1 Introduction

Until now, a subscriber's password has also been used for:

- SIP registration
- Access to the web
- API interface

For authentication purposes, PBX access data has to be stored in external systems. This represents a fundamental security risk, due to the fact that these third-party devices often have inadequate security. As a consequence, the access data to our systems might also be compromised.

Implementing these measures is intended to restrict access to our systems.

1.1 Scope of validity of the passwords

A unique password is generated for every external device authorised to access the PBX.

1.2 Single-use passwords

These passwords are generated in accordance with specific guidelines, are between 12 and 16 characters long, and cannot be edited. They are displayed once, when they are created, (only possible via a secure HTTPS connection), and can be saved to a clipboard.
1.3 Levels of authorisation

Subscribers will be able to use their password to access the PBX as before. They will be able to access the web interface and API via digest authentication.

A subscriber-specific web server/API password cannot be used for SIP registration. When the subscriber accesses the web server/API interface, authentication will also be performed by digest, because modifications to sensitive data (e.g. call forwarding) can be made there.

For security reasons, subscribers cannot use their password to access Action URLs. To do this, they must create a separate password that has the appropriate authorisation.

Action URLs can be triggered without digest authentication as soon as a subscriber creates this separate password and enables access to the Action URLs. However, the subscriber's password then also loses its authorisation to log in to the web interface/API. It can then only still be used for SIP registration.

<table>
<thead>
<tr>
<th></th>
<th>Scr. password</th>
<th>API password</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP registration</td>
<td>x</td>
<td>-</td>
</tr>
<tr>
<td>Web interface/API</td>
<td>Digest</td>
<td>Digest</td>
</tr>
<tr>
<td>Action URL</td>
<td>-</td>
<td>Digest or unsecured</td>
</tr>
</tbody>
</table>

1.4 Creating subscriber passwords

Subscribers can create other app-specific passwords.

Web/API password (page Subscriber (scr.) > All subscribers > Subscriber settings > Subscribers may generate own passwords for accessing the web server/API)

Action URLs (page Devices > Action URLs > Action URLs (incoming) > Subscribers may generate own passwords for Action URLs)

If these authorisations are set, the subscriber can create additional passwords or delete existing passwords.

The last password with authorisation to use the Web interface/API cannot be deleted. Only (sub-)administrators can go back to using the original password.

1.5 Creating device passwords

Passwords can also be created for specific devices (page Devices > Action URLs > Action URLs (incoming) > Passwords for accessing Action URLs).

These passwords can only be used to run Action URLs.

1.6 Forcing secure HTTPS connections

To ensure secure access to Action URLs, enable this option by clicking on Administration > IP configuration > Server configuration > Force HTTPS connection.

1.7 Management/administration page

The Devices > Action URLs > Action URLs (incoming) page has these configuration options:

- **Incoming Action URLs enabled**: Enable or disable this option across the entire system
- **Action URLs only within the local network**: Action URLs can only be run from your own network
Subscribers can create their own passwords for access to Action URLs: A subscriber can generate additional passwords or delete existing passwords (page Subscriber (scr.) > Properties > Basic settings). All these passwords are managed in the table. The passwords can be created either for the entire system (Admin, only for Action URLs) or for one specific subscriber (Web interface/API/Action URLs).

1.8 Switching authorisations for subscribers

The subscriber authorisation to switch relays has been expanded to include the switching of both relays and alarms.

Relays that are used in door opener operating mode are configured under Subscriber (scr.) > Properties > Authorisations > Open door.

1.9 Switching authorisations for alarms and relays

Relays and alarms can excluded from the authorisation to switch or control actions via Action URLs on an individual basis, irrespective of the subscriber passwords that have been configured.

Alarms

- Alarm can be triggered by Action URL (page Devices > Alarms > Configure)

Relays (e.g. door opener)

- Relay can be triggered by Action URL (page Devices > Relay (actuators) > Configure)

2 Requirements

Requirement: Firmware 7.0 or above

2.1 Triggering Action URLs as a subscriber

Action URLs

- Incoming Action URLs active/Subscribers may generate own passwords for Action URLs (page Devices > Action URLs)

Alarms

- Alarm can be triggered by Action URL (page Devices > Relay (actuators) > Configure)

Relays

- Relay can be triggered by Action URL (page Devices > Relay (actuators) > Configure)

Relays in door opener operating mode

Select doors (page Subscriber (scr.) > Properties > Authorisations > Open door)

Relays in all operating modes (except door opener) and alarms

- Switching relays and alarms (page Subscriber (scr.) > Features > Authorisations)

Create new password and set authorisation for access to Action URLs (page Subscriber (scr.) > Properties > Basic settings > Additional passwords > Configure).
2.2 Triggering Action URLs as a system user

Action URLs

☑ Incoming Action URLs active (page Devices > Action URLs)

Create new password and set authorisation for access to Action URLs (page Devices > Action URLs > Passwords for access to Action URLs > Configure).

Alarms

☑ Alarm triggered by Action URL (page Devices > Relay (actuators) > Configure)

Relays

☑ Relays triggered by Action URL (page Devices > Relay (actuators) > Configure)

3 Supported Functions

3.1 Basic structure of Action URLs

http://<IP address PBX>/
action_url?username=<username>&userpw=<password>&function=<functionname>&<parameterlist>

3.2 Authentication

A subscriber must enter their user name (username) and password (userpw) to authenticate themselves or use an Action URL.

