

ExtremeGuest Essentials Setup Guide

ExtremeCloud IQ Essentials Documentation

Published: March 2022 Part number: 9037476-00

Extreme Networks, Inc. Phone / +1 408.579.2800 Toll-free / +1 888.257.3000 www.extremenetworks.com

© 2022 Extreme Networks, Inc. All rights reserved.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. All other registered trademarks, trademarks, and service marks are property of their respective owners. For additional information on Extreme Networks trademarks, see www.extremenetworks.com/company/legal/trademarks.

Contents

Introduction to ExtremeGuest Essentials	.3
Initial Setup for ExtremeGuest Essentials	5
Test a Simple Accept and Connect	.13
Using HTTPS with ExtremeGuest Essentials	.21
How to use HTTPS	. 21

/ 2

Table of Figures

Figure 1:	Login Screen	5
Figure 2:	Add Network Policy	5
Figure 3:	Policy Details	6
Figure 4:	Add Wireless Networks	6
Figure 5:	Wireless configuration	7
Figure 6:	Device Templates configuration	7
Figure 7:	Device onboarding	8
Figure 8:	Policy name and location	8
Figure 9:	Update Devices	9
Figure 10:	Update Network Policy and Configuration	9
Figure 11:	Select Extreme Guest	9
Figure 12:	Enable ExtremeGuest Essentials	10
Figure 13:	Select wireless network	10
Figure 14:	Summary Page	11
Figure 15:	More Insights	11
Figure 16:	Additional dashboards and advanced configurations	12
Figure 17:	More Insights	14
Figure 18:	Policy Onboarding	15
Figure 19:	Create Onboarding Policy	16
Figure 20	: Create Rule	17
Figure 21:	Splash Template	18
Figure 22	: Template configuration	18
Figure 23	: User Templates	19
Figure 24	: Customize User Templates	20
Figure 25	: Apply Template	20

Introduction to ExtremeGuest Essentials

ExtremeGuest Essentials is a comprehensive guest management and engagement solution that customizes engagement by analyzing customer behavior and interest, and then tailoring services based on those insights. For example, using metrics that can be measured through ExtremeGuest Essentials, you can track how many customers use the guest network, how often they visit, and how much time they spend on the guest network.

It includes a customizable Dashboard that provides a holistic view of user data at the entity level or for individual sites. You can use the dashboard graphs and themes to create customized dashboards providing a comprehensive overview of user trends and engagement.

ExtremeGuest Essentials utilizes social networking behavior to increase patronage, expand brand exposure, and understand client demographics and preferences in a more comprehensive and personal way. Guest onboarding with sponsor approval is supported, allowing a sponsor to approve or deny guest access with a single click.

Use ExtremeGuest Essentials to configure and implement user notification policies and rules to specify the method used for all types of communication with guest user, such as communicating the passcode to newly registered guest users or sending a report to specified guest users.

Onboarding policies are used by ExtremeGuest Essentials to give flexibility when determining hotspot user access. Policies are matched to the hotspot user based on onboarding rules. Then the matching policy with the highest precedence number is used to onboard the hotspot user. An onboarding policy consists of one or more match criteria that are used to filter guests and apply an action.

ExtremeGuest Essentials includes a summary of captive portal splash templates. These splash templates are either customized-system templates or user-defined templates. The System Templates tab displays a summary of available captive portal splash screen templates, which you can use to download a system template and customize it to suit your requirements, clone a system template, or view a summary of networks to splash templates mapping.

The User Templates provide a robust, easy-to-use splash template builder wizard. Use the wizard's 'drag & drop' elements, color, text, and language customization tools and logo upload options to create your branded captive portal web pages, as well as the addition of photos and video.

You can analyze client and online user details at the site level. You can access a summary of all client status, as well as detailed information for each client. Drill down to the site level to view online and blocked user details for a specific site.

