OpenScape Business V2

SIP Attack Protection -
Diagnostic and SIP Provider configuration

Version 2.1

Table of Contents

Table of History

Date	Version	Changes
2013-08-08	1.0	Initial Creation
2017-10-20	2.0	Update for V2
2019-07-09	2.1	Update for V2R7 (inbound proxy list)

1 Introduction

In the past the systems were faced with different attacks from the Internet, thus the interfaces had to be equipped with a protection mechanism against such attacks. A hardened SIP stack as well as a SBC function has been implemented for OpenScape Business. Those measures require special attention to SIP provider configuration. SIP providers which use unknown IP addresses or ports will not work.

How does OpenScape Business help to protect against SIP attacks?

1. If configuring a new SIP endpoint, the system activates authentication by default and protects the access by a random password.
   -> registration hijacking is prevented
2. A SIP filter allows message reception from trusted peers only.
   Trusted peers are
   - registered endpoints
   - configured trunking partners
   - configured ITSP's

   -> all unauthorized peers are blocked
3. Message floods are detected and originating peers are blocked.
   -> avoid denial of service
4. Eventlogs for attack attempts / missing authentication are provided.
   -> get diagnostic information
5. Use dedicated server ports for internal and external traffic
   For connections to endpoints located in the internet a dedicated port with additional security measures is used.
   -> Only this port must be accessible through the firewall. Traffic to the internal port MUST be blocked.

If you are unable to

- register a SIP-client at OSBiz
- register at an ITSP
- cannot establish calls with an ITSP

this might be caused by a wrong configuration, which may end up in treating a certain endpoint /provider as "not trusted".

The following Events/Traces will give you helpful information in such cases.

2 Diagnostics of SIP-Attacks

2.1 SIP endpoint registration not possible

A registration problem can be observed in the SIP protocol

- REGISTER is answered with a "404 Not found" response
- REGISTER is answered with consecutive 401 responses
- REGISTER is NOT answered after several 401 responses

```
EventLogEntry from ERH [ldh:192.168.138.133] …):
EventType: Warning
EventCode: MSG_ERH_SECURITY_DENIAL
EventText: !!Possible-Attack: ErhBlackListObject: 192.168.138.235 : 5060 has reached limit the 1st
time
```

Recommended measures:

- First check that endpoint configuration is consistent with the system configuration credentials containing: call number, User-ID (often referred to as Auth-name) and password.
- If the endpoint does NOT allow the configuration of the User-ID you must change the SIP endpoint configuration in the system (SIP user ID MUST be identical to the call number).
- If problem persists, reenter the password in the system configuration. This will restart the security protection mechanism and allows for immediate registration.

