5.com/kb/en-us/solutions/public/17000/300/sol17333.html> for the list of the BIG-IP services allowed by default (called the **self-allow defaults** in the TMSH Reference guide). In most cases, the services on this list are sufficient.
- **Prevent access to any services on self IP addresses**
Select this option if you do not want to allow access to any services on BIG-IP self IP addresses. This is the factory setting of the BIG-IP when it ships.
- **Let me configure a custom set of services**
Select this option if you want to configure a custom subset of standard services and/or permit custom services to be accessible on all BIG-IP self IP addresses.

a. Which standard services to you want to allow?

Choose the standard services you want to allow. By default, all of the Standard services are in the **Selected** list. Use the remove arrow button (>>) to move services from the Selected list to the **Options** list. Services in the Options list are not allowed. Remember that BIG-IP DNS (GTM) will not work properly unless 'tcp:f5-iquery' is permitted.

b. Which other (non-standard) services do you want to allow?

If you have other, non-standard services you want to allow, first select the IP protocol from the list, and then type the port number. Click the **Add** button to include more non-standard services.

 **Warning** *After completing this iApp template, if/when you manually create new Self IP addresses on the BIG-IP system outside this iApp template, if you want to use your default policy (that is the standard set of services as in SOL17333 or the custom set of services you created), you must configure the **Port Lockdown** setting to **Allow Default** if using the web-based Configuration utility, or add **allow-service default** to the TMSH command **create /net self** command.*

NTP Configuration — AU-8(1,2)

In this section, you have the ability to specify the IP addresses of your primary and (if available) alternate NTP servers. A working NTP configuration is vital to BIG-IP management (and application) security.

1. What is the IP address or FQDN of the primary NTP server?

Type the IP or fully-qualified domain name of the primary NTP server.

2. What is the IP address or FQDN of the first alternate NTP server?

If you have another NTP server to add, type the first alternate server in this field. Alternate servers are optional but recommended. Once you have entered your first alternate server, if you have additional servers to add, press the Tab key or simply click any other field. The following question appears.

a. Which additional NTP servers do you want to include?

Once you enter the first alternate server, this question appears asking for additional NTP servers. If you have more servers you want to add to the list, type the IP address or FQDN in the box. Click the **Add** button to include more servers. Use the Remove button (x) if you accidentally include an extra row.

Auditing — AU-2, CM-5

In this section, you have the ability to configure audit logging of management actions. Typically you enable TMSH and MCP audit logs. Only if you do not have a syslog server to accept log messages (see *Syslog Configuration — AU-8, AU-9(2), AU-12(2)* on page 16) should you consider disabling logs to save BIG-IP disk space.

1. Do you want to enable TMSH audit logs?

Choose whether or not you want to enable TMSH audit logs. TMSH audit logging is an optional, recommended feature that logs messages whenever a BIG-IP system TMSH command is issued. The BIG-IP system logs the messages for these auditing events via syslog and in the file `/var/log/ltn`.

- **No, disable TMSH audit logs**
Select this option if you do not want to enable TMSH audit logs.
- **Yes, enable TMSH audit logs (recommended)**
Select this recommended option to enable TMSH audit logs.

2. Do you want to enable MCP audit logs?

Choose whether or not you want to enable MCP audit logs. MCP audit logging, similar to TMSH logging, is an optional, recommended 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) using any interface, including TMSH, management GUI, iControl, or SNMP. The BIG-IP system logs the messages for these auditing events via syslog and in the file `/var/log/ltn`.

- **No, disable MCP audit logs**
Select this option if you do not want to enable MCP audit logs.
- **Yes, enable level-1 basic MCP audit logs (recommended)**
Select this recommended option to enable MCP audit logs. This option logs user-initiated configuration changes.
- **Yes, enable level-2 verbose MCP audit logs**
Select this option if you want to enable verbose MCP audit logs. Level-2 logs user-initiated changes and configuration loads. This can be useful for additional troubleshooting information, however it could result in large log files and slower performance.
- **Yes, enable level-3 debug MCP audit logs (rarely needed)**
Select this option if you want to enable debug-level logging. This level logs all user- and system-initiated configuration changes.

