

# HP Access Control – Load Balancer Security in HP AC 16.7 and newer

#### **Table of Contents**

Overview	2
Citrix NetScaler	3
Certificate	3
Citrix NetScaler Service Groups	3
Session Persistence	6
F5 Load Balancers	7
Importing the HP AC Certificate to the F5	7
F5- Client-IP HTTP Profile	8
F5- X-Forwarded-For HTTP Client Profile	9
F5 - SSL Client and Server Certificate Profiles	9
Session Persistence	12

# **Overview**

In an ongoing effort to increase security, HP Access Control (HP AC) version 16.7 and newer will no longer support a passthrough Network Load Balancer (NLB) configuration. HP AC now ensures that the IP address of the requestor matches the IP address in the request. For jobs that go through an NLB, a header is inserted so that the IP address of the original requesting client is preserved.

The order in which HP AC will resolve a requesting client's IP address is as follows:

- 1. HP AC will first look for an arbitrary HTTP Header named CLIENT-IP.
- 2. If Client-IP is not present, then the first IP address in the HTTP Header X-Forwarded-For.
- 3. If XFF is not present, then it will use the REMOTE\_ADDR (which will be IP address the packet came from)

For this reason, HP AC Load balancer configurations will require, at a minimum, Client-IP or X-Forward-For configurations for the HTTPS virtual servers.

Additionally, because the packets are encrypted, the load balancer will need to decrypt the data, insert the appropriate header information, then re-encrypt it as it passes it on to the HP AC nodes. Therefore, the certificate used for HP AC, both the private and Public key certificate, needs to be imported into the load balancer and assigned to the HTTPS virtual server.

Below is an example of what the HTTP header would appear with Client -IP and or X-Forward-For enabled.



**Note:** The sections below are intended to provide information on where to apply the settings discussed above for both the F5 and NetScaler. Any changes made to production environments should be done by the customer with the approval of the appropriate IT administrators.

# **Citrix NetScaler**

## Certificate

To allow the load balancer to decrypt and re-encrypt traffic, the certificate used by HP AC must be applied to the SSL Service Group.

First import the HP AC certificate (root CA) into the Citrix NetScaler

**Note:** this document assumes administrators already have the .PFX containing the public and private key along with the associated password.

- 1. Navigate to **Traffic Management > SSL > Tools**
- 2. Select Import PKCS#12 from the Tools menu

<b>Q</b> Search in Menu		Traffic Management / SSL	
System	>	SSL	C
AppExpert	>		
Traffic Management	~	Getting Started	▼ Tools
Load Balancing	>	Server Certificate Wizard	Create Diffie-Hellman (DH) key
Priority Load Balancing	<u> </u>	Intermediate-CA Certificate Wizard	Export PKCS#12
Content Switching	<u> </u>	Root-CA Certificate Wizard Create and Install a Server Test Certificate	Manage Certificates / Keys / CSRs Start SSL certificate, key file synchronization for HA
Cache Redirection	() >	Install Certificate (HSM)	Start SSL certificate, key file synchronization for
DNS	>	CRE Management	OpenSSL interface
GSLB	>		
	$\sim$	Policy Manager SSL Policy Manager	Settings Change advanced SSL settings
Certificates	>		

## Citrix NetScaler Service Groups

For the NetScaler, the Client-IP setting is made in the Service Group settings page

1. Navigate to Traffic Management – Service Groups

Citrix NetSca	aler VPX (10	00)				HA Status Not configured	Partition default	~
Dashboard	Configuration	Reporting	Documentation	Down	loads			÷
<b>Q</b> Search in Menu	т	raffic Management / Lo	oad Balancing / Service	Groups				
System AppExpert		ervice Group	DS					
Traffic Management	~	Add Edit De	elete Manage Men	nbers	atistics	ename		
Load Balancing Virtual Servers	~	No action Service G	roup Name	<b>^</b>	State	Effective State	Protocol	Ma
Services		HPAC_HT	ГР		ENABLED	• DOWN	HTTP	
Service Groups		HPAC_SSL			ENABLED	• UP	SSL	
Monitors		HPAC_TCF	,		ENABLED	DOWN	TCP	
Metric Tables		CJZ_SG_N	IFPSECURE_HTTPS_PROTE	ECTION	ENABLED	DOWN	SSL	
Servers		CJZ_SG_N	IFPSECURE_LMS		ENABLED	PARTIAL-UP	TCP	
Servers		CJZ_SG_N	IFPSECURE_TCP		ENABLED	● UP	TCP	

