How To:

FortiGate Guest Network using HPE Aruba ClearPass for captive portal

Version	Date	Modified by	Comments
1.0	22.12.2023	Anders Lagerqvist Ulises Cazares	First version using FortiOS 7.4.1 and ClearPass 6.11.6

How to create a guest SSID on FortiGate with ClearPass captive portal

The goal of this document is to guide you through the steps required to implement a guest network solution based on Fortinet FortiOS 7.4.1 using a tunneled SSID with HPE Aruba ClearPass version 6.11.6. It is expected that this setup will remain relevant also for other recent versions.

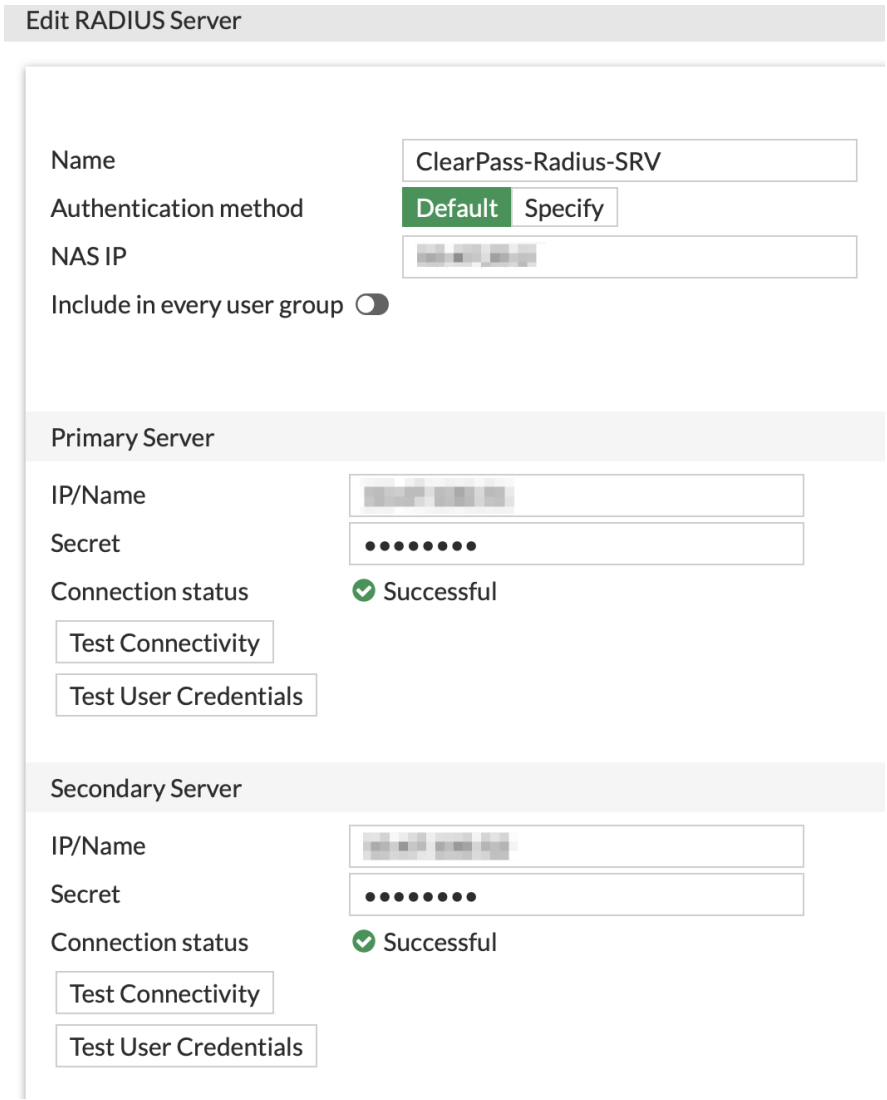
This document does not cover using a bridge mode SSID.

