🌐 MoFi 6500 Captive Portal

Complete Administrator Guide & Documentation

Version 2025.1 - September 18, 2025

📖 Overview

What is the MoFi Captive Portal?
A guest network management system that controls WiFi access by requiring users to view a splash page before accessing the internet.

🎨 Modern Design
Beautiful 2025-style responsive splash pages that work on all devices

🔐 Dual Authentication
Click-to-continue or password-protected access modes

🚫 Website Filtering
Built-in blocking for high-bandwidth streaming services

📊 Live Statistics
Real-time user count and connection information

🛠️ Easy Management
Web-based configuration with clear explanations

📱 Mobile Ready
Optimized for smartphones and tablets

🔧 System Components

- **Captive Portal Engine:** Core authentication system
- **Router Firmware:** Linux-based operating system
- **LuCI:** Web interface framework
- **iptables:** Network traffic control
- **Custom Templates:** Modern splash page designs

🚀 Quick Start Guide

Get your captive portal running in 5 minutes!

Step 1: Access Router Admin

```
URL: http://192.168.10.1 Username: root Password: admin
```

Step 2: Navigate to Captive Portal

Go to **Network** → **Captive Portal**
You'll see three main tabs:

- **Configuration:** Main settings and ACL rules
- **Splash Page Editor:** Customize content
- **Website Block List:** Manage filtering

Step 3: Basic Configuration

1. Check ✅ **"Enable Captive Portal"**
2. Select WiFi interfaces (default: guest networks)
3. Set authentication mode:
   - **No Password:** Leave "Portal Password" empty
   - **Password:** Enter password in "Portal Password" field
4. Click **"Save & Apply"**

Step 4: Test the System

1. Connect a device to guest WiFi
2. Open any website (like google.com)
3. Verify splash page appears
4. Complete authentication process
5. Confirm internet access works

⚠️ **Important:** Enabling captive portal disables hardware NAT acceleration. Apply only to guest networks for best performance.

⚙️ Configuration Options

Complete GUI Coverage: This documentation covers ALL 18 configuration options available in the MoFi Captive Portal GUI interface.

Basic Settings

Setting	Description	Default	Recommendations
Enable Captive Portal	Master on/off switch	Disabled	Enable for guest networks only
WiFi Interfaces	Which networks use portal (Multi-select)	default_ra, public2g, default_rax, public5g	Use public2g, public5g for guests only
Block High Bandwidth Websites	Enable streaming service filtering	Disabled	Enable for public WiFi to preserve bandwidth
Block GUI Access from Captive Portal	Prevent portal users from accessing router admin	Disabled	Enable for security. Alternative: http://192.168.5.1:1080
Gateway Name	Name shown to users (used as $gatewayname variable)	"Mofi Captive Portal"	Use your business/location name
Maximum Clients	Concurrent user limit	250	Set based on bandwidth capacity and router performance

Timeout Settings

Setting	Description	Default	Use Cases
Client Idle Timeout	Disconnect inactive users	1200 min (20 hrs)	60-240 min for high-turnover areas
Session Timeout	Maximum session length	1440 min (24 hrs)	480 min (8 hrs) for daily access

Advanced Settings

Setting	Description	Default	Use Cases
Debug Level	Verbosity of logging (0-3). Higher = more verbose	1	Set to 2-3 for troubleshooting issues
Enable Client Logging	Log all client authentication events	Disabled	Enable for monitoring and compliance
Redirect URL	URL to redirect users after authentication	Empty (stay on current page)	Example: http://www.mofinetwork.com
Portal Password	Password required for access (empty = click-to-continue)	Empty	Use "system" for admin bypass, custom for guests

Security Options

🔑 Portal Password
Empty: Click-to-continue mode
Set: Password required for access
Special: Use "system" for admin bypass

🚫 Block GUI Access
Prevents portal users from accessing router admin
Alternative: http://192.168.5.1:1080

🌐 Website Blocking
Filter high-bandwidth streaming services
Configure in "Website Block List" tab

🔐 Access Control Lists (ACL Rules)

Important: These are captive portal access controls that apply to different traffic paths. Each rule type controls different network flows and they operate independently.

⚠️ **Key Concept:** ACL rules use separate network traffic paths:

- **Authenticated Users:** Controls traffic THROUGH router to internet
- **Router Access:** Controls traffic TO router admin interface (192.168.10.1)
- **Pre-Authenticated:** Controls traffic before splash page completion

1. Authenticated Users

When Applied: Internet traffic THROUGH the router after completing captive portal
Traffic Path: Client → Router → Internet (FORWARD chain)

```
# Current Default Rules: block to 192.168.0.0/16 # Block other home networks (NOT this router) block to
10.0.0.0/8 # Block corporate networks (10.x.x.x) allow tcp port 22 # SSH access allow tcp port 53 # DNS
queries (TCP) allow udp port 53 # DNS queries (UDP) allow tcp port 80 # HTTP websites allow tcp port 88 #
Router management allow tcp port 443 # HTTPS websites
```

Result: Users can browse internet but cannot access other network segments. Router admin access (192.168.10.1) is controlled by separate Router Access rules.

2. Pre-Authenticated Users

When Applied: Users connected to WiFi but haven't completed the captive portal yet

```
# Current Default Rules: allow tcp port 53 # DNS queries (TCP) - needed for redirection allow udp port 53 #
DNS queries (UDP) - needed for redirection
```

Purpose: Only DNS is allowed so users can type "google.com" and get redirected to the captive portal, but they can't actually browse anything.

3. Router Access Users

When Applied: Direct access TO the router admin interface (192.168.10.1)
Traffic Path: Client → Router Admin (INPUT chain)
Key Point: These rules are completely separate from Authenticated Users rules and apply when visiting 192.168.10.1

```
# Current Default Rules: allow tcp port 22 # SSH to router (192.168.10.1:22) allow tcp port 23 # Telnet to
router allow tcp port 53 # DNS queries to router allow udp port 53 # DNS queries to router allow udp port 67 #
DHCP requests to router allow tcp port 80 # Router web interface (HTTP) allow tcp port 88 # Router management
services allow tcp port 443 # Router web interface (HTTPS)
```

Why Separate Rules: This is why you can access 192.168.10.1 admin even with "block to 192.168.0.0/16" in Authenticated Users - they control different traffic paths (TO router vs THROUGH router).

Rule Format Examples

Rule	Meaning	Use Case
`allow tcp port 80`	Allow HTTP web browsing	Basic internet access
`allow tcp port 443`	Allow HTTPS secure browsing	Secure websites
`block to 192.168.10.0/24`	Block access to main LAN	Security isolation
`allow tcp port 22`	Allow SSH connections	Admin access

Common Port Numbers

Web Services

- **Port 80:** HTTP (websites)
- **Port 443:** HTTPS (secure websites)
- **Port 8080:** Alternative HTTP

Network Services

- **Port 53:** DNS (name resolution)
- **Port 67:** DHCP (IP assignment)
- **Port 123:** NTP (time sync)

Admin Services

- **Port 22:** SSH (secure shell)
- **Port 23:** Telnet (insecure shell)
- **Port 88:** Router management

MAC Address Control

Control which devices can access the captive portal based on their hardware MAC address.

Setting	Description	Format	Use Case
MAC Address Control	Choose "Allow" (whitelist) or "Block" (blacklist) mode	Dropdown selection	Security/access control policy
Allowed MAC Addresses	Only these devices can see captive portal (whitelist mode)	aa:bb:cc:dd:ee:ff	Restricted access environments
Blocked MAC Addresses	These devices are denied captive portal access (blacklist mode)	aa:bb:cc:dd:ee:ff	Ban problematic devices
Trusted MAC Addresses	These devices bypass captive portal entirely (immediate internet access)	aa:bb:cc:dd:ee:ff	Staff devices, IoT devices, printers

MAC Address Format: Use colon-separated format like `aa:bb:cc:dd:ee:ff`. You can find device MAC addresses in router's DHCP client list or device network settings.

Complete GUI Options Summary

Tab	Total Options	Option Names
Configuration	18 options	Enable Portal, WiFi Interfaces, Block Websites, Block GUI, Gateway Name, Max Clients, Idle Timeout, Session Timeout, Debug Level, Logging, Redirect URL, Password, Auth Users (ACL), Pre-Auth Users (ACL), Router Users (ACL), MAC Control, Allowed MACs, Blocked MACs, Trusted MACs
Splash Page Editor	1 option	Splash Page HTML Content (full HTML editor with template variables)
Website Block List	1 option	Blocked Domains List (domain names, one per line)

🔑 Authentication Modes

Mode 1: Click-to-Continue (No Password)

Configuration

Leave "Portal Password" field **empty**

User Experience

1. Connect to WiFi network
2. Open any website
3. See splash page with "Accept & Continue" button
4. Click button to get internet access