#### 2. Edit Settings

	Dashboard	Configuration	Reporting	Documentation	Down	loads				٠	٥
G	Load Bal	ancing Servi	ce Group								
	Basic Settings							/	Help		
	Name Hi Protocol 53 State EN	PAC_SSL SL NABLED		Cache Type Cacheable Health Monitoring		SERVER NO YES			Advance	d Settings	
	Effective State  Traffic Domain Comment	UP		AppFlow Logging Monitoring Connection Number of Active Conn AutoScale Mode	Close Bit ections	ENABLED NONE 0 DISABLED			+ The	esholds & Tim	eouts
	Service Group	Members		ANIIOGER MONT		ersnoe e			+ 554	Profile	
	2 Service Group	Members						>	+ Mo	nitors	
	Settings						/	×	+ 554	Parameters	
Ľ	SureConnect Surge Protection	OFF		Use Client IP N Client Keep-alive N	0						

3. Select the Client-IP Check box and add "Client-IP" in the Header section

To use the X-Forward Setting, use "X-Forwarded-For" in the header section

Settings	×	
El SureConnect ()	Settings	>
Use Proxy Port	E SureConnect ()	
Down State Flush	Surge Protection	
Use Client IP	W Use Proxy Port	
Clerit Keep-alive	Own State Flush	
E 10P Buffering	Use Clent IP	
HTTP Compression	Cient Keep-alve	
Ciert IP	E TCP Buffering	
Heiader	HTTP Compression	
Circle all	B Client P	
Cierc-iP	Header	
_	V. forward for	
bik .	(independent)	
	OK	

From the steps above, you will be in the SSL Service Group.

4. On the Basic Settings Page, Select the Plus sign next to Certificates on the Right-hand tool bar

Settings		/ ×	+ Profiles
SureConnect Surge Protection OFF Use Proxy Port YES Down State Flush ENABLED	Use Client IP NO Client Keep-alive NO TCP Buffering NO HTTP Compression NO Client IP ENABLED Header Client-IP AutoScale Mode DISABLED		+ SSL Profile + Monitors + SSL Parameters + Certificate
SSL Ciphers		/ ×	r certificate

5. Select the arrow to the right of Client Certificate

Certificate	×
No CA Certificates	>
No Client Certificate	$\rightarrow$

6. A pop up will appear for Client Certificate binding- Select Add Binding then select the arrow on the following pop-up



7. The Client Certificate list appears- Locate and select the correct certificate, then press the Select button in the upper left

Service	Group Client Certificates Binding	g / Client Certificate Binding	/ Client Certificates		
Clien	t Certificates				×
Select	Install Updat	e Delete Sel	ect Action 🗸	s	earch 🗸
	Name	Common Name	Issuer Name	Days to Expire	Statu
0	ns-sftrust-certificate	SFTrust default PJSSIL	SFTrust default PJSSIL	5338	Valid
0	ns-server-certificate	default NQLSUN	default NQLSUN	4541	Valid
۲	NETSCALER.EOMHB.SHARED	NETSCALER.EOMHB.SHARED	LRSRICA1	3200	Valid

#### **Session Persistence**

Best practice in HP AC is ensuring the load balancer virtual server's session persistence is set with a value high enough to prevent conflicts with end user during an HP AC associated interaction.

For NetScaler, the settings are completed with Persistency Groups

- 1. Navigate to Traffic Management-Persistency Groups
- 2. Select Add
- 3. Provide a name for the group
- 4. In Persistence select **SOURCEIP**
- 5. Set the Time-Out to a minimum of **300 (seconds)**
- 6. In the Virtual Servers box, add all of the HP AC virtual servers
- 7. Select Create in the bottom left

