

UNCLASSIFIED



F5 BIG-IP STIG REVISION HISTORY

30 January 2025

Developed by DISA for the DOD

UNCLASSIFIED

REVISION HISTORY		
Document Revised	Description of Change	Release Date
<ul style="list-style-type: none"> - F5 BIG-IP Access Policy Manager, V2R3 - F5 BIG-IP Advanced Firewall Manager, V2R1 - F5 BIG-IP Application Security Manager, V2R1 - F5 BIG-IP Device Management, V2R3 - F5 BIG-IP Local Traffic Manager, V2R3 	<ul style="list-style-type: none"> - Rule numbers updated throughout due to changes in content management system. <p>F5 BIG-IP Access Policy Manager, V2R4:</p> <ul style="list-style-type: none"> - F5BI-AP-999999 - Added requirement to sunset the STIG. <p>F5 BIG-IP Advanced Firewall Manager, V2R2:</p> <ul style="list-style-type: none"> - F5BI-AF-999999 - Added requirement to sunset the STIG. <p>F5 BIG-IP Application Security Manager, V2R2:</p> <ul style="list-style-type: none"> - F5BI-AS-999999 - Added requirement to sunset the STIG. <p>F5 BIG-IP Device Management, V2R4:</p> <ul style="list-style-type: none"> - F5BI-DM-999999 - Added requirement to sunset the STIG. <p>F5 BIG-IP Local Traffic Manager, V2R4:</p> <ul style="list-style-type: none"> - F5BI-LT-999999 - Added requirement to sunset the STIG. 	30 January 2025
<ul style="list-style-type: none"> - F5 BIG-IP Access Policy Manager, V2R2 	<p>F5 BIG-IP Access Policy Manager, V2R3:</p> <ul style="list-style-type: none"> - F5BI-AP-000023 - Updated with new procedure for TMOS UI banner. - F5BI-AP-000230 - Updated "Maximum Session Timeout" value to 8 hours or less instead of 24 hours. - F5BI-AP-000231 - Added requirement to deny access when revocation data is unavailable using OCSP. - F5BI-AP-000232 - Added requirement to configure OCSP in the Access Policies to ensure revoked user credentials are prohibited from establishing an allowed session. - F5BI-AP-000233 - Added requirement to configure OCSP in the Access Policies to ensure revoked machine credentials are prohibited from establishing an allowed session. - F5BI-AP-000234 - Added requirement to not use the On-Demand Cert Auth VPE agent as part of the APM Policy Profiles. 	29 January 2024

REVISION HISTORY		
Document Revised	Description of Change	Release Date
	<ul style="list-style-type: none"> - F5BI-AP-000235 - Added requirement to configure APM Access Policies that grant access to web application resources to allow only client certificates that have the User Persona Name (UPN) value in the User Persona Client Certificates. - F5BI-AP-000236 - Added requirement to limit authenticated client sessions to initial session source IP. - F5BI-AP-000239 - Added requirement to set the "Max In Progress Sessions per Client IP" value to 10 or less. - F5BI-AP-000240 - Added requirement to explicitly configure assigned resources with an authorization list for all resources. - F5BI-AP-000241 - Added requirement. If the Access Profile Type is LTM+APM and it is not using any connectivity resources (such as Network Access, Portal Access, etc.) in the VPE, the F5 BIG-IP appliance must be configured to enable the HTTP Only flag. - F5BI-AP-000242 - Added requirement to enable the "Secure" cookie flag. - F5BI-AP-000243 - Added requirement to disable the "Persistent" cookie flag. - Updated STIG title to remove 11.x. 	
- F5 BIG-IP Device Management, V2R2	F5 BIG-IP Device Management, V2R3: <ul style="list-style-type: none"> - F5BI-DM-000163 - Updated requirement to restrict a consistent inbound IP for the entire management session. - F5BI-DM-000291 - Added requirement to configure DOD Consent Banner for SSH. - Updated STIG title to remove 11.x. 	
- F5 BIG-IP Local Traffic Manager, V2R2	F5 BIG-IP Local Traffic Manager, V2R3: <ul style="list-style-type: none"> - F5BI-LT-000093 - Made grammatical updates in check and fix. - F5BI-LT-000213 - Updated entire requirement with new procedure. - F5BI-LT-000310 - Removed requirement. Duplicate of the APM requirement. - F5BI-LT-000317 - Added requirement to configure OCSP to ensure revoked credentials 	