Initial Setup for ExtremeGuest Essentials

To set up ExtremeGuest Essentials, you will create a network policy, onboard a device, and launch the ExtremeGuest Essentials app. Follow these steps:

1. Log into ExtremeCloud IQ.

ExtremeCloud	Aggregate Daily Data Traffic Management Events per Day Aggregate Daily Client Sessions 48.48PB 10.66b 310.69m
Email Password LCGIN Forgot your password? Reset it here Don't have an account? Register here	Image: state in the
© 2022 Estreme Nervorks - All Rights Reserved. ISO 27001 Certificate Service Availability	Washington Walkedow Washington Commany in Cele Same Candidate Subject of the Same Candidate Same

Figure 1: Login Screen

- 2. Set up the Network Policies:
 - a. Select Configure > Network Policies > ADD NETWORK POLICY

0	CONFIGURE		
*	Network Policies		
_0>	Common Objects	ADD NETWORK POLICY EXPRESS POLICY SETUP	_
** >	Users	302W 🞯	e
	Guest Essentials Users	1 SSID := test-Guest Unsecured (Open) Net 1	1 5
盘 >		1 DEVICE TEMPLATE := AP_302W 0	2 A A
		ADD NETWORK ADD DEVICE TEMPLATE	

Figure 2: Add Network Policy

- b. Enter a Policy Name
- c. Select Save

	Extre	meCloud [®] IQ Pilot					
Ø	CIES	Network Policies > Nev	v Poli				
*		POLICY DETAILS	WIRELESS NETWORKS	DEVICE TEMPLATES	ROUTER SETTINGS	ADDITIONAL SETTINGS	DEPLOY POLICY
_⊡> ;**>	NETWOR	New Policy					
	GURE -	What type of polic	y are you creating?				
₽>	CONFL	Vireless	Switching Routing				
		Please name your	policy				
		Policy Name *	Network Policy Name				
		Description					
					1		
		Enable Presence Analytics	OFF				
?							
>	>	EXIT					SAVE
Figu	ire 3	Policy Details					

- 3. Set up the Wireless Networks:
 - a. Select the WIRELESS NETWORKS tab
 - b. Select the +icon



Figure 4: Add Wireless Networks

- c. Enter a Name (SSID)
- d. Enter a Broadcast Name
- e. Under SSID Authentication, select Open
- f. (Optional) Assign a VLAN
- g. Select SAVE

OLICIES	Broadcast Name * VIFIR Radio (G GHz only) VIFIR Radio (G GHz only) VIFIR Radio (G GHz only)	
ORK PC	SSID Usage	
- NETM	SSID AUTHENTICATION MAC AUTHENTICATION	
CONFIGURE	Enterprise O Personal D WPA/WPA2/WPA3 Private Pre-Shared Key	WEP Copen Unsecured
	Enable Captive Web Portal	
	User Access Settings Configure your GoS, VLAN, Frewall policies, and Traffic Tunnelling	
	Default User Profile default-profile + 55= VLAN : 1 + 55=	
	Additional Settings 4 Configure your Availability Scheduling, Security Controls, Optional Settings, and Client Monitoring	
	FYIT	

rigure 5. Whereas configuration

- 4. Add the corresponding device templates:
 - a. Select the **DEVICES TEMPLATES** tab (See Figure 3: Policy Details for the location of the Device Templates tab)
 - b. Select the 🕇 icon and a device from the list
 - c. Give the template a name
 - d. Under the WifiO and WifiI tabs, select as Client Access mode.
 - e. Select SAVE TEMPLATE

	Extre	meCloud [®] IQ Pilot				۹ 🖬	≜ Θ ⊑	
¢	ES							^
*>	POLIC	CONFIGURATION	ASSIGN		SELECT ALL PORTS	DESELECT ALL PORTS		
ED>	ORK	Device Configuration	ExtremeCloud IQ	ETH 0	CONSOLE	WIFI 0 WIFI 1		
\gg	NETW	Advanced Settings				<u>a</u>		
 >	URE -							ï
€>	CONFIG		Wireless Interfac Control actions from th Note: Please ensure the WIFIO W	es ▼ Access Point's Wi-Fi ports radio profile setting conforms to the re	gulatory channel and transmit p	ower.		
			External Antenna	Omni • External antenna only for AP122X, A	AP245X, and AP1130			1
			Radio Status	ON				l
			Radio Mode	802.11g/n				ł
			Radio Profile	radio_ng_ng0 • + Note: Only the AP510C, AP510CX, A AP460S6C, and AP460S12C suppor	NP550, AP650, AP650X, AP3050 tts MU-MIMO on its WI-Fi0 Inter	C, AP305CX, AP302W, AP410C, lace	AP460C,	
			Radio Usage	Client Mode	Client Access	Backhaul Mesh Link	Sensor	
			Enable SDR (Softw Dynamic selection of	are Defined Radio) f radio band				
>	>	EXIT				CA	NCEL SAVE TEMPLATE	

Figure 6: Device Templates configuration

- 5. Onboard a device:
 - a. Select Manage > Devices
 - b. Select + > Advanced Onboarding
 - c. Select either Deploy your devices to the cloud or Deploy your devices locally
 - d. Select Let's Get Started!
 - e. Refer to the online Onbording Getting Started Guide for the complete onboarding procedure.