Group Name*	_			
HPAC_ Persistencey_Group	0			
Persistence*	_			
SOURCEIP	~ <b>?</b>			
Pv4 Netmask				
255 . 255 . 255 . 255				
Pv6 Mask Length				
128				
lime-out				
	0			
300	<u> </u>			
300 Backup Persistence*				
300 Backup Persistence* NONE	~			
300 Backup Persistence* NONE Use vServer Persistence*	~			
300 Backup Persistence* NONE Use vServer Persistence* Virtual Server Name*	~			
300 Backup Persistence* NONE Use vServer Persistence* Virtual Server Name* Available (55)	Select All	Configured (4)	Remove All	
300 Backup Persistence* NONE Use vServer Persistence* Virtual Server Name* Available (55) VS_WBLANCHET_VPSA_LMS	Select All	Configured (4)	Remove All	
300 Backup Persistence* NONE Use vServer Persistence* Virtual Server Name* Available (55) VS_WBLANCHET_VPSA_LMS VS_WBLANCHET_MFPSECURE_SO	Select All	Configured (4) NSLB_HTTPS NSLB_HTTP	Remove All	
300 Backup Persistence* NONE Use vServer Persistence* Virtual Server Name* Available (55) VS_WBLANCHET_VPSX_LMS VS_WBLANCHET_MFPSECURE_St MJM_VS_MXVPSX_HTTP	Select All	Configured (4) NSLB_HTTPS NSLB_HTTP NSLB_IPP	Remove All	0
300 Backup Persistence* NONE Use vServer Persistence* Virtual Server Name* Available (55) VS_WBLANCHET_VPSX_LMS VS_WBLANCHET_MFPSECURE_SO MJM_VS_MXVPSX_HTTP MJM_VS_MXVPSX_HTTPS	Select All	Configured (4) NSLB_HTTPS NSLB_HTTP NSLB_IPP NSLB_LPD	Remove All	0
300 Backup Persistence* NONE Use vServer Persistence* Virtual Server Name* Vs_wBLANCHET_VPSA_LMS VS_WBLANCHET_MFPSECURE_SC MJM_VS_MXVPSX_HTTP MJM_VS_MXVPSX_HTTPS MJM_VS_MX_IPP	Select All	Configured (4) NSLB_HTTPS NSLB_HTTP NSLB_IPP NSLB_LPD	Remove All	0

# **F5 Load Balancers**

For the F5 configuration the HTTP profile is how the Client\_IP or X-Forwarded-For settings are applied. The SSL profile (s) is where the certificate(s) used by HP AC are applied. These profiles are then applied to the virtual servers created for HP AC.

In this version of F5 (BIG-IP 12.1.2 Build 0.0.249), the Profile section is located under Local Traffic from the left-hand main menu section.

#### Importing the HP AC Certificate to the F5

Add the Certificate used by HP AC. Normally this will be the root CA if using a signed certificate. If using a selfsigned certificate created by HP AC, the certificate PFX file will be in the root of HP AC with the NLB virtual hostname as the friendly name.

1. Navigate to System – File Management – SSL Certificate List – Import

Retwork		
System		40
Configuration	Þ	20
Device Certificates	Þ	10:20 10:40 11:00 11:20 11:40
File Management	Þ	Data Group File List
Disk Management	Г	iFile List
Software Management	Þ	External Monitor
License		
Resource Provisioning		Assets Octificate List
Platform		
High Availability	Þ	Iw4o6 Tables

- 2. From the drop-down list, select the **PKCS 12** option.
- 3. In the following pop-up, create a Certificate name and add the Password then click Import

System » File Manageme	nt : SSL Certificate List » Import SSL Certificates and Ke	eys
		SSL Certificate/Key Source
SSL Certificate/Key Source		Import Type PKCS 12 (IIS)
Import Type	Certificate	Certificate Name     Create New Overwrite Existing
	Select xisting	
Certificate Name	Kev	Certificate Source Choose File No file chosen
		Paseword
Certificate Source	Certificate	Key Security Normal
Free Space on Disk	PKCS 12 (IIS)	Free Space on Disk 228 MB
Thee Space of Disk	Archive	Cancel Import
Cancel Import	Certificate Revocation List	

Once successful and the certificate appears in the SSL Certificate list, create the HTTP profile.

