Auto provisioning: HTTP Digest

Introduction

HTTP Digest access authentication is one of the agreed-upon methods a device can use to negotiate credentials with a HTTP server to increase the security. This extra security can also be used during the HTTP Auto provisioning process.

HTTP digest is always been available in the Gigaset devices, but with the latest software additional functionality is added.

- N510 BL192 or higher.
- N720 BL84 or higher
- DE900/700 BL02.00.10 or higher
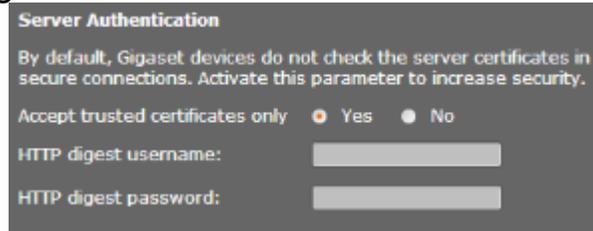- DE410/310 BL02.00.07 or higher

Security

We only support HTTP Digest authentication. Only for testing, the DE devices also can use the HTTP Basic authentication.

Web-Interface configuration

In the webinterface of the device go to: **Settings - Security Settings - Server Authentication.**

Enter the HTTP Digest Username and Password.

Server Authentication

By default, Gigaset devices do not check the server certificates in secure connections. Activate this parameter to increase security.

Accept trusted certificates only   ● Yes   ● No

HTTP digest username:

HTTP digest password:

When the device connects to the Auto provisioning server and will receive the message 401 unauthorised,

The device will try to connect again using the integrated Username and Password.

Then the provisioning server will answer again with the message 401 unauthorised because it is not the correct Username and Password.

The device will try to connect again using the Username and Password you have provided.

The configuration file will be downloaded.

This feature is often used in a Broadsoft Auto provisioning process.

Username and Password via the keypad of the device

Only available in:

- DE900/700 BL02.00.11 or higher
- DE410/310 BL02.00.08 or higher

When the device connects to the provisioning server and the username/password authentication fails, the device will show this in the display of the phone and you can enter these via the keypad of the device.

1. User enters username and password and presses OK; phone tries to authenticate once
2. User leaves it empty and presses OK; phone tries to authenticate once
3. User does nothing and timeout; Phone stops authentication process
4. User presses Back or Cancel; Phone stops authentication process

Phone saves the username and password only when authentication is passed.

N720 auto provisioning parameters

XML syntax:

<SYMB_ITEM ID="BS_IP_Data.aucS_HTTP_DIGEST_USERNAME" class="symb_item" value="broadsoft-username"/>

<SYMB_ITEM ID="BS_IP_Data.aucS_HTTP_DIGEST_PASSWORD" class="symb_item" value="broadsoft-password"/>

Tag Name	Value	Location in web-interface
S_PROV_USERNAME	Max. 50 characters	<S_PROV_USERNAME class="string" value="broadsoft-username"/> Available only when: I_PHONE_SYSTEM=5; symbolic NVM where custom parameter will be stored: BS_IP_Data.aucS_HTTP_DIGEST_USERNAME
S_PROV_PASSWORD	Max. 50 characters	<S_PROV_PASSWORD class="string" value="broadsoft-password"/> Available only when: I_PHONE_SYSTEM=5; symbolic NVM where custom parameter will be stored: BS_IP_Data.aucS_HTTP_DIGEST_PASSWORD
I_PHONE_SYSTEM	0=default setting; 5=Broadsoft	<I_PHONE_SYSTEM class="integer" value="5"/> symbolic NVM where custom parameter will be stored: BS_IP_Data.ucI_PHONE_SYSTEM

- Introduction
- Security
- Web-Interface configuration
- Username and Password via the keypad of the device
- N720 auto provisioning parameters