	ExtremeCloud IQ Pi	lot
0	MANAGE	CONNECTION STATUS 1 Online / 1 Offline
*>	Summary	T Default View
	Planning	+ ⊥ ✓ ■ Quick Add Devices >
**>	Devices	Advanced Anboarding ME POLICY
 >	Client 360	AH-57f000 essentials
6 >	Users	PLM-Flo-2173 essentials

Figure 7: Device onboarding

6. When the device is reported online in ExtremeCloud IQ, assign the location and the network policy you created in step 2 on page 4.

Extren	neClo	oud IQ Pil	ot									
5	CONN 1 Onl	IECTION STATU	S	C TOTAL A	APPS O		CLIENT	rs o		USERS 0		
Ŧ	D	efault View										
	+	± ∕ ĭ	1						Enter Hostna	me, MAC Addr or	Serial # Q U	TILITIES
		STATUS	HOST NAME	POLICY	UPTIME	MGT IP ADDRESS	CLIENTS	MAC	LOCATION	SERIAL #	FEATURE LICENSE	DEVK
		000	AH-57f000	essentials	N/A	10.10.13.197	0	40882F57F00	PLM LAB >:	0302201208024		Pilot
		008 1	PLM-Flo-2173	essentials	10d 4h 52m	10.10.13.186	0	BCF3105EB48	PLM LAB >:	0410200520217		Pilot
		00	SIM-4DA594	Assign Policy	N/A	192.168.151.226	0	FF50D64DA5	PLM LAB >:	9899183642790		Not I
										•		

Figure 8: Policy name and location

- 7. After the very first onboarding and assignment of the network policy, perform a complete CONFIG PUSH on the onboarded AP.
 - a. Select a device or devices.
 - b. Select UPDATE DEVICES

De	fault View					1		Showing	3 of 3 1 Selec	ted Select: Al	l Pages, None
+	1	i				1	iai # Q UTILITIES	ACTIONS	b UPDAT	E DEVICES	III G
	STATUS	HOST NAME	NETWORK POLICY	UPTIME	MGT IP ADDRESS	СЦ	FEATURE LICENSE	DEVICE LICENSE	MODEL	NTP STATE	OS VERSION
	$\bigcirc \bigcirc $	AH-57f000	essentials	N/A	10.10.13.197	0	8024	Pilot	AP302W	Enabled	10.3.4.0
a	008	PLM-Flo-2173	essentials	15d 4h 50m	10.10.13.186	0	20217:	Pilot	AP410C	Enabled	10.4.4.0
	80	SIM-4DA594	Assign Polic	S N/A	192.168.151.226	0	.2790	Not Required	AP460C	Enabled	10.4.4.0 (1
4						5					•



- c. Select Update Network Policy and Configuration and then Complete Configuration Update
- d. Select PERFORM UPDATE

0			ON STA	TUS	Г	Device Update	×	0 0		S O Rogue A
	De +		View	ĩ		2 devices will be updated Device List may need to be reloaded/refreshed to see some changes due to the update.		showing	3 of 3 2 Selec	ted Select: / E DEVICES
			TUS			Update Network Policy and Configuration Delta Configuration Update Update Network device with charact configuration		CENSE	MODEL	NTP STATE
a		0)	217	Complete Configuration Update Update device with all configurations. Used to reset device to ExtremeCloud IQ configuration settings. (Supported only on devices running HOS or IQE Timware)				
		٢			594	Upgrade IQ Engine and Extreme Network Switch Images		ired		
						Activation Time for Extreme Networks Devices Running Images				
						SAVE AS DEFAULTS CLOSE PERFORM UPDAT				