#### F5- Client-IP HTTP Profile

The first profile will be the HTTP profile for Client-IP

- 1. Expand Local Traffic-Profiles-Services-HTTP
- 2. In the HTTP window, select Create from the right

Hostname: CTSUPPORTF5 CTSUPPORTLO IP Address: 10.10.71.100	CAL	Date: Sep Tene: 8:37	13, 2019 AM (CDT)	HTTP Com	0				
Main Help About           Statistics           IApps	Loca Ø -	I Traffic 3	Virtual S Ferver List	Web Accel FTP TFTP DNS RTSP ICAP	Instantion	HTTP			
💽 DNS		- Status	Name     AutoE54	Request Ac	o - Services - Current SSI - Authentication	e - Ostabeses + Message Flooting + (	Paskiesz	Patoral	
Local Traffic	8	-		-					
	1.000		AuthF55	Diameter	•	Search			Create
Network Map	8	0	AuthF55 AuthF56	Diameter DHCPv4	• • Name	Search	# Application © P	Parent Profile	Create
Network Map	0	0	AuthF55 AuthF56 AuthF58	Diameter DHCPv4 DHCPv6	Name     Name     Norme     Norme     Norme     Normen	Search	# Application © P	Parent Profile	Create Partition / Path Common Common
Network Map Virtual Servers Policies	0	0	AuthF55 AuthF56 AuthF58 GabeF5	Diameter DHCPv4 DHCPv6 RADIUS	Anne     HTTP_miert     XrOewARD     clevt_p	Search	* Application © P http http	Parent Profile	Create. Partition / Path Common Common
Network Map Virtual Servers Policies Profiles	E E E Service	0	AuthF55 AuthF56 AuthF58 GabeF54	Diameter DHCPv4 DHCPv6 RADIUS SIP		Search	e Application e P http http http http jittp jittp	Parent Profile	Create Partition / Path Common Common Common Common
Network Map Virtual Servers Policies Profiles	Service		AuthF55 AuthF56 AuthF58 GabeF5-	Diameter DHCPv4 DHCPv6 RADIUS SIP SMTP		Search	# Application © P http http http http http http http htt	Parent Profile	Create. Partition / Path Common Common Common Common Common
Network Map Virtual Servers Policies Profiles IRules Rools	Conter		AuthF55 AuthF56 AuthF58 GabeF5-	Diameter DHCPv4 DHCPv6 RADIUS SIP SMTP SMTPS	Hame     HTTP_meet     XrOewARD     clent_b_tent     clent_b_tent     clent_b_tent     htp     clent_b_tent     htp     tentput	Search	e Application e P Intp Intp Intp Intp Intp Intp Intp Intp	Parent Profile	Create Partition ( Path Common Common Common Common Common Common Common

- 3. Provide a name for the profile and under **Settings**, check the **Custom** box from the left.
- 4. In the **Request Header Insert** field add the following syntax- *CLIENT-IP:[getfield [IP::client\_addr] % 1]*
- 5. The remainder of the settings can be left as default- Select **Update** at the bottom of the page.

Local Traffic » Profiles : Serv	ices : HTTP » New HTTP Profile	
General Properties		
Name	CLient-IP	
Proxy Mode	Reverse	
Parent Profile	http	
Settings	Custor	m 🗹
Basic Auth Realm		
Fallback Host		
Fallback on Error Codes		
Request Header Erase		
Request Header Insert	CLIENT-IP:[getfield [IP::client_addr] % 1]	
Response Headers Allowed		

### F5-X-Forwarded-For HTTP Client Profile

Alternatively, the X-Forwarded-For profile can be used. Follow the same steps above but instead of using Request Header Insert field, enable the Insert X-Forwarded-For option further down in the settings section

seneral Properties		
Name	XFORWARD	
Partition / Path	Common	
Proxy Mode	Reverse	
Parent Profile	http •	
lettings		Custom
Basic Auth Realm		
Falback Host		
Fallback on Error Codes		
Request Header Erase		
Request Header Insert		
Response Headers Allowed		
Request Chunking	Preserve •	
Response Chunking	Selective •	
OneConnect Transformations	R Enabled	
Redirect Rewrite	None •	
Encrypt Cookies		
Cookie Encryption Passphrase		
Confirm Cookie Encryption Passphrase		
Insert X-Forwarded-For	Enabled *	

### F5 - SSL Client and Server Certificate Profiles

As discussed at the beginning of this white paper, the HP AC certificates need to be applied to allow the load balancer to open the encrypted packets, insert header information, and re-encrypt before forwarding on to the HP AC Pull Print nodes.