REVISION HISTORY		
Document Revised	Description of Change	Release Date
<p>- F5 BIG-IP Advanced Firewall Manager, V1R1</p> <p>- F5 BIG-IP Application Security Manager, V1R1</p>	<p>are prohibited from establishing an allowed session.</p> <p>- Updated STIG title to remove 11.x.</p> <p>F5 BIG-IP Advanced Firewall Manager, V2R1:</p> <p>- DISA migrated this STIG to a new content management system. The new content management system renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version number to V2R1.</p> <p>- Updated STIG title to remove 11.x.</p> <p>F5 BIG-IP Application Security Manager, V2R1:</p> <p>- DISA migrated this STIG to a new content management system. The new content management system renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version number to V2R1.</p> <p>- Updated STIG title to remove 11.x.</p>	
<p>- F5 BIG-IP Access Policy Manager, V2R1</p> <p>- F5 BIG-IP Device Management, V2R1</p>	<p>F5 BIG-IP Access Policy Manager, V2R2:</p> <p>- F5BI-AP-000191 - Updated rule title, check, and fix; removed "After a fixed period of time," which will be a separate requirement.</p> <p>- F5BI-AP-000230 - Added a new requirement for Maximum Session Timeout.</p> <p>- Rule numbers updated due to changes in content management system.</p> <p>F5 BIG-IP Device Management, V2R2:</p> <p>- F5BI-DM-000007 - Removed from STIG. The system is unable to do a session lock. This is done at the management station level as with many other applications. The product is configured to terminate the session upon idle timeout.</p> <p>- F5BI-DM-000137 - Reworded all fields for clarity. Added CCI-000057 and CCI-000879 and upgraded to CAT I.</p> <p>- F5BI-DM-000163 - Removed idle timeout configuration settings because that is configured</p>	27 November 2023

REVISION HISTORY		
Document Revised	Description of Change	Release Date
- F5 BIG-IP Local Traffic Manager, V2R1	<p>in F5BI-DM-000137. Reworded requirement statement to address the remaining requirement IP restriction. Changed the CCI and parent SRG to match the topic of this requirement, which is DOS protection.</p> <ul style="list-style-type: none"> - Rule numbers updated due to changes in content management system. <p>F5 BIG-IP Local Traffic Manager, V2R2:</p> <ul style="list-style-type: none"> - F5BI-LT-000093 - Made minor updates to requirement wording. Combined with CCI-000057. - F5BI-LT-000141 - Removed requirement. This is a management station check and is not applicable to the application. - F5BI-LT-000191 - Updated rule title, check, and fix; removed “After a fixed period of time,” which will be a separate requirement. - F5BI-LT-000310 - Added a new requirement for Maximum Session Timeout Value of 24 hours or less. - Rule numbers updated due to changes in content management system. - Revision History format for multipart STIGs revised to ensure clarity in the versioning. 	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V2R1	<ul style="list-style-type: none"> - F5 BIG-IP Access Policy Manager STIG, V1R1 - F5 BIG-IP Device Management STIG, V1R7 	<p>- DISA migrated the F5 BIG-IP STIG to a new content management system. The new content management system renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version number to V2R1.</p> <p>Access Policy Manager:</p>	23 October 2020

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
	- F5 BIG-IP Local Traffic Manager, V1R4	<p>- F5BI-AP-000147 - Changed Parent SRG to SRG-NET-000517-ALG-000006, CCI-002361.</p> <p>- F5BI-AP-000151 - Changed Parent SRG to SRG-NET-000519-ALG-000008, CCI-002364.</p> <p>- F5BI-AP-000197, F5BI-AP-000199, F5BI-AP-000205, F5BI-AP-000207, F5BI-AP-000209 - Removed requirement; it is no longer in the parent SRG.</p> <p>Device Management:</p> <p>- F5BI-DM-000290 - Added a policy to APM stating if F5 is being used to authenticate users for web applications, the HTTP_Only flag must be set.</p> <p>Local Traffic Manager:</p> <p>- F5BI-LT-000139 - Changed Parent SRG to SRG-NET-000521-ALG-000002, CCI-001494.</p> <p>- F5BI-LT-000141 - Changed Parent SRG to SRG-NET-000514-ALG-000514, CCI-000057.</p> <p>- F5BI-LT-000143 - Changed Parent SRG to SRG-NET-000515-ALG-000515, CCI-000058.</p> <p>- F5BI-LT-000147 - Changed Parent SRG to SRG-NET-000517-ALG-000006, CCI-002361.</p> <p>- F5BI-LT-000151 - Changed Parent SRG to SRG-NET-000519-ALG-000008, CCI-002364.</p> <p>- F5BI-LT-000197, F5BI-LT-000199, F5BI-LT-000205, F5BI-LT-000207, F5BI-LT-000209 - Removed requirement; it is no longer in the parent SRG.</p> <p>The following STIGs were not updated this release:</p> <p>- F5 BIG-IP Advanced Firewall Manager, V1R1</p>	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- F5 BIG-IP Application Security Manager, V1R1	
V1R4	- F5 BIG-IP Local Traffic Manager, V1R3	Local Traffic Manager: - V-60273 - Rule title updated to reference 800-52 Revision 2, which has superseded Revision 1. - V-60319 - Removed from STIG and placed in DNM status. Application does not provide session lockout function. Current Fix does not address the requirement to lock the session. The following STIGs were not updated this release: - F5 BIG-IP Device Management STIG, V1R7 - F5 BIG-IP Access Policy Manager STIG, V1R1 - F5 BIG-IP Advanced Firewall Manager, V1R1 - F5 BIG-IP Application Security Manager, V1R1	24 July 2020
V1R7	- F5 BIG-IP Device Management STIG, V1R6	Device Management: - V-60091- Change check and fix procedures to require a Set the MaxClients = 10 (or less) to fix the mismatch with the actual requirement. The following STIGs were not updated this release: - F5 BIG-IP LTM STIG, V1R3 - F5 BIG-IP Access Policy Manager STIG, V1R1 - F5 BIG-IP Advanced Firewall Manager, V1R1 - F5 BIG-IP Application Security Manager, V1R1	24 January 2020
V1R6	- F5 BIG-IP Device Management STIG, V1R5	Device Management: - V-97729 - Added new requirement. - Updated overview for clarification. Local Traffic Manager:	25 October 2019