Figure 10: Update Network Policy and Configuration

- 8. Launch ExtremeGuest Essentials:
 - a. Select Essentials > Extreme Guest



- b. Select Enable

🗾 Extreme	Cloud IQ Pilot	9 II 0 A 0 E
 ▲ ● ♥ ♥ ♥ ● ♥ ♥ ♥ ● ♥ ♥ ● ♥ ♥ ● ♥ ♥ 	ExtremeGuest Essentials Guest Access and Analytics	Want to know more about ExtremeGuest Essentials?
>	Cloud-managed Guest Access & Analytics Simple and secure guest onboarding options including sponsored guest access, self-registration with SHS/Email notification and social ID logins Completely customizable location specific splash pages with built-in splash template builder ExtremeGuest also includes rich set of analytics providing deep business insight into guest behavior across all your locations	Enable to explore Guest Services Included with Pilot subscription - no additional cost
Figure 12:	Enable ExtremeGuest Essentials	

9. Select the open wireless network you created and select apply (see step 3 on page 5).



Figure 13: Select wireless network

As devices start to use the WLAN, the ExtremeGuest Essentials Summary screen begins to load data and display analytics.



Figure 14: Guest Essentials Summary

You can view additional details by selecting More Insights.



Figure 15: More Insights

On the **More Insights** page, you can configure additional dashboards and advanced configurations as shown is Figure 16: Additional dashboards and advanced configurations.



Figure 16: Additional dashboards and advanced configurations

Test a Simple Accept and Connect

The following steps take you through the process of testing a simple accept and connect operation.

- 1. Configure the Network Policy.
 - a. Open Network Policies
 - b. Edit the existing policy (see step 2 on page 4 to locate your policy)
 - a. Select its edit icon.

i ¹¹	•	5
		dit
	Unsecured (Open) Net	1
TES ;=		
1		
1		
OPK		ATE
	ATES :== 1 1	Unsecured (Open) Net ATES := 1 1 1

- b. Follow steps 3a 3d on page 5 and create an open WLAN
- c. Select Enable ExtremeGuest Essentials
- d. (Optional) Select a VLAN
- e. Select Save

Name (\$505 * Hunt/Guest	Brancus son comp	ale of 5 Gen		
Broadcast Name * Hunt/Guest	with Radio (5 Get	r enty)		
SSID Usage MEANTENTICATION NO. A	UNANGADON			
Enterprise WPA / WPA2 / WPA3	O Personal WPA / WPA2 / WPA3	👌 Private Pre-Shared Key	÷ ₩₽	e Open Unsecured
Enable Captive Web Portal				
Enable ExtremeGuest Essentials	201			
Configure your session times, DHCRyDNS sarv	ors, Domain Name, Network and Secarity Settings			
Walled Garden				
+ #				
D RIVERT NAME	RENCE	РЕОТОСОК		PORT
		No-records found.		
User Access Settings Certigure your Oct. VLAX, Ferenal policies.	and Traffic furnaling			
Default User Profile default-profile VLAN 1	+ 04			

2. Push the configuration to the AP. To do this, follow the procedures in step 7 on page 8 but replace step c with **Delta Configuration Update**