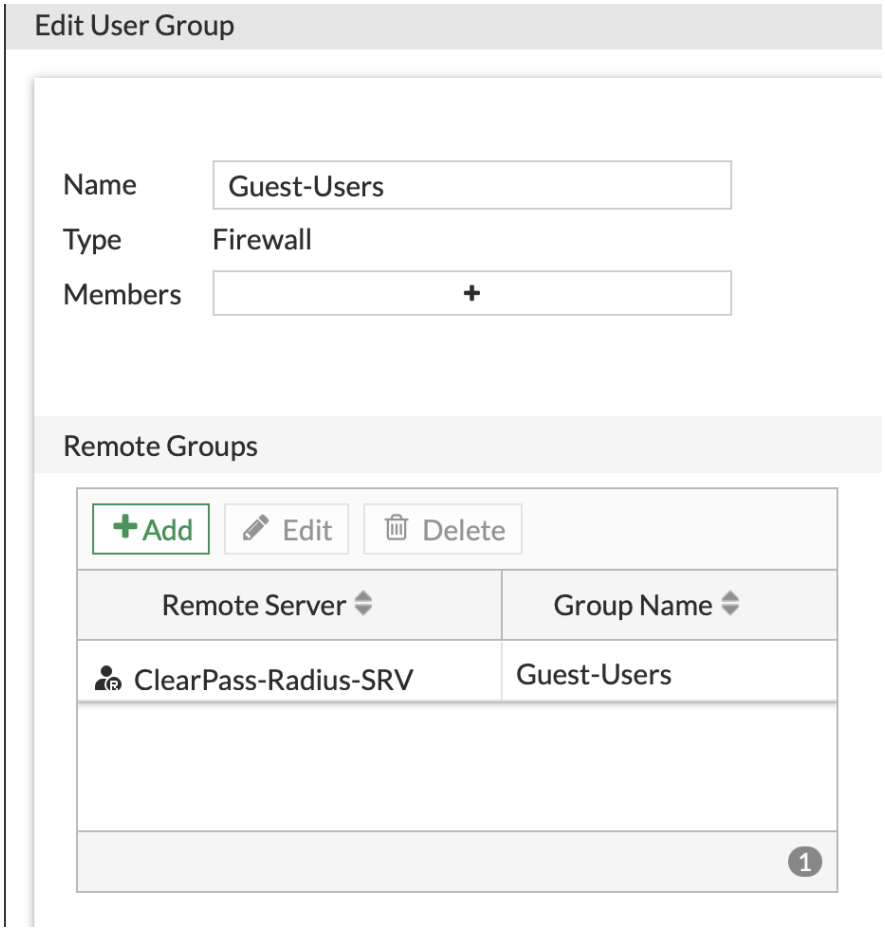
As this document does not to go into all details on how to configure a FortiGate or ClearPass, it is expected that the reader already has basic knowledge of these products.

It is a prerequisite to have proper certificates signed by a public CA (Certificate Authority) installed on both the FortiGate and on the ClearPass guest portal to avoid client warnings when they connect to the guest network. The certificate may be a wildcard certificate or unique to the two devices. Failing to use a public signed certificate may cause connection warnings and failure to successfully connect to the guest network.

Required configuration on the FortiGate:

First step is to create ClearPass as a RADIUS server for the MAC-caching part and create the user-group that ClearPass should return after authentication is successful, in this example it is “Guest-Users”.





Next step is to create the SSID with the desired names and features. In this example the FortiGate will also act as DHCP server for the guest users.