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
	- F5 BIG-IP LTM STIG, V1R2	<p>- V-60311 - Set a TCP profile 'idle-timeout' set to 600/900 seconds would be more accurate to meet the requirement.</p> <p>The following STIGs were not updated this release:</p> <ul style="list-style-type: none"> - F5 BIG-IP Access Policy Manager STIG, V1R1 - F5 BIG-IP Advanced Firewall Manager, V1R1 - F5 BIG-IP Application Security Manager, V1R1 	
V1R5	- F5 BIG-IP Device Management STIG, V1R4	<p>Device Management:</p> <ul style="list-style-type: none"> - F5BI-DM-000133 - Corrected Check Content; changed "Verify 'SSL' is configured..." to "Verify 'Encryption' is configured..." <p>The following STIGs were not updated this release:</p> <ul style="list-style-type: none"> - F5 BIG-IP LTM STIG, V1R2 - F5 BIG-IP Access Policy Manager STIG, V1R1 - F5 BIG-IP Advanced Firewall Manager, V1R1 - F5 BIG-IP Application Security Manager, V1R1 	28 July 2017
V1R4	- F5 BIG-IP Device Management STIG, V1R3	<p>Device Management:</p> <ul style="list-style-type: none"> - F5BI-DM-000007 - Changed requirement from 900 Seconds (15 minutes) to 600 seconds (10 minutes) to coincide with the setting in F5BI-DM-000137. <p>The following STIGs were not updated this release:</p> <ul style="list-style-type: none"> - F5 BIG-IP LTM STIG, V1R2 - F5 BIG-IP Access Policy Manager STIG, V1R1 - F5 BIG-IP Advanced Firewall Manager, V1R1 - F5 BIG-IP Application Security Manager, V1R1 	28 April 2017

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V1R3	<ul style="list-style-type: none"> - F5 BIG-IP Device Management STIG, V1R2 - F5 Big-IP LTM STIG, V1R1 - F5 BIG-IP Device Management STIG Overview 	<p>Device Management:</p> <ul style="list-style-type: none"> - F5BI-DM-000041 - Removed check from STIG as inherently meets. <p>Local Traffic Manager:</p> <ul style="list-style-type: none"> - F5BI-LT-000203 - Updated Check Content and Fix Text Sections. - F5BI-LT-000057, F5BI-LT-000059, F5BI-LT-000061, F5BI-LT-000063, F5BI-LT-000065; Updated Vulnerability Discussion, Check Content, and Fix Text sections. <p>Overview:</p> <ul style="list-style-type: none"> - Added Section 1.8 Product Approval Disclaimer. <p>The following STIGs were not updated this release:</p> <ul style="list-style-type: none"> - F5 BIG-IP Access Policy Manager STIG, V1R1 - F5 BIG-IP Advanced Firewall Manager, V1R1 - F5 BIG-IP Application Security Manager, V1R1 	28 October 2016
V1R2	<ul style="list-style-type: none"> - F5 BIG-IP Device Management STIG, V1R1 - F5 BIG-IP Device Management STIG Overview 	<p>Device Management:</p> <ul style="list-style-type: none"> - STIG V-60155 updated Rule Title, Check Content, and Fix Text to require only eight (8) characters be changed instead of 15 when changing a password. - STIG V-60137 updated Rule Title, Check Content, and Fix Text to require the use of NIAP evaluated cryptographic mechanisms. <p>Overview:</p> <ul style="list-style-type: none"> - Overview updated Other Considerations Section. <p>The following STIGs were not updated this release:</p> <ul style="list-style-type: none"> - F5 BIG-IP Access Policy Manager STIG, V1R1 - F5 BIG-IP Advanced Firewall Manager, V1R1 	23 October 2015

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- F5 BIG-IP Application Security Manager, V1R1 - F5 BIG-IP LTM STIG, V1R1	
V1R1	- NA	- Initial Release.	29 May 2015