E	Extreme	Cloud IQ	×	ExtremeGuest : 0	Configuration /	× +													3 <u>111</u>	Ø	×
4	\rightarrow	C ŵ		🖸 🔒 https	://va2.extrem	ecloudiq.c	om/#/dev	íces						70%		☑ ☆	-				≡
6	Getting	Started F	Business	Lab Private Cloud	Lab 🖪 Con	nect - Locati	on 🖪 101	Essentials													
-	Extr	emeClo	ud IQ Pilot													5	9	A. E	Richard H	tunt	IE.
	Enter			STATUS			_	_	_					ALARMS O				SEC	URITY	E Cau	~
	VICES		32 Online / 15 (1,10.	or or the	Device Up	date				×		ALCOND 12 C				O Rogue APs	10 Rogue Clier	its .	-
₽ >	- DE	×	Default View				1 device will	be updated D	wice List n	nav need to be reloaded/refreshed to see some chan	uges due to the updat		^		She	owing 45	of 45 1 Sele	cted Select:	All Pages, No	ne	
*>	NAGE		T ± *					13					an C		i A	CTIONS	UPDA	TE DEVICES		ľ., (
di >	MAI		STATUS	HOST NAME	POLICY	UPTIME	Update N	etwork Policy a	ind Configu	ration				OS VERSION	NOAGENT C	HANNEL	POWER	CHANNEL	POWER	X	
			0	AH-046680	FE-ATOM	N/A	O Delta Upda	te device with	changed co	infiguration.				10.0.9.2 (10.	N/A N	4/A	Down	Auto	Auto		
			0	FE-ATOM-1	FE ATOM	N/A	O Com	plete Configura	all configura	e ations. Used to reset device to ExtremeCloud IQ configur	ration			10.0.9.2 (10.	N/A N	VA.	Down	Auto	Auto		
5			. • 8	FE-ATOM-4	FE-ATOM	N/A	setti	ngs. (Supporter	l only on de	vrices running HOS or IQE Firmware)				10.0.9.2 (10.	N/A N	VA	Down	Auto	Auto		
*			. • 8	FE-ATOM-2	FE-ATOM	N/A	Upgrade	IQ Engine and	Extreme Ne	twork Switch Images				10.0.9.2 (10.	N/A N	1/A	Down	Auto	Auto		
0			. • 8	FE-ATOM-3	FE-ATOM	N/A	Actuation Tin	no for Extramo	Naturatics D	andres Durater Insure				10.0.9,2 (10,	N/A N	VA.	Down	Auto	Auto		
٢			0 • 0	AH-046640	FE-ATOM	N/A	Activate	a next school :	receivers rel	kantina manaalisi				10.0.9.2 (10.	N/A N	VA.	Down	Auto	Auto		
				AH-046880	FE-ATOM	N/A	O Accivace	at next repoot (requires rec	sooting manuality)			~	10.0.9.2 (10.	N/A N	¥/A	Down	Auto	Auto		4
				FE-305-4	FE- LAB-305C	N/A				SAVE AS DEFAULTS	CLOSE PER	FORM UPDATE		10.2.2.0 (10	N/A N	1/A	Down	Auto	Auto		Ľ
			0 • 0	FE-305-3	FE- LAB-305C	N/A	Managed	10.10.13.155	0	BCF31092458 RichH INC = 0.3052008153144	2020-11-02 13:58:21	AP305C		10.2.2.0 (10.	N/A N	U/A	Down	Auto	Auto		
			. • 8	FE-305-1	FC- LAB-305C	N/A	Managed	10.10.13.160	0	BCF31091F30K RichH INC = 03052008152814	2020-12-07 14:12:39	AP30SC		10.2.3.0 (10.	N/A N	2/A	Down	-157	20		
			. • 8	FE-305-2	FE- LAB-305C	N/A	Managed	10.10.13.863	0	BCF31091F3C(RichH INC > 03052008152817	2020-11-02 11:46:33	APSOSC		10.2.2.0 (10.	N/A N	ųΆ	Down	Auto	Auto		
			. • •	FE-410I-1	Assign Polic	6d 4h 23m	Managed	10.10.13.178	3	489805FD30ERichHINC > 1943Y-16136		AP410		7510-015	N/A A	uto	Auto	149	20		
				FE-410-UP	FE-4IOC- Essentials	Od Oh 28m	Managed	10.10.13.152	0	BCF3105EA30 RichH INC : 04102005202103	2020-12-09 15-18-15	APHOC		10.2.3.0 (10	N/A N	1/A	Down	40	19		
				FE-410-Office	FE-410C- Essentials	Od 1h 8m	Managed	103013193	0	BCF3105DEB4 RichHINC > 04102005201568	Device Update Failed.	APHIOC		10.23.0 (10.	. N/A. N	1/A	Down	157	18		
				FE-410-Studio	FE-4IOC- Essentials	Od 3h 43m	Managed	10.10.13.365	0	BCF3105DBCC RichH INC : 0410200520179	2020-12-09 15.21.59	AP4IOC		10.2.3.0 (10.	. N/A N	1/A	Down	44	19		
				FE-410-Garage	FE-4IOC- Essentials	N/A	Managed	10.10.13.186	0	BCF3105EB48 RichH INC : 04102005202175	2020-12-09 15:23:27	AP4IOC		10.23.0 (10	N/A 1		20	165	18		
				FE-460	Assign Polic	3d 12h 12m	Managed	10.10.13.199	1	489BD5FD61C RichH INC : 1949Y-I0141		AP460		7.510-015	N/A A	uto	Auto	149	20		
				FE-7532-SW	Assign Polic	16d 23h 15m	Managed	10.10.13.32	5	84248D18938/ RichH INC : 14182522200857		AP7532		7510-015	N/A A	ALIEO	Auto	36	20		
100				Seaway-AP1-75E898	Assign Polic	2d Oh 19m	Managed	101010111	9	88500175E891 RichH INC : 18015522200211		AP7532		751.0-015_	N/A 1		Auto	165	20		
0				Seaway-AP5-75E8B8	Assign Polic	2d 9h 3m	Managed	10.1010136	6	B8500175E8B: RichH INC + 18015522200219		AP7532		7.510-015_	N/A 1		Auto	153	-20		
\$	>		m = 0	Seaway-AP3-75E908	Assian Polic	Art Art 72m	Managed	101010113	7.6	BASOD175ER0: Richiel INC 1 IR015572200239		AP7532		7510-005	N/A 6		Auto	40	20		~