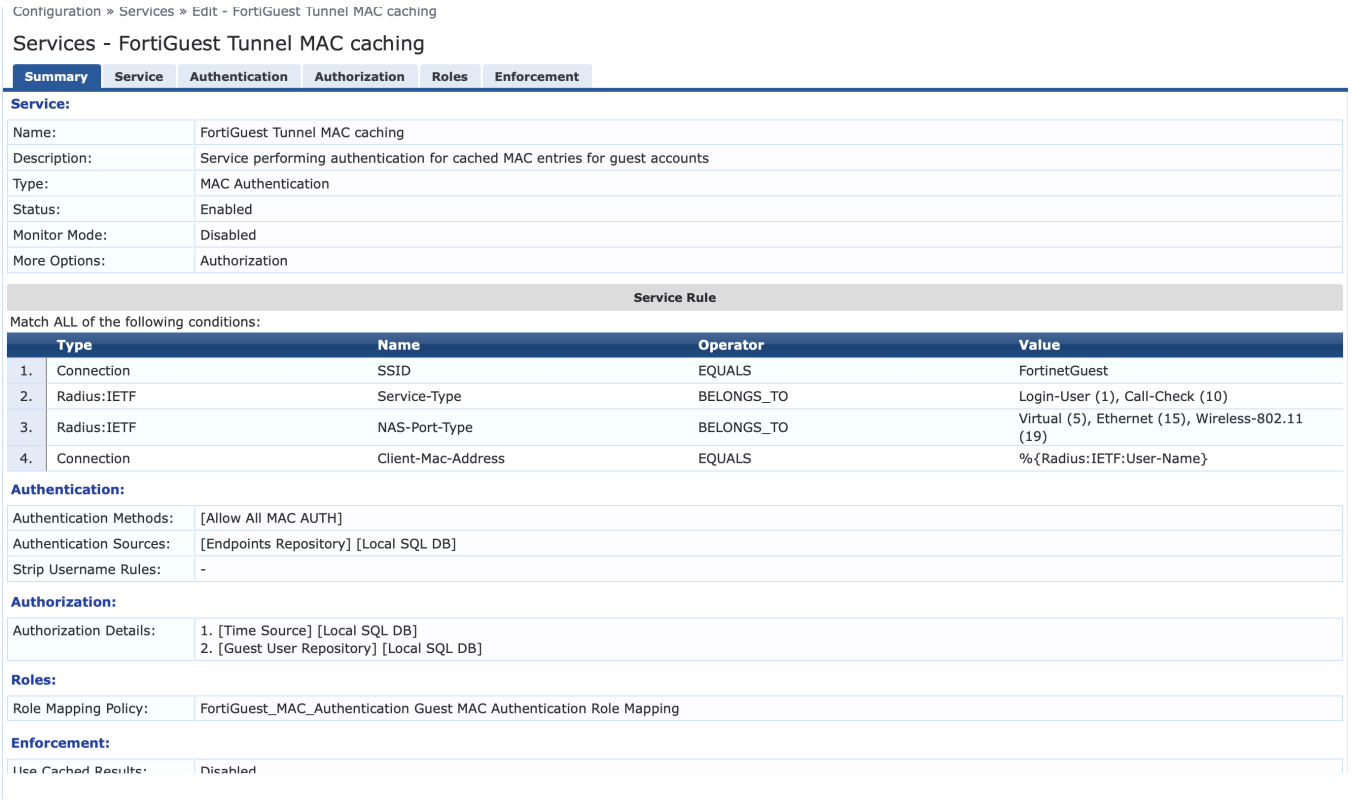
```
config wireless-controller vap
   edit "FortinetGuest"
      set ssid "FortinetGuest"
      set security captive-portal
      set external-web "fqdn-to-clearpass-guest-portal/guest/pagename.php"
      set mac-auth-bypass enable <- This is to allow MAC caching
      set selected-usergroups "Guest-Users"
      set security-exempt-list "FortinetGuest-exempt-list" <- This should allow http/https, dns etc to resolve
the ClearPass server and any other exempt services being allowed before signing on to the guest network.
      set schedule "always"
   next
end
```

This is pretty much all on the FortiGate SSID configuration done, but you must also create the firewall policy to allow the guest users to connect to the ClearPass servers, to the Internet, and any other destinations after successful authentication on the ClearPass portal.

Required configuration on the ClearPass guest portal:

You need to create two services in ClearPass Policy Server, one for the MAC caching, and one for the guest registration, in that order.