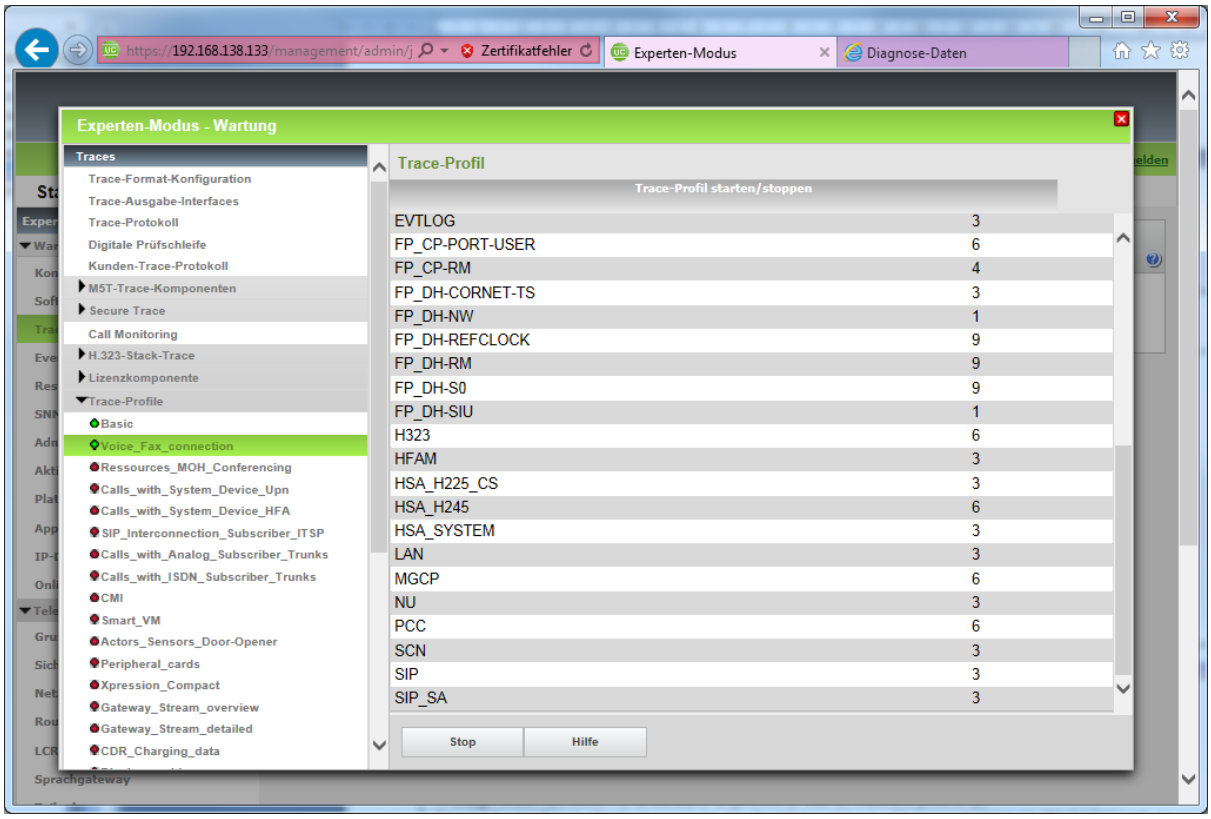
For a detailed analysis of the problem please activate the trace profiles *SIP_Registration and SIP_Interconnection_Subscriber_ITSP*.

A problem with the configuration of the credentials will be printed in the tracelog file:

```
(SIP_REG [ldh:192.168.138.133]… ):
Authentication for REGISTER (Call-ID: 3547641419@192_168_138_235) not successful (no or wrong creds provided)
```

2.2 Connection problems

SIP messages received from an unknown or "not trusted" peer are blocked and not processed by the OSBiz system. If you suspect SIP attacks or face SIP connection problems, please **activate the trace profile Voice_Fax_Connection**.