- 3. To onboard guest devices:
 - a. Select More Insights > Configure > Onboarding > Policy



b. Select 🖶 icon to onboard guest devices

ExtremeGuest E	ssentials			O User Xxxx User's Lab
CONFIGURE	Onboar	ding Policy		
✓ Settings				C 4
Authorization Policy		Name	Description	Action
Access Groups		Default	default onboarding policy for all u	ser regi
V Deployment	0	SponsorGA	SponsorGA	0
Location	0	OPT-IN	OPT-IN	Û
Network		SeawayGuest	SeawayGuest	Û
Devices				
V Notification				
Policy				
V Onboarding				
Policy				
Rules				

Figure 18: Policy Onboarding

- 4. Add an **Onboarding Policy** (see Figure 18: Policy Onboarding to find the Policy screen):
 - a. Select 🛨 icon
 - b. Enter a Policy Name
 - c. Enter the Criteria #1 parameters:
 - i. For Conditions, select Any
 - ii. For Action, select Register Client
 - iii. For Validity and Group, enter days, hours, or mins for which the registered client is valid
 - iv. For Select a group, select GuestAccess
 - b. Select Save

••	Extreme Guest Esse	entials			O User Xxxx User's Lab	
٢	CONFIGURE	Onboarding Policy				
\$	 Settings Authorization Policy Access Groups 	Policy Name*: Description:	Policy Name Policy Descriptior			
	✓ Deployment	Criteria #1	Description:		+ -	
	Location	Condition(s)		Action	Validity and Group	
	Network Devices	Any	~	Register Client 🗸	0 Day(s) 0 Hour(s) 30 Min(s)	
	✓ Notification			•	Select a group	
	Policy					
	✓ Onboarding Policy					
	Rules					
	Splash Templates					
	Users					
	Clients					
•					Save Cance	el

Figure 19: Create Onboarding Policy

- 5. Add a rule (see Figure 18: Policy Onboarding to find the Rules screen):
 - d. Select 🛨 icon
 - e. Enter a Rule Name
 - f. Select a **Policy**
 - g. Select a WLAN Network
 - h. Select a Location
 - i. Select a Precedence Level

The Precedence Level determines the priority of a rule. The lower the value, the higher the priority. Rules with lower precendence will be applied first. The level ranges from 1 to 100.

j. Select Save

Create Rule			
Rule Name*			
Rule Name			
Policy*			
Policy	~		
Network			
All Networks	~		
Location			
PLM LAB			~
Precedence Level*			
7	-		
		Save	Cancel

Figure 20:Create Rule

- 6. Configure the Splash Template:
 - a. Select Accept_and_Connect under the System Templates tab
 - b. Select the clone \Box icon

CONFIGURE C	Andrew Researching	
Settings	System remplaters	
Authorization Policy		
Access Groups	Balancia la par Company!	
✓ Deployment		05
Location	Company	ea
Network	NUMP Address 7	-
Devices	Sector And	=
✓ Notification		
Policy	Accept_and_Connect	Accept_and_Connect_w
✓ Onboarding		Cone System Template.
Policy	Websens to car Company!	
Rules		
Splash Templates	Company	08
Users		Central
Clients		=
	Email_Access	Social_WIFI_with_Face
•		
2 · · · · · · · · · · · · · · · · · · ·		

Figure 21: Splash Template

- c. Customize the Splash Template
 - i. Drag and drop the layouts into the template
 - ii. Complete each layout

۲	CONFIGURE	Clone System Template Name			
٥	✓ Settings Authorization Policy	Landing Welcome +			• •
•	Access Groups	Image	o x	×	Select Theme
	Location			8	Layouts -
	Network Devices				
	V Notification				
	v Onboarding				
	Policy Rules				
	Splash Templates				
	Users	Login Options	οx	×	
	Clients	ACCEPT &			
		Terms and Conditions	¢ ×	×	Tomplatos
>		Terms And Conditions Privacy Policy			iempiards