Best For

- Public spaces (cafes, libraries)
- High-traffic guest networks
- Minimal friction requirements

Mode 2: Password Authentication

Configuration

Enter password in "Portal Password" field

User Experience

1. Connect to WiFi network
2. Open any website
3. See splash page with password form
4. Enter the shared password
5. Click "Continue to Internet"

Best For

- Business guest networks
- Controlled access environments
- Temporary access codes

Special Passwords

Password	Effect	Session Timeout	Use Case
`system`	Unlimited access	No timeout	Admin/staff devices
Custom password	Normal access	Configured timeout	Guest users

🎨 Splash Page Customization

Available Templates

splash.html
Mode: Click-to-continue
Features: Modern design, terms & conditions, user statistics

splash_sitewide.html
Mode: Password authentication
Features: Password form, security focus, professional layout

Current Design Features

- ✅ **2025 Modern Styling:** Gradients, rounded corners, shadows
- ✅ **Mobile Responsive:** Perfect on all screen sizes
- ✅ **Live Statistics:** Shows current user count
- ✅ **Professional Branding:** MoFi logo and corporate appearance
- ✅ **Terms & Conditions:** Collapsible legal text
- ✅ **Connection Info:** User IP and gateway details

Customization Options

Access: Go to "Splash Page Editor" tab in captive portal configuration

Full HTML Editing

- Complete HTML/CSS control
- Syntax highlighting editor
- Real-time preview

Template Variables

- Dynamic content insertion
- Live data display
- Automatic updates

Image Support

- Logo customization
- Background images
- Brand assets

📊 Template Variables

Template variables are dynamic placeholders that get replaced with live data when users see the splash page.

Basic Variables

Variable	Description	Example Output
`$gatewayname`	Gateway name from config	"MoFi Guest Network"
`$authtarget`	Click-to-continue URL	"http://192.168.5.1:2050/auth/?token=abc123"
`$authaction`	Password form action URL	"http://192.168.5.1:2050/auth/"
`$imagesdir`	Images directory path	"images"

Client Information

Variable	Description	Example Output
`$clientip`	User's IP address	"192.168.5.156"
`$clientmac`	User's MAC address	"aa:bb:cc:dd:ee:ff"
`$clienttoken`	Unique session token	"abc123def456"

Gateway Statistics

Variable	Description	Example Output
`$nclients`	Current connected users	"15"
`$maxclients`	Maximum allowed users	"250"
`$uptime`	Router uptime	"2 days, 14:32:05"

Usage Examples

```
<!-- Display gateway name --> <h1>$gatewayname</h1> <!-- Show connection statistics --> <p>Users Online:
$nclients / $maxclients</p> <!-- Display user information --> <p>Your IP: $clientip</p> <!-- Create continue
button --> <a href="$authtarget">Continue to Internet</a> <!-- Password form --> <form action="$authaction">
<input type="hidden" name="tok" value="$tok"> <input type="password" name="password" required> <button
type="submit">Connect</button> </form> <!-- Add logo --> <img src="$imagesdir/mofi_banner.gif" alt="Logo">
```

Current Implementation: The MoFi splash pages use $nclients/$maxclients to show live user count and $clientip to display connection info in the footer.

🚫 Website Blocking

How Website Blocking Works

1. Enable "Block High Bandwidth Websites" in main configuration
2. Configure blocked domains in "Website Block List" tab
3. Blocked sites return error pages instead of loading
4. Changes take effect immediately (no restart required)

Default Blocked Services

Video Streaming

- Netflix (netflix.com)
- YouTube (youtube.com, youtu.be)
- Hulu (hulu.com)
- Disney+ (disneyplus.com)
- Amazon Prime Video

Live Streaming

- Twitch (twitch.tv)
- Facebook Live
- Instagram Live
- TikTok videos

File Sharing

- Dropbox large files
- Google Drive videos
- OneDrive media
- Torrent sites

Adding Custom Blocks

```
# Domain Format (one per line): example.com subdomain.example.com social-media-site.com # Wildcard Examples:
youtube.com # Blocks ALL YouTube subdomains facebook.com # Blocks ALL Facebook subdomains *.streaming.com #
Blocks all subdomains
```

Performance Note: Website blocking adds minimal overhead but extensive lists (100+ domains) may impact performance on high-traffic networks.

🔧 Troubleshooting

Common Issues & Solutions

❌ Captive Portal Not Appearing

Symptoms: Users connect to WiFi but don't see splash page
Solutions:

1. Verify "Enable Captive Portal" is checked
2. Confirm correct WiFi interfaces selected
3. Try with different device or incognito browser
4. Check service status: `ssh root@192.168.10.1 "/etc/init.d/captiveportal status"`
5. Restart service: `ssh root@192.168.10.1 "/etc/init.d/captiveportal restart"`

❌ Password Authentication Failing

Symptoms: Correct password is rejected
Solutions:

1. Check password spelling and case sensitivity
2. Avoid complex special characters
3. Clear browser cache or use incognito mode
4. Verify password is saved in configuration

❌ No Internet After Authentication

Symptoms: Splash page works but no internet access
Solutions:

1. Check ACL rules for authenticated users
2. Ensure ports 80 and 443 are allowed
3. Verify DNS rules in pre-authenticated users
4. Test router's own internet connectivity

❌ High CPU Usage / Slow Performance

Symptoms: Router becomes slow or unresponsive
Solutions:

1. Reduce maximum clients setting
2. Implement shorter session timeouts
3. Optimize website block lists
4. Apply captive portal to fewer interfaces

Log File Locations

Log Type	Location	Contents
Captive Portal	`/tmp/ndslog.log`	Authentication events, client connections
System	`/var/log/messages`	General system events and errors
Authentication	`/tmp/binauth.log`	Password authentication attempts

Debug Commands

```
# Check service status ssh root@192.168.10.1 "/etc/init.d/captiveportal status" # View real-time logs ssh
root@192.168.10.1 "tail -f /tmp/ndslog.log" # List current clients ssh root@192.168.10.1 "ndsctl clients" #
Check configuration ssh root@192.168.10.1 "uci show captiveportal" # Test DNS resolution ssh root@192.168.10.1
"nslookup google.com"
```

✅ Best Practices

🔒 Security Recommendations

Password Management

- Change passwords regularly (monthly)
- Use strong passwords (8+ characters)
- Document password changes for staff
- Use "system" password for admin devices

Network Isolation

- Block private networks (192.168.x.x, 10.x.x.x)
- Limit router access from guest networks
- Use MAC filtering for sensitive environments
- Monitor connected devices regularly

Access Control

- Use appropriate timeout settings
- Limit concurrent users based on capacity
- Implement fair usage policies
- Regular security audits of ACL rules

⚡ Performance Optimization

Client Management

- Set realistic maximum client limits
- Use 60-240 minute timeouts for most cases
- Monitor concurrent user patterns
- Adjust limits based on usage data

Resource Usage

- Apply to guest networks only
- Monitor CPU and memory usage
- Optimize block lists (essential only)
- Schedule maintenance during low usage

👤 User Experience

Splash Page Design

- Keep authentication process simple
- Ensure mobile-first design
- Provide clear instructions
- Maintain professional appearance

Terms & Conditions

- Use clear, understandable language
- Keep policies reasonable and fair
- Update terms regularly
- Ensure local law compliance

📅 Maintenance Schedule

Frequency	Tasks	Time Required
Daily	Monitor user count, check alerts, verify connectivity	5 minutes
Weekly	Review logs, update block lists, check performance	15 minutes
Monthly	Rotate passwords, update terms, backup config, security audit	30 minutes
Quarterly	Full system review, firmware updates, performance optimization	1-2 hours

📊 Recommended Settings by Environment

Environment	Authentication	Session Timeout	Max Clients	Website Blocking
Coffee Shop	Click-to-continue	120 minutes	50-100	Enable (streaming)
Hotel	Room number password	24 hours	200-500	Selective
Office Guest	Daily password	8 hours	25-50	Enable (social media)
Library	Click-to-continue	240 minutes	100-200	Enable (gaming/streaming)

📞 Support & Resources

Documentation
Repository: Mofi-Network-Inc/mofi6500-lintel-20231128
Path: /docs/MoFi_Captive_Portal_Complete_Guide.htm
Version: 2025.1 (September 18, 2025)

Router Access
LAN Interface: http://192.168.10.1
Alternative (when blocked): http://192.168.5.1:1080
SSH: ssh root@192.168.10.1

Quick Reference
Service Control: /etc/init.d/captiveportal
Config File: /etc/config/captiveportal
Templates: /etc/captiveportal/htdocs/

Latest Updates (2025.1): Modern splash page design, enhanced template variables, comprehensive ACL explanations, live statistics display, improved mobile responsiveness.

© 2025 MoFi Network Inc.
This documentation is provided for MoFi 6500 router administrators
Generated on September 18, 2025 | Version 2025.1