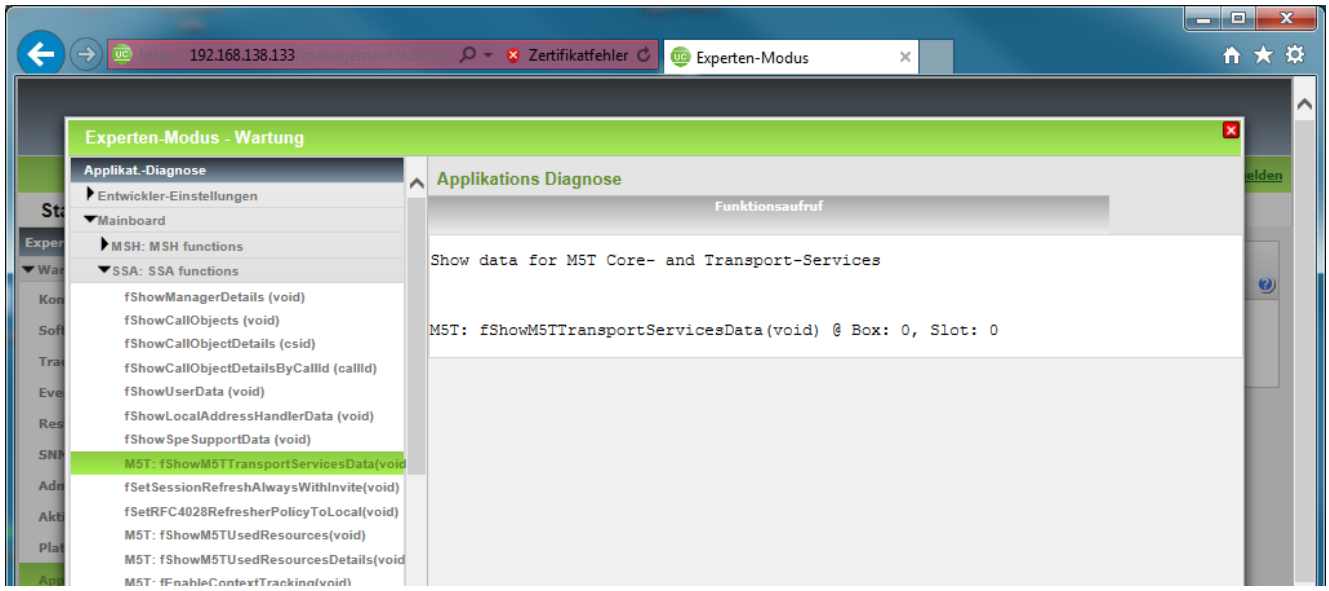


With this profile activated all blocked messages will be printed in the tracelog file, containing the peer address and SIP message:

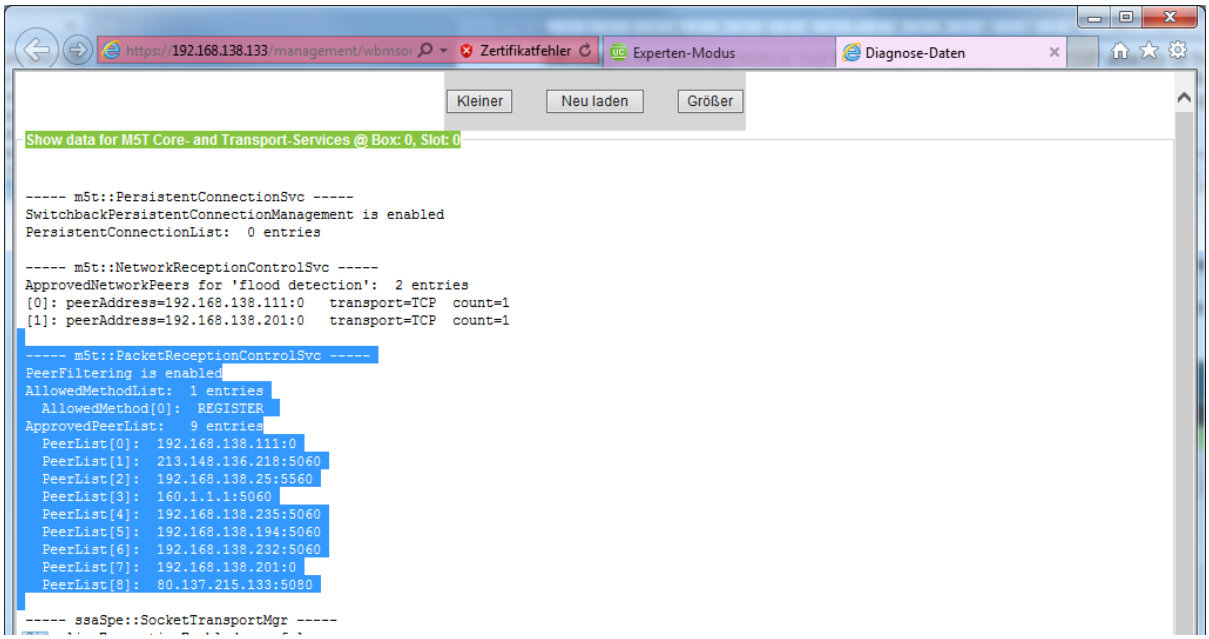
```
(SIP_SA [ldh:192.168.138.72] 0x3023 "11/24/2011 15:40:57.611601" CSipEngine.cpp 6764)

PacketReceptionControlMgr:EvUnapprovedPeerPacketReceived  PeerAddr=192.168.138.70:43597
method=OPTIONS
```

Check the “trusted Peer list”: A diagnostic function is available to print the list of trusted peers at

`Expert mode > Maintenance > Application diagnostics > Mainboard > SSA:SSA functions > fShowM5TTransportServicesData`



When calling this function by pressing “Send”, a list containing all trusted peers will be printed. If port=0 is listed for an IP-address, all ports are accepted, otherwise the listed port only.



Check the IP address to find out where the source is located:

- IP-Address of ITSP
- unknown public IP-Address
- internal IP-Address

1. If the “blocked” packets are received from your ITSP:

For each active ITSP a profile describing the ITSP interface is provided.