Figure 22: Template configuration

- d. Select the save 🖹 icon
- 10. Configure User Templates:
 - a. Select the User Templates tab
 - b. Select the add + icon

	¥ T	-
Welcome to our Company!	Organization Name	
	Login	
	Enter Unersame	
	Kritvelo kuonaali- Eriter Paascode	
	Gair Sgill	
	Not registered?	
ACCEPT & CONNECT	Webs	
Tarms and Conditions () Phylocy Milley	Grant	
	Terms and Los Morea 1 Privace Perce	

Figure 23: User Templates

- c. Customize the template
 - i. Drag and drop the layouts into the template
 - ii. Complete each layout
- d. Select the check mark your new template to distribute the splash page to the network

	Log	n	
	110.004440-		
	Enter Usernome		
	RECEIVED PAIDCODE/		
	Enter Passcode		
	000 C	Serie	
	Torgot Resizione	Register Now	
	(Dr) Sign	in using	
	Marningrill The Google CAsth requests an Please use full browser instead	e prohibited on the embedded webeie I of the embedded browser	WL.
	F	in	
	ferms And Condition	E Physics Polica	
Nepean		Û	°
			Apply Template To
	Organizati	on Name	Network
	100	0	

Figure 24: Customize User Templates

- e. Select a Location
- f. Select a Network
- g. Select Add
- h. Select Apply

OCATION			NETWORK	ACTION
PLM LAB			Sponsor	Û
ocation:	PLM LAB	-		

Figure 25: Apply Template

The operation is complete. You can test the splash page setup with a device.

Using HTTPS with ExtremeGuest Essentials

Browser updates are causing security exceptions when the user submits their login credentials. This occurs because they are using HTTP in an HTTPS connection. The following procedure is an option if you want to prevent security exceptions. The procedure requires a domain certificate that is pushed to the Access Points (AP) through ExtremeCloud IQ, adding a dummy record in your Domain Name Server (DNS) file for the webserver Fully Qualified Doman Name (FQDN).

How to use HTTPS

1. Obtain a certificate. You can use your company's wildcard domain certificate. If you do not have one, you will have to purchase one from a well-known Certificate Authority (CA) provider.

There are two different certificate formats that can be used:

e. A wildcard certificate where the Common Name (CN) is a wildcard domain.

*.*domain*.com à CN=*.iqe-ext.com

f. A certificate with CN as a dummy hostname, for example *guest* or *eguest*.

hostname.domain.com à CN=guest.iqe-ext.com or CN=eguest.iqe-ext.com

- 2. Map the hostname to an IP address
 - a. On the DNS server serving the wireless guest clients, create an "A" record
 - b. Map the hostname to a private unused IP address. For example:

guest.iqe-ext.com 300 INA 192.168.14.1

NOTE: IP mapping can be to any private unassigned address. The IP address is a placeholder.

- c. Verify the FQDN resolves using nslookup.
- d. Verify that the wireless clients connecting to the guest SSIDs are pointed to the DNS.

NOTE:

The same FQDN *hostname.domain*.com used as the CN needs to be specified as a webserver name in the Wireless Local Area Network (WLAN).

- 3. Import the certificate and corresponding private key into ExtremeCloud IQ.
 - a. Log into ExtremeCloud IQ.
 - b. Select Configure > Common Objects > Certificate > Certificate Management
 - c. Select the import 📩 icon

🗘 🔀 CONFIGURE	COMMON OBJECTS						-	÷ v
> Network Policies	> Policy	Cer	tificate Managemen	it				
Common Objects	> Basic	+	/古古■					
Users	Security		File Name	Туре	Encrypte d	Size	Date Modified	Description
	· · · · · · · · · · · · · · · · · · ·		Default_CA.pem	CA	true	875	Fri Sep 04 2020 07:20:21 GMT- 0400 (Eastern Daylight Time)	Default CA file
Guest Essentials U	sers > QOS		Default-CWPCert.pem	CERT_KE Y	false	2172	Fri Sep 04 2020 07:20:21 GMT- 0400 (Eastern Daylight Time)	Default cwp key file
⊖ >	> Management		Default_key.pem	KEY	true	963	Fri Sep 04 2020 07:20:21 GMT- 0400 (Eastern Daylight Time)	Default key file
	Network		Default-Server_cert.pem	CERT	false	912	Fri Sep 04 2020 07:20:21 GMT- 0400 (Eastern Daylight Time)	Default server cert file
			Default-Server_key.pem	KEY	false	887	Fri Sep 04 2020 07:20:21 GMT- 0400 (Eastern Daylight Time)	Default server key file
	> Authentication							
	V Certificate							
	Certificate Management							