This is the MAC caching service:



Configuration » Services » Edit - FortiGuest Tunnel MAC caching

Services - FortiGuest Tunnel MAC caching

Summary | Service | Authentication | Authorization | Roles | Enforcement

Service:

Name:	FortiGuest Tunnel MAC caching
Description:	Service performing authentication for cached MAC entries for guest accounts
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	Disabled
More Options:	Authorization

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Connection	SSID	EQUALS	FortinetGuest
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Virtual (5), Ethernet (15), Wireless-802.11 (19)
4.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}

Authentication:

Authentication Methods:	[Allow All MAC AUTH]
Authentication Sources:	[Endpoints Repository] [Local SQL DB]
Strip Username Rules:	-

Authorization:

Authorization Details:	1. [Time Source] [Local SQL DB] 2. [Guest User Repository] [Local SQL DB]

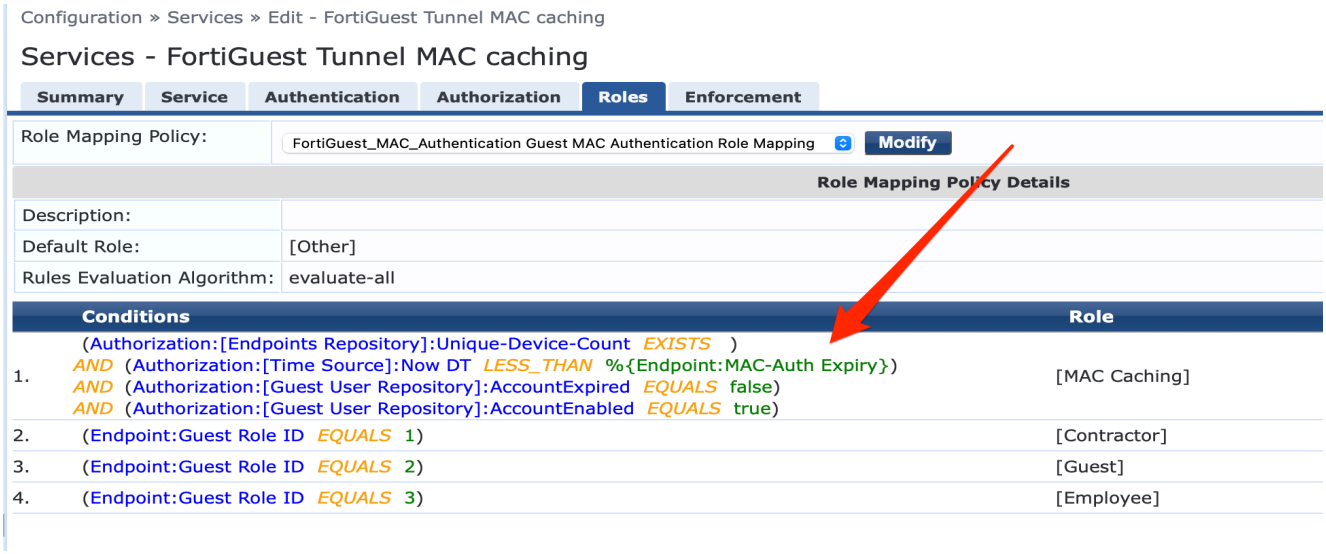
Roles:

Role Mapping Policy:	FortiGuest_MAC_Authentication Guest MAC Authentication Role Mapping

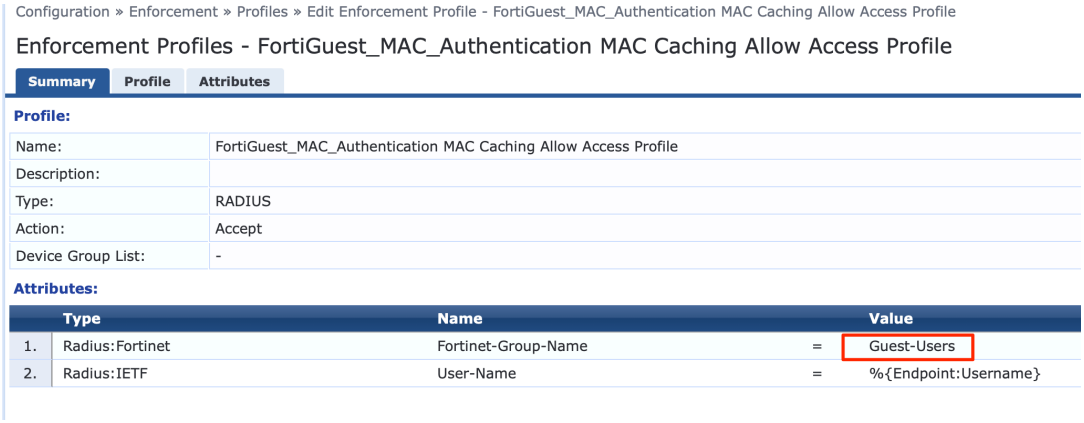
Enforcement:

Use Cached Results:	Disabled

The role mapping shown to allow the “MAC Caching” role, rest is same as regular guest role mapping.