 **Warning** *This level of logging should only be used on advice from F5 technical support because it has a severe performance impact.*

Syslog Configuration — AU-8, AU-9(2), AU-12(2)

In this section, you have the ability to enable the use of ISO-format dates in log messages (generally required for SP-800-53r4 compliance). You may also add syslog servers to receive log messages. Any syslog servers you specify using the NIST iApp template receives messages in parallel with any syslog servers you may have configured outside the iApp.

1. Should log messages use ISO date format?

Choose whether you want log messages to use ISO date format (YYYY-MM-DDThh:mm:ssZ) or use the BIG-IP date format inherited from older TMOS versions but no longer recommended. If you are unsure, choose the ISO date format.

- **Yes, log messages should use ISO date format (recommended)**
Select this recommended option to use the ISO date format in log messages.
- **No, use the obsolete BIG-IP date format**
Select this option only if you have a reason to continue using the old BIG-IP data format that is no longer recommended.

2. Do you want to add syslog servers?

Choose whether you want to add syslog servers to the configuration, or if the system uses only syslog servers configured outside the iApp template. Adding syslog servers using the iApp template does not replace or remove existing syslog servers.

- **No, the system uses syslog servers configured outside this iApp**
Select this option if you do not want to add any syslog using the iApp template.
- **Yes, use this iApp to add syslog servers**
Select this option to add syslog servers to the iApp configuration. You must specify the servers in the following question.
 - a. *Which syslog servers do you want to add?*
Specify the syslog servers you want to add.
In the **Server** field, type the IP address or FQDN of the syslog server.
In the **Port** field, change the default port (514) if necessary.
In the **BIG-IP source IP** field, type the IP address from which the BIG-IP should send messages to each syslog server (the IP must be assigned to the management port or a self IP), or leave the wildcard (*) to let the BIG-IP system choose.

Finished

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

If you want to remove the Application Service created with the NIST iApp template, consider using the option to revert to pre-iApp configuration documented in the initial section of the iApp template.

Archived

NIST SP-800-53r4 Security Controls Review

The following is a summary of security controls from Appendix F of NIST SP-800-53r and how they map to BIG-IP capabilities.

Access Control Family

AC-1 - Access Control Policy and Procedures

This control would be implemented outside of BIG-IP.

AC-2 - Account Management

The lifecycle of user accounts and roles associated with them is the focus of this control. The iApp enables configuration of authentication sources (local, LDAP, RADIUS, etc.) as well as inactivity timeout and remote role assignment in support of this control. Also see SC-10, IA-2.

AC-3 - Access Enforcement

Access to the BIG-IP must be made through approved means. Related to AC-2, remote authentication and role determination help satisfy this control.

AC-4 - Information Flow Enforcement

This control addresses information flow within and between systems. The iApp supports this control mainly by enforcing boundary protections; see SC-7.

AC-5 - Separation of Duties

Encourages use of role-based access control (RBAC). BIG-IP supports a variety of different security roles. Users may be assigned roles on the BIG-IP or by reference to a central authority (for example, mapping via an LDAP attribute).

AC-6 - Least Privilege

BIG-IP supports this control using role-based access control, Administrative Partitions, and auditing. The iApp does not include management of Administrative Partitions. Also see AU-9, CM-5.

AC-7 - Unsuccessful Login Attempts

To protect account credentials against brute-force attacks you should lock accounts after a certain number of unsuccessful login attempts. The maximum count is configurable in the iApp template.

AC-8 - System Use Notification

You should warn users about policies governing their access to the system. The iApp helps you configure a suitable “banner” message for display at logon.

AC-9 - Previous Login (Access) Notification

Upon logon, users should be notified of their last successful logon time plus additional logon history. BIG-IP displays the last logon time to SSH and console users but not Management GUI users. Additional logon history information is available via TMSH and shell only.

AC-10 - Concurrent Session Control

Limit the number of concurrent sessions by user or account type. BIG-IP can limit the total number of concurrent Management GUI users (though not specific users or account types) so the iApp lets you adjust that number. No equivalent limits can be placed on command-line or SNMP access.