- 1. Navigate to Local Server-Profiles-SSL-Client
- 2. Click Create on the right of the new SSL Client window

C Local Testilo	Data Format	Normalized •								
ji Local traffic	Auto Refresh	Local Traffic III Profiles : SSL : Client								
Network Map		o Services Content Databases Persistence	Protocol							
Virtual Servers	Local Traffic Summary	SSL - Authentication - Message Routing - Other -								
Policies	Object Type Total									
Folicies	Mintual Services 20	Search	Create							
-> Profiles	Services >	V Name Application	Parent Profile . Partition / Pat							
		wom-default-clientssl c	fientssl Common							
iRules	Content	Crypto-server-default-clientssi	fientssl Common							
Pools	Databases >	Clientssi-secure c	tientssl Common							
No. Aug		Clentsal-insecure-compatible	dientsal Common							
Nodes	Persistence	Clientssi (	none) Čommon							
Monitors 💽	Protocol >									
Traffic Class	SSL 🖕 🕠	Client 💿								
Address Translation	Authentication >	Server 💿								
	Message Routing	OCSP Stapling								
Acceleration	Classification									
Device Management	Other >									

3. Create a Profile name then check the **Custom** box on the left

- 4. The Certificate key Chain configuration becomes available, click Add
- 5. Select the appropriate certificate from the drop-down. Provide the passphrase if required.
- 6. Click **Add** when complete

**Note:** If a PFX file was originally imported into the F5 then the certificate name may appear the same. Otherwise you may have a Key (Root CA) with a different name than the certificate.

Local Traffic » Profiles : SSL	Client » New Client SSL Profile		Add SSL Certificate to	> Key Chain	
			Certificate	default /Common	-
General Properties			Key	NLBF5	
Name	SSL Profile Name		Chain	NLBVIP1-2	
			Passphrase	NLBVIP1-4	
Parent Profile	clientssl •		OCSP Stapling	NLBVIP1-5 NLBVIP1-6	
Configuration: Basic •		Custom 🗹		NLBVIP1-7 NLBVIP1-8	Add Cancel
	A			NLBVIP1-9	
			Add SSL Certificate to	Key Chain	
Certificate Key Chain			Add SSL Certificate to	Key Chain NLBF5	•
Certificate Key Chain	Add Edit Delete		Add SSL Certificate to Certificate Key	Key Chain NLBF5 NLBF5	•
Certificate Key Chain	Add Edit Delete		Add SSL Certificate to Certificate Key Chain	Key Chain NLBF5 NLBF5 None	•
Certificate Key Chain Proxy SSL	Add Edit Delete	ø	Add SSL Certificate to Certificate Key Chain Passphrase	Key Chain NLBF5 NLBF5 None	•
Certificate Key Chain Proxy SSL Proxy SSL Passthrough	Add Edit Delete	8	Add SSL Certificate to Certificate Key Chain Passphrase OCSP Stapling	Key Chain NLBP5 NLDP5 None None	•
Certificate Key Chain Proxy SSL Proxy SSL Passthrough Client Authentication	Add Edit Delete	₽ P Custom □	Add SSL Certificate to Certificate Key Chain Passphrase OCSP Stapling	Key Chain NLBP5 NLBP5 None Mone	•

- 7. Follow step 2 above but select Server this time instead of Client
- 8. Complete the remaining steps 3-6 to add the certificates to the SSL Server Profile.

~~			Partition / Path		Common		Local Traffic » Profiles : SSL : Server » New Server SSL Profile
	Local Iraffic		Proxy Mode	Proxy Mode F			
	Network Map		Parent Profile		http	•	General Properties Name Server SSL Profile Name
	Virtual Servers	÷	Catting a				Parent Profile serverssi •
	Policies	÷	Basic Auth Baalm				Configuration: Basic Custom M Certificate None V
	Profiles	×	Services				Key N.BFS
	iRules	•	Content +				SSL Ferward Prexy NL8VIP1-2 16 SSL Ferward Prexy Bypass NL8VIP1-3 16 SSL Ferward Prexy Bypass 16 SSL Ferward Prexy
	Pools	-	Databases +				Prany SSL NLEVIP1-5 (# Prany SSL Pesafitrough (# RUPL-5) (#
	Nodes	+	Persistence 📀				
	Monitors		Protocol				
	Traffic Class (		SSL →	Clien	t	•	
	Address Translation	->	Authentication	Serve	er	$\odot$	
	~		Message Routing	OCS	P Stapling	$\odot$	
	Acceleration		Classification 📀 io	ons	Enabled		
	Device Management		Other >		None •		]