The enforcement policy to allow access without requiring Captive Portal if you already have a valid guest account is shown here:



Note the “Guest-Users” being sent, need to match what you created on the FortiGate earlier. Also sending the User-Name to see that on the FortiGate when looking at the users.

The 2nd service to use the Captive Portal is shown here:

Configuration » Services » Edit - FortiGuest Tunnel Guest Registration

Services - FortiGuest Tunnel Guest Registration

Summary | Service | Authentication | Authorization | Roles | Enforcement | Accounting Proxy

Service:

Name:	FortiGuest Tunnel Guest Registration
Description:	Service for guest access via captive portal (non-802.1x)
Type:	RADIUS Enforcement (Generic)
Status:	Enabled
Monitor Mode:	Disabled
More Options:	1. Authorization 2. Accounting Proxy

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	Connect-Info	EQUALS	web-auth
2.	Radius:IETF	Service-Type	EQUALS	Login-User (1)
3.	Radius:IETF	NAS-IP-Address	BELONGS_TO_GROUP	Fortinet Devices

Authentication:

Authentication Methods:	1. [PAP] 2. [MSCHAP] 3. [CHAP]
Authentication Sources:	[Guest User Repository] [Local SQL DB]
Strip Username Rules:	-
Service Certificate:	-

Authorization:

Authorization Details:	1. [Endpoints Repository] [Local SQL DB] 2. [Guest User Repository] [Local SQL DB]

Roles:

Role Mapping Policy:	FortiGuest_MAC_Authentication Guest MAC Authentication Role Mapping

Note the NAS-IP-Address where the FortiGate is included in the group.

Standard guest role mapping rule:

Configuration » Services » Edit - FortiGuest Tunnel Guest Registration

Services - FortiGuest Tunnel Guest Registration

Summary | Service | Authentication | Authorization | Roles | Enforcement | Accounting Proxy

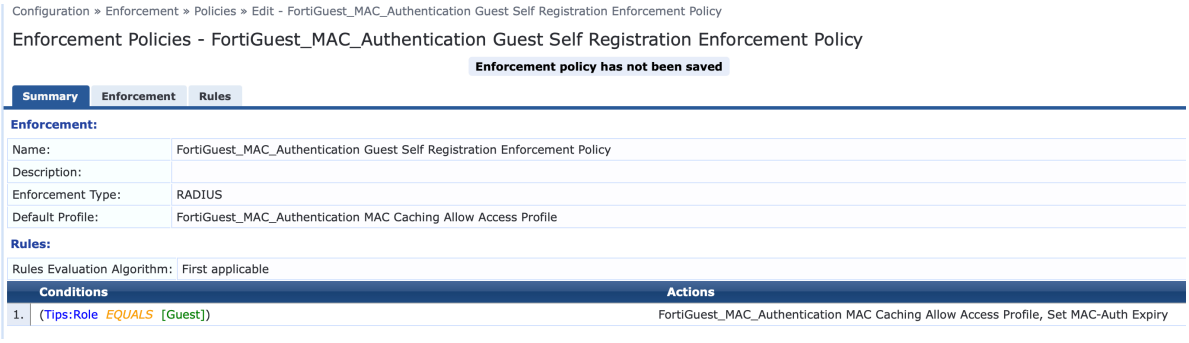
Role Mapping Policy:	FortiGuest_MAC_Authentication Guest MAC Authentication Role Mapping [Modify]