AC-11 - Session Locking

Session locking differs from automatic logout due to idleness because the user's session state is maintained. BIG-IP does not have this feature. A screen- or client-locking feature on the user's workstation could help meet this control.

AC-12 - Session Termination

The BIG-IP Management GUI displays a suitable message to meet this control, but neither SSH nor console access support it.

AC-13 - Supervision and Review

This control appeared in earlier revisions of SP-800-53 but has been withdrawn.

AC-14 - Permitted Actions without Identification or Authentication

This control addresses actions, if any, available without user authentication or authorization. The BIG-IP does not offer any services to unauthenticated/unauthorized users.

AC-15 - Automated Marking

This control appeared in earlier revisions of SP-800-53 but has been withdrawn.

AC-16 - Security Attributes

This control relates to associating security attributes to information in storage, in process, and in transmission. The NIST iApp template does not expose any configuration items related to this.

AC-17 - Remote Access

Addressing this control will go beyond the BIG-IP. However, all remote management access to the BIG-IP uses encrypted transport (AC-17(2)) except SNMP. Also see SC-7 for boundary protection which also controls remote access.

AC-18 - Wireless Access

There are no BIG-IP configuration options specifically related to wireless networking. This control would mainly be addressed outside BIG-IP and by compliance to SC-7.

AC-19 - Access Control for Mobile Devices

There are no BIG-IP configuration options specifically related to mobile devices. This control would mainly be addressed outside BIG-IP and by compliance to AC-3 and SC-7.

AC-20 - Use of External Information Systems

This control relates to communications with systems in other administrative domains. BIG-IP management only operates in a single administrative domain so no BIG-IP configuration options are responsive.

AC-21 - User-Based Collaboration and Information Sharing

This control would be implemented outside of BIG-IP.

AC-22 - Publicly Accessible Content

This control would be implemented outside of BIG-IP.

AC-23 - Data Mining Protection

This control would be implemented outside of BIG-IP.

AC-24 - Access Control Decisions

This control would be implemented outside of BIG-IP.

AC-25 - Reference Monitor

This control concerns the incorporation of the “reference monitor” concept into system design and implementation. The internal architecture of BIG-IP is beyond the scope of the NIST iApp template.

Awareness and Training

None of the controls (AT-*nn*) in this section are relevant to BIG-IP or the NIST iApp template.

Audit and Accountability

AU-1 - Audit and Accountability Policy and Procedures

This control would be implemented outside of BIG-IP.

AU-2 - Audit Events

The iApp lets you activate audit event recording for changes made through TMSH and through MCPD (the latter records changes initiated via any user interface).

AU-3 - Content of Audit Records

The contents of BIG-IP audit records are basically fixed.

AU-4 - Audit Storage Capacity

Space for storing audit records (logs) on BIG-IP is not directly configurable, but you should send audit records to a remote server (see AU-9) and apply this control that context.

AU-5 - Response to Audit Processing Failures

There are no BIG-IP configuration options specifically related to this control.

AU-6 - Audit Review, Analysis, and Reporting

This control would be implemented outside of BIG-IP.

AU-7 - Audit Reduction and Report Generation

This control would be implemented outside of BIG-IP.

AU-8 - Time Stamps

To meet this control you may configure compliant (ISO) time stamps for audit messages (also see AU-12) and configure NTP server(s) as sources of accurate time (AU-8(1), AU-8(2)).

AU-9 - Protection of Audit Information

User roles (AC-6) control access to audit information on BIG-IP. You should send audit records to a remote server (AU-9(2)) and apply this control in that context. The NIST iApp lets you configure remote syslog servers.

AU-10 - Non-Repudiation

There are no BIG-IP configuration options specifically related to this control.

AU-11 - Audit Record Retention

BIG-IP Audit record log rollover is not directly configurable. You should send audit records to a remote server and apply this control in that context (see AU-9).

AU-12 - Audit Generation

This control would mostly be implemented outside BIG-IP. You may configure compliant (ISO) timestamps for audit messages (AU-12(2), see AU-8).