Provider Registrar and Provider Proxy can be configured either by an IP-Address or Hostname. It is important to know that the system accepts incoming SIP packets only from the peers specified by these entries.

Configuration examples:

IP-Address / Host name	Port	Packets accepted from
87.237.24.13	5060	87.237.24.13:5060
Sipgate.de	5060	IP Address returned from DNS-A query:5060
vp.thinktel.ca	0	All IP-Addresses returned from DNS-SRV and DNS-A queries

If a provider operates different servers, DNS should be used to resolve all possible IP-addresses from where incoming SIP packets must be accepted.

The following measures are provided by the OSBiz system to overcome possible problems with blocked messages:

- Some ITSPs use different servers, where the corresponding addresses are signaled in the Contact: or Record-route: header fields. For such providers the profile must be configured with the parameter `ApprovedPeerSelection=OutOfResponseHeaders`. (Available since OSBiz V1R3)
- Most providers use a symmetric UDP connection for SIP signaling, where all SIP traffic is sent and received on the same port (=default behavior of the system). If an ITSP wants to use different ports for sending and receiving the corresponding profile must be configured with the parameter `UdpMode=asymmetricUDP`. (Available since OSBiz V1R3)
- For ITSP’s where the SIP server cannot be addressed via DNS the configuration allows to enter additional server(s) in the field “inbound proxy” (since V2R7 a list could be entered)

2. If the packets are received from “unknown” public IP-Addresses:

Attention! In this case your system is attacked from SIP devices outside your network.

Check firewall settings as described in 2.2.1.

3. If the packets are received from “unknown” internal IP-Addresses:

Find out the device sending blocked SIP messages. You have most probably a wrong configuration in the device. Please check the security settings if the parameters in the device are configured according to the parameters in the system.

2.2.1 Basic firewall rules

The basic rules listed here should be check in the firewall between OSBitz and the internet::

1. no forwarding to the internal SIP ports exist
2. If external SIP endpoints are used:
   port forwarding is configured for EXTERNAL SIP port(s) only
3. If ITSP are used which need access to the SIP server port (e.g. UDP transport without registration):
   port forwarding is configured for EXTERNAL SIP port(s) only
4. if b) or c) are not used: disable port forwarding for SIP completely

2.3 Possible Attack from outside detected (REGISTER with spoofed address)

```
EventLogEntry from ERH [ldh:192.168.138.90] ….:
EventType: Warning
EventCode: MSG_ERH_SECURITY_DENIAL
EventText: !!Possible-Attack: SIP_PContactInfo-IpAddress does not match with sender
contact=192.168.138.200,sender=89.227.45.11
```

Recommended measures:

- Check firewall settings as described in 2.2.1

2.4 Message flood leads to Peer blocking

```
EventLogEntry from SIP_SA [ldh:192.168.138.90] ….:
EventType: Major
EventCode: SIP_INVALID_PARAMETER_VALUE
EventText: NetworkReceptionSvc: SIP message flood  PeerAddr=89.227.45.11:5060 blocked
```

Recommended measures:

- Check firewall settings as described in 2.2.1
- Eliminate source, if attack is internal.

2.5 Authentication was switched OFF

```
EventLogEntry from ERH [ldh:192.168.138.90] ….:
EventType: Major
EventCode: MSG_ERH_SECURITY_DENIAL
EventText: fGetERHSIPSubConfigValues: Warning! SIP Authentication is deactivated for
subscriber=3561
```

Recommeded measures:

- Switch authentication on again
- Check, if there is unauthorized administration access to the system, if this was not done intentionally

About Unify

Unify is the Atos brand for communication and collaboration solutions. At the core of the Atos Digital Workplace portfolio, Unify technology enables organizations of all sizes to transform the way they collaborate, creating a more connected and productive workforce which can dramatically improve team performance, individual engagement and business efficiency.

Unify products represent a strong heritage of technology innovation, reliability and flexibility. Their award-winning intuitive user experience can be delivered through almost any device and in any combination of cloud or on-premise deployment. Augmented by Atos' secure digital platforms, vertical solutions and transformation services, they set the global standard for a rich and reliable collaboration experience that empowers teams to deliver extraordinary results.

Unify.com

unify
atos collaboration solutions