Role Mapping Policy Details

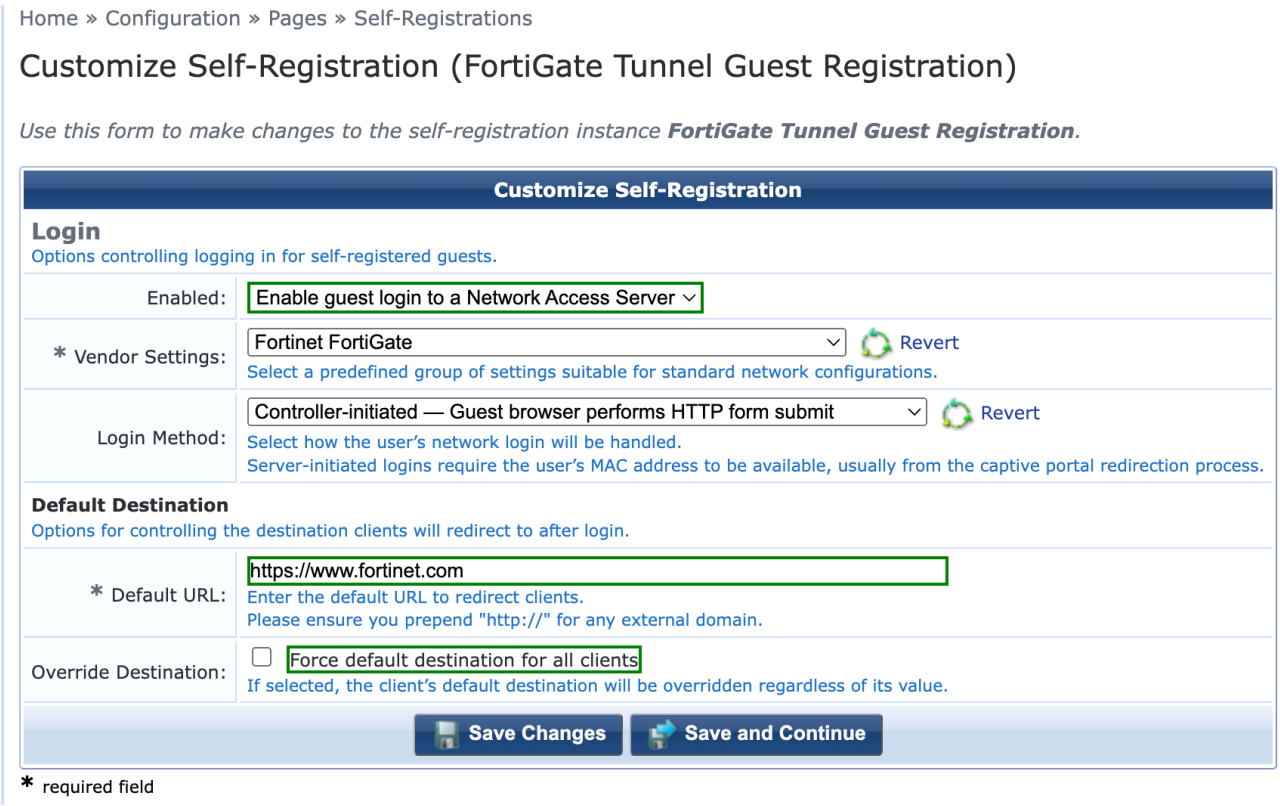
Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	evaluate-all

	Conditions	Role
1.	(Authorization:[Endpoints Repository]:Unique-Device-Count *EXISTS*) *AND* (Authorization:[Time Source]:Now DT *LESS_THAN* %{Endpoint:MAC-Auth Expiry}) *AND* (Authorization:[Guest User Repository]:AccountExpired *EQUALS* false) *AND* (Authorization:[Guest User Repository]:AccountEnabled *EQUALS* true)	[MAC Caching]
2.	(Endpoint:Guest Role ID *EQUALS* 1)	[Contractor]
3.	(Endpoint:Guest Role ID *EQUALS* 2)	[Guest]
4.	(Endpoint:Guest Role ID *EQUALS* 3)	[Employee]