AU-13 - Monitoring for Information Disclosure

This control would be implemented outside of BIG-IP.

AU-14 - Session Audit

BIG-IP does not provide the capability envisioned by this control. A portion of this information could be selected from the audit message stream (see AU-2, AU-12).

AU-15 - Alternate Audit Capability

The BIG-IP retains copies of audit messages sent to remote servers for a few days, typically (see AU-4). An alternate procedure to retrieve audit data from BIG-IP could be defined in case a remote audit log server is unavailable or damaged.

AU-16 - Cross-Organizational Auditing

This control would be implemented outside of BIG-IP.

CA Family of Controls

These controls would be implemented outside of BIG-IP.

CM-1 - Configuration Management Policy and Procedures

These controls would be implemented outside of BIG-IP.

CM-2 - Baseline Configuration

BIG-IP UCS and SCF files may furnish data required to implement these controls. f5 Enterprise Manager and BIG-IQ products may also be utilized.

CM-5 - Access Restrictions for Change

BIG-IP RBAC and auditing features support CM-5(1). The NIST iApp helps you configure those features. The BIG-IP supports signature verification for TMOS software updates (CM-5(3)).

CM-7 - Least Functionality

The NIST iApp lets you adjust the services accessible on self IP addresses so you can constrain the functionality of BIG-IP in the network.

CM-8 - Information System Component Inventory

These controls would be implemented outside of BIG-IP. However, f5 Enterprise Manager or BIG-IQ products may be utilized in the implementation of these controls.

Contingency Planning

Most of the controls (CP-*nn*) in this family would be implemented outside of BIG-IP. Some exceptions are noted here.

CP-7 - Alternate Processing Site

BIG-IP supports configuration synchronization and functional failover device groups, as well as global traffic management (GTM), so f5 customers can build highly-reliable systems within and among different processing sites (“data centers”).

CP-9 - Information System Backup

BIG-IP typically does not store user data and generally the device configuration is all that must be backed up to enable service recovery in the event of a failure. Logs may be backed up through remote syslog. Enterprise Manager or BIG-IQ may be used to automate backup of BIG-IP device configuration and historical statistical data. The NIST iApp only helps you configure remote syslog.

CP-10 - Information System Recovery and Reconstitution

You may recover BIG-IP automatically in certain high-availability scenarios, by hand, or using f5 Enterprise Manager or BIG-IQ products. The NIST iApp does include any relevant options.

Identification and Authentication

Most of the controls (IA-*nn*) in this family would be implemented outside of BIG-IP. Important exceptions are noted here.

IA-2 - Identification and Authentication (Organizational Users)

BIG-IP supports user authentication to local or external directories using single- or multi-factor credentials. The NIST iApp lets you configure external authentication/directory services and parameters. The only way to disable BIG-IP's shared management user accounts is by configuring “Appliance Mode” but the NIST iApp template does not address that feature.

IA-3 Device Identification and Authentication

The NIST iApp helps you configure secure access to external authentication/directory services using TLS/SSL or shared-secret schemes for mutual authentication.

IA-4 - Identifier Management

These controls would be implemented outside of BIG-IP.

IA-5 - Authenticator Management

The NIST iApp lets you configure password policy for local authentication as well as security for authentication data used with external authentication/directory services.

Incident Response

These controls would be implemented outside of BIG-IP.

Maintenance

These controls would be implemented outside of BIG-IP.

Media Protection

These controls would be implemented outside of BIG-IP.

Physical and Environmental Protection

These controls would be implemented outside of BIG-IP.

Planning

These controls would be implemented outside of BIG-IP.

Personnel Security

These controls would be implemented outside of BIG-IP.

Risk Assessment Policy and Procedures

These controls would be implemented outside of BIG-IP.

System and Services Acquisition

These controls would be implemented outside of BIG-IP.

System and Communications Protection

Many of the controls (SC-*nn*) in this family would be implemented outside of BIG-IP. Important exceptions are noted here.