Now that the profiles have been created, they can be assigned to the SSL virtual server

1. Select Local Traffic-Virtual Servers and Edit or Create the SSL Virtual Server

Ma	in Help A	bout	Local	Traffic »	Virtual Se	rvers : Virtu	al Serve	r List	
100 s	Statistics		۰ م	Virtual S	erver List	Virtual Addr	ess List		
	Apps								
			1				Sea	arch	Create
<b>53</b> 🛛	DNS		<	Status	<ul> <li>Name</li> </ul>	_			
<u>.</u>				•	QAVS_63	5			
090 L	ocal Traffic			•	QAVS_63	1			
	Network Map			•	QAVS_55	56			
L	Virtual Servers	•		•	QAVS_51	5			
	Policies	Þ		•	QAVS_38	9			
	Profiles		•	0	QAVS80				
	iRules			•	QAVS443				
	Pools		-						
	Nodes		-						
	Monitors	(+)							
	Traffic Class	•							
	Address Translation	÷							
			-						
A (2)	Acceleration		-						
	Device Management			10.00					
			Enabl	e Disab	le Delete	t			

- 2. If the virtual server currently exists, navigate to the configuration section.
- 3. Locate the HTTP Profile and select either the Client-IP or X-Forward profile created earlier in this white paper.

General Properties							
Name	NLBF5						
Description	HPAC SSL 443						
Туре	Standard •						
Source Address							
Destination Address/Mask	10.10.15.x						
Service Port	443 HTTPS V						
Notify Status to Virtual Address							
State	Enabled •						
Configuration: Basic •							
Protocol	TCP						
Protocol Profile (Client)	tcp v						
Protocol Profile (Server)	(Use Client Profile)						
HTTP Profile	XFORWARD V						
FTP Profile	None V						
RTSP Profile	None 🔻						
SSH Proxy Profile	None						

4. Next, navigate further down to the Server and Client SSL Profile and move the proper certificate profiles to the selected box

SSL Profile (Client)	Selected /Common	Available
SSL Profile (Server)	Selected /Common	Available

5. Select **Update** at the bottom of the page.

#### **Session Persistence**

Best practice in HP AC is ensuring the load balancer virtual server's session persistence is set with a value high enough to prevent conflicts with end user during an HP AC associated interaction.

To create the Persistence Profile, Navigate to Local Traffic- Profiles- Persistence

- 1. Select **Create** on the right
- 2. Persistence Type Source Address Affinity
- 3. Select **Custom** to enable the configuration options
- 4. Set the Timeout value to minimum of 300 (5 minutes)

NOTE: Administrators may choose a different value however, best practice is a minimum of 5 minutes

**NOTE**: "Source\_5min" is used here as an example only.

Statistics			
	General Properties		
iApps	Name	Source_5min	
S DNS	Persistence Type	Source Address Affinity	
	Parent Profile	source_addr •	
	Configuration		Custom 🗹
Network Map	Match Across Services		Ø
Virtual Servers	Match Across Virtual Servers		
Policies	Match Across Pools		
Profiles	Hash Algorithm	Default V	Ø
iRules >	Timeout	Specify ▼ 300 seconds	Ø
Pools >	Prefix Length	None T	
Nodes	Map Proxies	✓ Enabled	•
Monitors 🔶	Override Connection Limit		
Traffic Class	Cancel Repeat Finished		

For F5, the Persistence profile is applied in each virtual server

- 1. Navigate to Local Traffic-Virtual Servers
- 2. Select the first HP AC virtual server
- 3. Select Resources tab at the top
- 4. Set the **Default Persistence Profile**

**NOTE**: "source\_5min" is used here as an example only.

<b>M</b>	Statistics	*	-	Properties	Reso	urces	Statist	ics	
	iApps	Loa	nd B	Balancing					
S DNS		De	Default Pool			Pool_Active_Active			T
			Default Persistence Profile		9	source_5mi	n 🔻		
480		Fa	allba	ack Persistence Profi	le	None	•		
	Network Map		Update						
	Virtual Servers								
	Policies	iRu	les						
	Profiles	Na	me						

hp.com/go/support

Current HP driver, support, and security alerts delivered directly to your desktop

© Copyright 2019 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Created September 2019