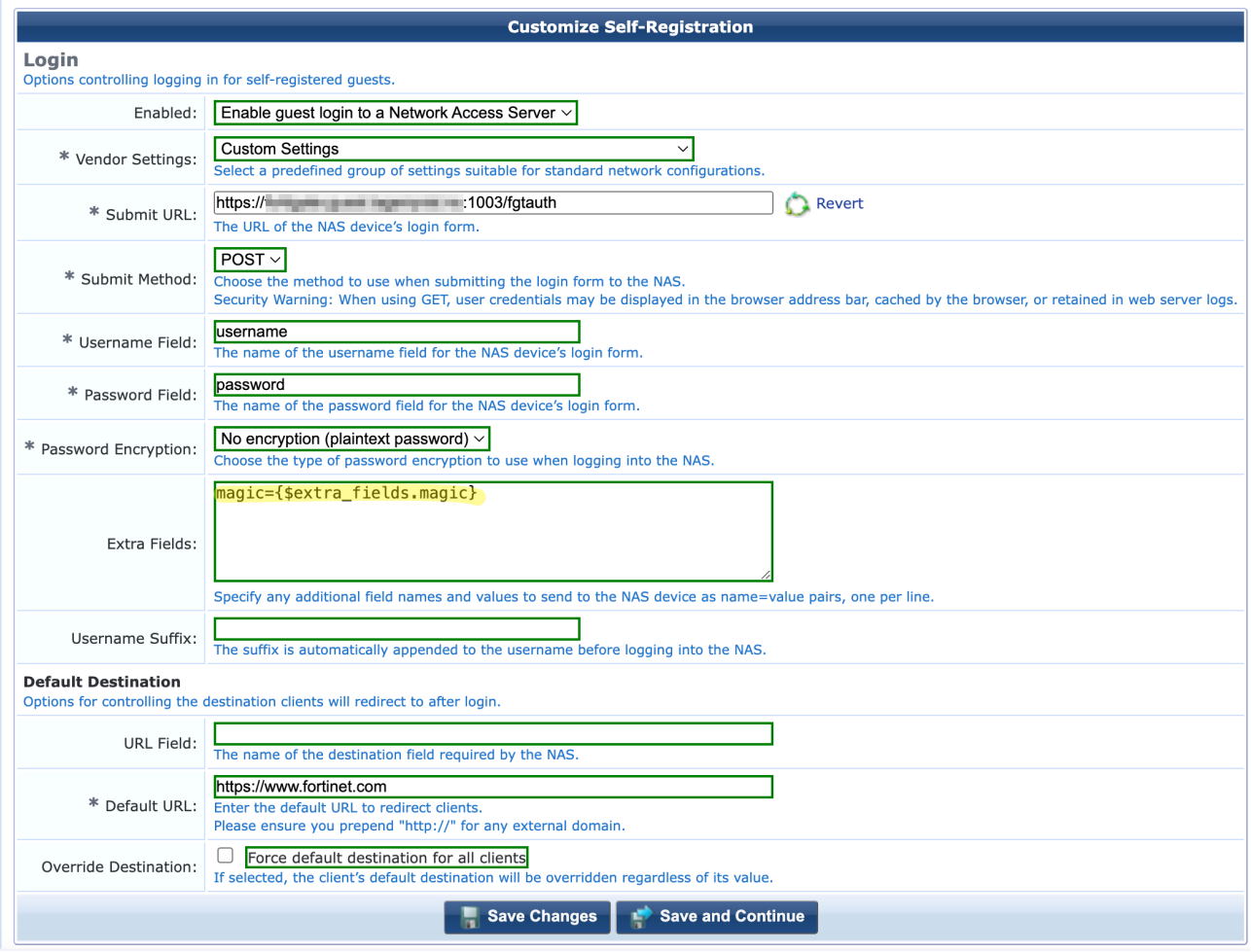
Standard guest enforcement, which sends over the “Guest-User” to FortiGate and updates the account expiration time:



For the guest portal settings, you decide if you want sponsor based, send SMS etc like always, and for the NAS vendor settings, you can just use the default Fortinet FortiGate:



It is still possible to use the previously used “Custom” settings, but if so, must add the details in the “Extra Fields” settings like this:



Note that the “Submit URL:” is the IP or FQDN of the FortiGate guest interface. It is highly recommended to use https and port 1003 for the captive portal, but if you are using http, ensure that the port number used is 1000.