SC-5 - Denial of Service Protection

BIG-IP is hardened against certain Denial of Service attacks but the NIST iApp only lets you configure the failed-login retry limit. Note that the NIST iApp template relates to the management functions of the BIG-IP. Very extensive and powerful controls outside the NIST iApp are applicable to application traffic handled by BIG-IP.

SC-7 - Boundary Protection

The NIST iApp lets you manage the IP subnets from which BIG-IP management may be accessed as well as services accessible on self IP addresses.

SC-10 - Network Disconnect

The NIST iApp exposes several timeout settings for access to the system.

SC-17 - Public Key Infrastructure Certificates

The NIST iApp does not manage TLS/SSL PKI certificates or cryptographic material as such. However, you can select the appropriate certificates and keys for single-ended and mutual authentication of connections to external authentication/directory services.

SC-21 - Secure Name/Address Resolution Service

As of this writing the BIG-IP management plane does not offer support for DNSsec which the NIST iApp template can access.

System and Information Integrity

These controls would be implemented outside of BIG-IP.

Appendix: User roles

This appendix contains a list and description of the available BIG-IP user roles.

Role	Description
Acceleration Policy Editor	This role allows users to view, create, modify, and delete all BIG-IP Application Acceleration Manager policy objects in all administrative partitions. Users can also view, create, update, and delete Application Acceleration Manager profiles.
Administrator	This role grants users complete access to all objects on the system. These users can change their own passwords and cannot have any other user role on the system. Users with the Administrator role have access to all partitions on the system, and this partition access cannot be changed.
Application Editor	This role grants users permission to modify nodes, pools, pool members, and monitors. These users can view all objects on the system and change their own passwords.
Auditor	This role grants users permission to view all configuration data on the system, including logs and archives. Users with this role cannot create, modify, or delete any data, nor can they view SSL keys or user passwords. Users with the Auditor role have access to all partitions on the system, and this partition access cannot be changed.
Certificate Manager	This role grants users permission to manage device certificates and keys, as well as perform Federal Information Processing Standard (FIPS) operations.
Firewall Manager	This role allows users complete access to all firewall rules and supporting objects, including rules in all contexts, address lists, port lists, and 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; and DoS Device Configuration (the L2-L4 DoS protection configuration). Firewall Managers may be granted access on all partitions or a single partition. Since global and management port rules are defined in Common, only Firewall Managers with rights on Common are allowed to modify global and management port rules. Firewall Managers have no create, update, or delete rights to any other objects, but otherwise have the same read access as the Manager role. Notably, the Firewall Manager role has no permission to create, update, or delete non-network firewall configuration, including Application Security or Protocol Security policies.
Fraud Protection Manager	This role grants users permission to configure the BIG-IP Fraud Protection Service (FPS) module. This is only available (and visible) if you are using 11.6 or later.
iRule Manager	This role grants users permission to create, modify, and delete iRules. Users with this role cannot affect the way that an iRule is deployed. A user with this role can be assigned universal access to administrative partitions.
Guest	This role grants users permission to view all objects on the system except for sensitive data such as logs and archives. Users with this role can change their own passwords.
Manager	This role grants users permission to create, modify, and delete virtual servers, pools, pool members, nodes, custom profiles, custom monitors, and iRules. These users can view all objects on the system and change their own passwords.
Operator	This role grants users permission to enable or disable nodes and pool members. These users can view all objects and change their own passwords.
Resource Administrator	This role grants users complete access to all partitioned and non-partitioned objects on the system, except user account objects. In addition, accounts with the Resource Administrator role can change their own passwords. Users with the Resource Administrator role have access to all partitions on the system, and this partition access cannot be changed.
User Manager	<p>A user with a User Manager role on all partitions (that is, with universal access) can manage user accounts in these ways:</p> <ul style="list-style-type: none"> - 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. <p>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.</p>
Web Application Security Administrator	This role grants users access to BIG-IP Application Security Manager security policy objects. These users have read-only permission for these profile types: HTTP, FTP, and SMTP. These users have no access to other LTM objects, nor to any TMOS objects. They can, however, change their own passwords. With respect to security policy objects, this role is similar to the Administrator role. You can assign this role only when the BIG-IP system includes the Application Security Manager module. Users with this role have access to all partitions on the system, and this partition access cannot be changed.
Web Application Security Editor	This role grants users permission to view and configure most parts of Application Security Manager. Users with this role have no access to other BIG-IP objects. They can, however, change their own passwords. You can assign this role only when the BIG-IP system includes the Application Security Manager module.