Figure 26: Certificate Management

- 4. Import the Certificate and Certificate Key files
 - a. Choose SELECT
 - b. Select the certificate file or certificate key file
 - c. For File Type, select CERT or CERT_KEY
 - d. (Optional) Select one or both options for Certificate Conversion Options
 - e. Select SAVE
 - f. Repeat these steps for CERT_KEY

••	Extre	meCl	oud IQ Pilot		Q	¢	θ		E
€ } ≫>	N OBJECTS	VAGEMENT	Certificate Management ⇒ Impo Import	rt Certificate					
_⊡> ;**>	соммо	CATE MAI	File*	SELECT					
∷ >	IFIGURE -	CERTIFIC	File Type Certificate Conversion Options	CERT *					
₿ >	CON			Convert the certificate format from PFX to PEM Convert the certificate from DER to PEM					
							CANCEL	SAVE	
									•

Figure 27: Certificate Management import

- 5. Concatenate the certificate and private key
 - a. Select Configure > Common Objects > Certificate > Certificate Management
 - b. Select the add icon (see + in Figure 26: Certificate Management for the location of the icon)
 - c. Select Concatenate an existing certificate and private key
 - d. Enter an HTTPS Certificate/Key Name. This is the name that is displayed when selecting the HTTPS certificate in the WLAN.
 - e. For Certificate, select the one you supplied.
 - f. For **Private Key**, select the private key obtained from the CA.

NOTE: The Private Key file is generated when creating a Certificate Signing Request (CSR). Save the file and upload it here.

g. For **Password**, enter the Private Key password used when the CSR was generated. If a password was not used for the CSR generation, then leave **Password** blank.

••	Extre	meCle	oud IQ Pilot				
 ✿ ↓ ↓	CONFIGURE - COMMON OBJECTS	CERTIFICATE MANAGEMENT	Certificate Management > Create Create Certificate/Ke ExtremeCloud IQ CA Server CSR Concatenate an existing certificate Self-signed certificate	Certificate/Key Y ate and private key			
•>			HTTPS Certificate/Key Name *	Guest-Cert			
א> ם			Description				
6			Certificate *	SrvrCert.pem -	IMPORT		
•			Private Key	Srv-PrivKey.pem 👻	IMPORT		
			Password	Show Password		CANCEL	SAVE

- 6. Create the WLAN
 - a. Select Configure>Network Policies
 - b. Select the WIRELESS NETWORKS tab
 - c. Right-click the add icon + and select All Other Networks (standard)
 - d. Enter a Name (SSID)
 - e. Enter a Broadcast Name
 - f. Under SSID Usage, select Open (Unsecured)
 - g. Select Enable ExtremeGuest Essentials
 - h. Select Advanced Configuration
 - i. Select Enable HTTPS and select the HTTPS certificate file you created in step 5 on page 22
 - j. Enter the **Webserver Domain Name**. This is the FQDN that was mapped to the customer DNS in step 2 on page 21.
 - k. Select Save

	MAC AUTHENTICATION			
Interprise WPA/WPA2/WPA3	O Personal WPA / WPA2 / WPA3	👌 Private Pre-Shared Key	. WEP	P Open Unsecured
nable Canthus Web Dostal	sec 1			,
nable ExtremeGuest				
ssentials				
dvanced Configuration	n -			
onfigure your Security Settings				
ecurity	Enable HTTPS			
ecurity	Enable HTTPS HTTPS certificate Guest-Cert.pem *			
scurity	Enable HTTPS HTTPS certificate Guest -Cert.pem			
scurity	Enable HTTPS HTTPS certificate Guest-Cert.pem Webserver Domain Name guest.iqe-ext.com			
ecurity	Enable HTTPS HTTPS certificate Guest-Cert.pom Webserver Domain Name guest.lge-ext.com			
valled Garden	Enable HTTPS HTTPS certificate Guest-Cert.pem Webserver Domain Name iguest.iqe-ext.com			
valled Garden	Enable HTTPS HTTPS certificate Guest-Cert.pom Webserver Domain Name guest.lge-ext.com			

Continue with the common setup based on the guest use case.