- Username: Subscriber's internal number for which the password has been generated. In the case of system-wide passwords, this is the username of the Admin username (Administration > Dealer/operator data > Administrator access > Administrator access > Change > Admin user name).
- Passwd: Subscriber password generated under Subscriber (scr.) > Properties > Basic settings or admin password generated under Devices > Action URLs.

3.3 Switching a relay

https://<IP address PBX>/
action_url?username=<username>&userpw=<password>&function=setRelay&identityNumber=<relay Identification number>&status=<0 or1>

Example:
The Action URL switches on the relay with ID number 301 for subscriber 44

https://192.168.0.240/ action_url?username=44&userpw=q5eV2VhB6srAbr&function=setRelay&identityNumber=301&status=1

Response:

{  
  responseText: "OK",
  responseCode: 0,
3.4 Querying relay status

https://<IP address PBX>/
action_url?username=<username>&userpw=<password>&function=getRelayStatus&identityNumber=<relay identification number>

Example:
The Action URL queries the relay with ID number 307 for the administrator

https://192.168.0.240/
action_url?username=admin&userpw=qPll7IN6oUCNCyt&function=getRelayStatus&identityNumber=307

Response:

{
responseText: "OK",
responseCode: 0,
status: 1,
number: 307,
type: "getRelayStatus"
}

3.5 Changing relay status

https://<IP address PBX>/
action_url?username=<username>&userpw=<password>&function=setRelayStatus&identityNumber=<relay identification number>&status=<0 or 1>

Example:
The Action URL switches off the relay status with ID number 307 for the administrator

https://192.168.0.240/
action_url?username=admin&userpw=qPll7IN6oUCNCyt&function=setRelayStatus&identityNumber=307&status=0

Response:

{
responseText: "OK",
responseCode: 0,
number: 307,
type: "setRelayStatus"}
3.6 Triggering an alarm

https://<IP address PBX>/
action_url?username=<username>&userpw=<password>&function=setAlarm&alarmNumber=<alarm phone number>

Example:
The Action URL triggers the alarm with internal number 61 for subscriber 44

https://192.168.0.240/
action_url?username=44&userpw=q5eV2VhB6srAbr&function=setAlarm&alarmNumber=61

Response:

{
    responseText: "OK",
    responseCode: 0,
    number: 61,
    type: "setAlarm"
}

The alarm's status can be reported using (outgoing) Action URLs.

3.7 Error messages

<table>
<thead>
<tr>
<th>No.</th>
<th>Error message</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>10146</td>
<td>Action URL - Incoming Action URL not activated</td>
<td>Enable Incoming Action URLs active (Devices &gt; Action URLs)</td>
</tr>
<tr>
<td>10147</td>
<td>Action URL - Incoming Action URL only within local network</td>
<td>Check Action URLs only within local network (Devices &gt; Action URLs)</td>
</tr>
<tr>
<td>10148</td>
<td>Action URL - No alarm with this Phone Number</td>
<td>Check alarm's phone number (Devices &gt; Alarms)</td>
</tr>
<tr>
<td>10149</td>
<td>Action URL - No authorisation to enable this alarm</td>
<td>Enable Alarm can be triggered by Action URL for the corresponding alarm (Devices &gt; Alarms &gt; Configure)</td>
</tr>
<tr>
<td>10150</td>
<td>Action URL - No relay with this Identity Number</td>
<td>Check relay ID number (Devices &gt; Relays (actuators))</td>
</tr>
<tr>
<td>10151</td>
<td>Action URL - No authorisation to switch this relay</td>
<td>Enable Relay can be triggered by Action URL (Devices &gt; Relays (actuators) &gt; Configure)</td>
</tr>
<tr>
<td>No.</td>
<td>Error message</td>
<td>Help</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>10152</td>
<td>Action URL - Subscriber is not authorized to enable alarm</td>
<td>Enable <strong>Switching of relays and alarms</strong> <em>(Subscriber (scr.) &gt; Properties &gt; Authorisations)</em></td>
</tr>
<tr>
<td>10153</td>
<td>Action URL - Subscriber is not authorized to switch door relay</td>
<td>Select doors <em>(Subscriber (scr.) &gt; Properties &gt; Authorisations &gt; Open door)</em></td>
</tr>
<tr>
<td>10154</td>
<td>Action URL - Subscriber is not authorized to switch relay</td>
<td>Enable <strong>Switching of relays and alarms</strong> <em>(Subscriber (scr.) &gt; Properties &gt; Authorisations)</em></td>
</tr>
<tr>
<td>10155</td>
<td>Action URL - Can not set status of relay</td>
<td></td>
</tr>
<tr>
<td>10156</td>
<td>Action URL - Can not get status of relay</td>
<td></td>
</tr>
<tr>
<td>10157</td>
<td>Action URL – Parameter missing or wrong.</td>
<td>Action URL structure incorrect <em>(parameter missing or value invalid)</em></td>
</tr>
<tr>
<td>10158</td>
<td>Action URL - Other error</td>
<td></td>
</tr>
</tbody>
</table>