Document Revision History

Version	Description	Date
1.0	New deployment guide to accompany the updated NIST iApp template	11-12-2015
1.1	Updated the guide for RC-4 of the iApp template. This revision adds support for BIG-IP v11.5.3. The main difference for v11.5.3 is the "Fraud Protection Manager" role was not available in 11.5.3, and is only present in v11.6 and later. Also added the iRule Manager role that was missing in previous versions of the iApp, and clarified the answers and inline help for the MCPD audit log section.	12-02-2015
1.2	Clarified the description in the Remote Roles section on <i>page 11</i> to include the numeric values that indicate the appropriate BIG-IP role.	12-08-2015
1.3	<ul style="list-style-type: none"> - Added a new question to the iApp template if you specified LDAP as your authentication method asking if the directory user objects include group-membership attributes (like memberOf). - Added All as an option for remote-role partition access. 	12-16-2015
1.4	Updated the guide for RC-5 of the iApp template, now available on downloads.f5.com in the RELEASE_CANDIDATE directory. There were no changes to the iApp template from RC-4, but it puts this iApp on the path to full F5 support.	10-18-2016
1.5	<p>Updated the guide for RC-5 of the iApp template, now available on downloads.f5.com in the RELEASE_CANDIDATE directory. RC-5 contains the following changes to the iApp template:</p> <ul style="list-style-type: none"> - All customer secrets/passwords in the iApp template are now securely stored. Previously, although secrets were stored in Secure Vault for use, some may have been stored in cleartext in the iApp reconfiguration data. - Added support for BIG-IP versions 12.1 and 12.1.1. - Made error messages produced by the template easier to understand. - If using RADIUS authentication, you are now limited a maximum of 10 servers. Previously there was no limit. - The source-IP option on additional syslog servers is honored in this version, previously this field was ignored. 	12-15-2016
1.6	Updated the guide for the fully supported v1.0.0 of the iApp template, now available on downloads.f5.com. This version of the template include support for BIG-IP v12.1.2, and is now a fully supported release. Corrected an issue in the iApp what would result in a failure when configuring custom ports for Self IP port lockdown.	02-08-2017
1.7	Updated the guide for v1.0.1rc1 of the iApp template, now available on downloads.f5.com in the Release-Candidates directory. This maintenance release contains no visible changes to this guide or the iApp presentation, but was released to correct an issue in the iApp what would result in a failure when configuring custom ports for Self IP port lockdown.	10-12-2017
1.8	Updated the guide for v1.0.1rc2 of the iApp template, now available on downloads.f5.com in the Release-Candidates directory. This maintenance release contains no visible changes to this guide or the iApp presentation, but was released to correct an issue where the iApp would fail with "unknown property" when adding additional servers.	5-10-2018
1.9	Updated the guide for v1.0.1rc3 of the iApp template, now available on downloads.f5.com in the Release-Candidates directory. This maintenance release contains no visible changes to this guide or the iApp presentation, but was released to correct an issue where the iApp would incorrectly detect Appliance Mode.	06-07-2018
2.0	Updated the guide for v1.0.1rc4 of the iApp template, now available on downloads.f5.com in the Release-Candidates directory. This maintenance release contains no visible changes to this guide or the iApp presentation, but was released to correct an issue where the iApp would remove line breaks from user-edited login banners.	07-26-2018

2.1	Updated the guide for v1.0.1rc4 of the iApp template, now available on downloads.f5.com in the Release-Candidates directory. RC-5 contains the following changes to the iApp template: <ul style="list-style-type: none">- The iApp template now lets you define roles for up to ten groups of users.- Note that if you are using TMOS version 14.0.0, the password minimum length must be in range 6-255.	01-31-2019
-----	--	------------

Archived

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

