

# FAQ Maxwell - HTTP Digest

## Introduction

To ensure that a device is right device that is allowed to download the provisioning file, the access to the (HTTP(S))provisioning server can be protected using HTTP Digest.

A username and password can be used to confirm the identity of a user before sending sensitive information.

| Valid for Maxwell |   |   |   |
|-------------------|---|---|---|
| Basic             | 2 | 3 | 4 |

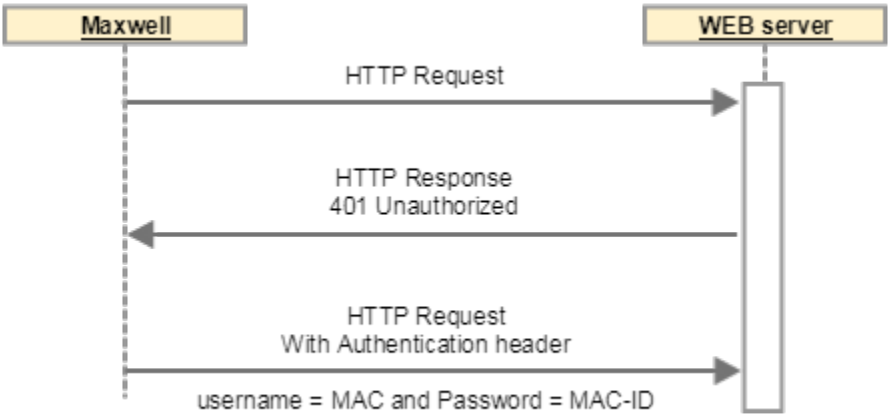
## 1. Normal HTTP Digest Authentication Scheme

1. The Maxwell sends the server a request to download the provisioning template.
2. The WEB-server receives the request and requires an authentication. The WEB-server checks if the authentication information is in the request. Because this is the first request, there is no authentication information available. The WEB-server responds returning an 401 Unauthorized.
3. The client receives the WEB-server challenge and gathers the required credentials. A new request is sent containing the username and hashed secret key.

Username = Maxwell MAC address (12 Digits)  
Password = Maxwell MAC-ID (12 Digits)

The MAC-ID can be collected when you register the device to the [Gigaset Re-direct server](#).

4. When username and password are correct, the provisioning template is downloaded.



## 2. First Authentication fails

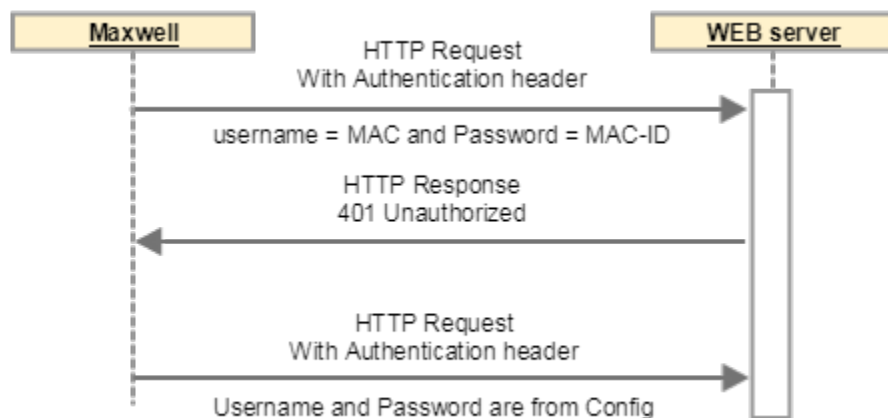
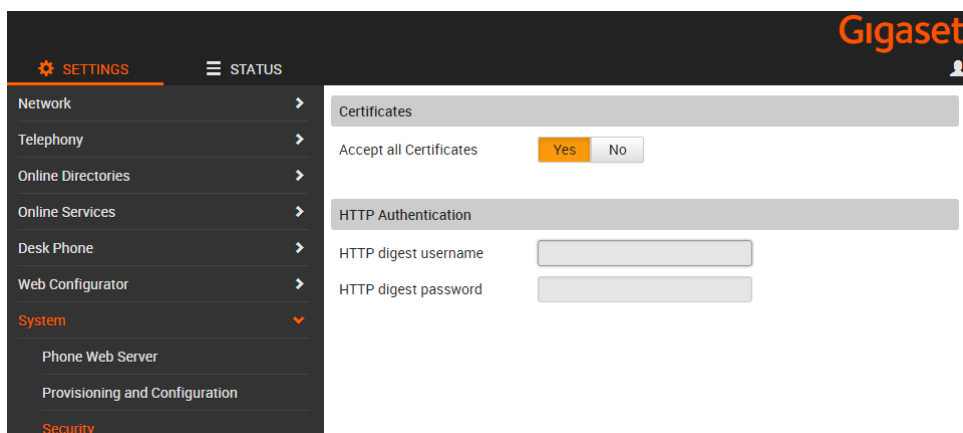
1. The client receives the WEB-server challenge and gathers the required credentials. A new request is sent containing the username (MAC address) and hashed secret key (MAC-ID).
2. The WEB-server receives the request and requires an authentication. The WEB-server checks if the authentication information is in the request. The wrong authentication information is available. The WEB-server responds returning an 401 Unauthorized.
3. The client receives the WEB-server challenge and gathers the required credentials coming from the device configuration. A new request is sent containing the username and hashed secret key.

Username = **Settings - System - Security - HTTP digest**

**username**

Password = **Settings - System - Security - HTTP digest**

**password**



## 3. Second Authentication fails

This functionality is available from Software 2.18.3 or higher.

1. The client receives the WEB-server challenge and gathers the required credentials coming from the device configuration. A new request is sent containing the username and hashed secret key.
2. The WEB-server receives the request and requires an authentication. The WEB-server checks if the authentication information is in the request. The wrong authentication information is available. The WEB-server responds returning an 401 Unauthorized.
3. On the Maxwell display, the user can add the Username and Password Manually.

### Provisioning Authentication

Username

15:24  
25.04.2017

Password

Abc

Back

Save

If you press **"No"** key then menu will be gone after 60 seconds.

If you press **"Any"** key then 60 seconds timer will be set to 0 again, 60 seconds after pressing the last key, the menu will be gone.

To start provisioning using these credentials, you need to press the **"Save"** key.

You can try 3 times, will still fails, the menu will be gone. You need to reboot or press provisioning in web-interface to get menu again.

If the entry is correct, the username and password is stored in the web-interface:

SETTINGS

STATUS

Network

Telephony

Online Directories

Online Services

Desk Phone

Web Configurator

System

Phone Web Server

Provisioning and Configuration

Security

Certificates

Accept all Certificates 

Yes

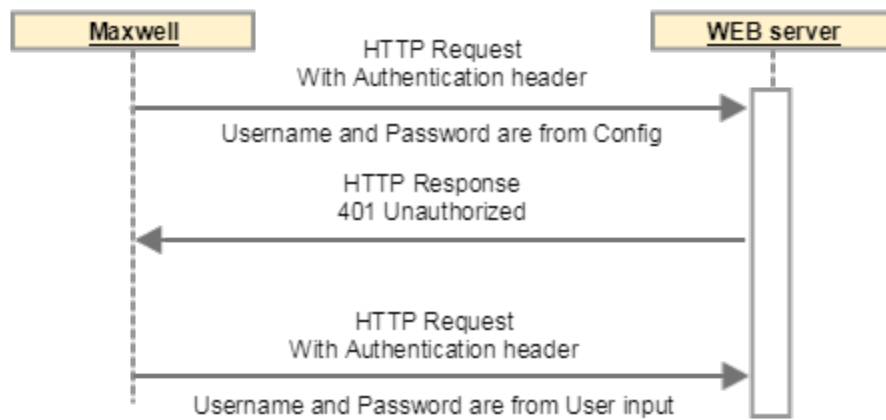
No

HTTP Authentication

HTTP digest username

HTTP digest password

Gigaset



### Provisioning

The following provisioning Parameters are available, these values are used in step 3.

#### Web-interface: Settings - System - Security

|                                  |                      |
|----------------------------------|----------------------|
| System.Security.HTTPAuthUsername | HTTP Digest username |
| System.Security.HTTPAuthPassword | HTTP Digest password |

### Redirect server

From software 2.25, it is possible to enter the HTTP Digest username and Password via the redirect server.

http://<HTTP digest username>:<HTTP digest password>@<provisioning URL>

MAC-ID: 7C2F80123456-1234

URL: http://Username:Password@prover.url/dms/gigasetmaxwell/7c2f809 ▼

Provider: ▼

### Broadsoft

When connected to Broadsoft, the HTTP Digest username and password in the Broadsoft web-interface can be found:

Go to: **Users - Profile - Addresses - Configure Identify/Device Profile - Authentication**

#### Authentication

☐ Use Identity/Device Profile Type Credentials

☒ Use Custom Credentials

\* Device Access User Name: 21051972

\* Device Access Password:

\* Re-type Device Access Password: