

USP SECURE ENTRY SERVER®



UNITED SECURITY PROVIDERS

Documentation Series

Appliance

User Guide

Version 5.18.0.2



United Security Providers AG
www.united-security-providers.ch
info@united-security-providers.ch

Headquarter Stauffacherstrasse 65/15 CH-3014 Bern Tel. +41 31 959 02 02
Baslerpark Mürtschenstrasse 27 CH-8048 Zürich Tel. +41 44 496 61 11



UNITED SECURITY PROVIDERS

Copyright © 2026 United Security Providers AG

This document is protected by copyright under the applicable laws and international treaties. No part of this document may be reproduced in any form and distributed to third parties by any means without prior written authorization of United Security Providers AG.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESSED OR IMPLIED REPRESENTATIONS AND WARRANTIES, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED TO THE EXTENT PERMISSIBLE UNDER THE APPLICABLE LAWS.



Contents

1 Introduction	1
1.1 Purpose of Document	1
1.2 Target Audience	1
1.3 Glossary	1
2 Overview	2
2.1 Appliance Platforms	2
2.1.1 MaxMind GeoIP License	2
2.1.2 Hardware Appliance	2
2.1.3 Virtual Appliance	2
2.2 Network Environment	4
2.2.1 Interface Roles	4
2.3 Special Setups	5
2.3.1 Standalone Appliance	5
2.3.2 USP Secure Entry Server® Cloud Appliance	5
2.4 High Availability Setups	5
2.4.1 Active/Passive	6
2.4.2 Active/Active	7
3 Installation	8
3.1 Installation on Virtual environment	8
3.2 System Requirements for SES Appliance	8
3.3 Create Virtual Machine template	8
3.4 Prepare and create Network Adapters	9
3.5 Configure Network Interfaces on the Virtual Machine	9
3.6 Initial SES Appliances Setup	11
3.7 Interface Configuration	13
3.8 Activating the initial configuration	13
4 Connecting the Hardware Appliance	13
4.1 Software Installation with Hardware Appliance	14
4.2 Administration Web GUI Access	14



5	Using USP Secure Entry Server®	14
5.1	USP Secure Entry Server® Components	14
5.2	Web GUI Overview	16
5.2.1	Main Navigation	17
5.3	Console Menu	19
5.4	Configuration Lifecycle	20
5.4.1	Committing	20
5.4.2	Testing	20
5.4.3	Activation	20
5.4.4	Synchronization	20
6	Configuration	21
6.1	Network Setup	21
6.1.1	Appliance Hostname	21
6.1.2	Interface Settings	21
6.1.3	Create a new virtual host	22
6.1.4	Create a new location	25
6.1.5	Security Profile	27
6.1.6	Target Manager	32
6.1.7	Security Profile Templates	34
6.1.8	Enabling / Using Authentication	36
6.1.9	Authentication Basics	37
6.1.10	Login Process Example	39
6.1.11	Custom Properties	41
6.1.12	Setup Authentication Service Standalone Appliance	41
6.1.13	Connect Remote Standalone Authentication Service	42
6.2	High Availability Setup	43
6.2.1	HA Active/Passive	43
6.2.2	HA Active/Active	44
6.2.3	Session Transfer	45
6.2.4	High Availability Status	45
6.3	Automatic Certificate Management Environment (ACME)	46
6.3.1	Preconditions	46
6.3.2	Limitations	46
6.3.3	Migration to ACME managed certificates	46
6.3.4	Configuration	46
6.3.5	Enable ACME for a vhost	47
6.3.6	Config Export & Backup ACME	48
6.4	User Management	48
6.4.1	User Roles	48



7 Operation	49
7.1 Configuration Backup & Recovery	49
7.1.1 Configuration export	49
7.1.2 Configuration import	49
7.1.3 System backup	49
7.1.4 System recovery	49
7.1.5 Automated remote backup	50
7.2 Appliance Update	50
7.3 Log Management and Analysis	51
7.3.1 Log Management	51
7.3.2 Log Message forwarding	52
7.3.3 Log Viewer	53
7.3.4 Traffic Analyzer	53
7.4 Monitoring	54
7.4.1 System health status	54
7.4.2 Local SNMPD Server	54
7.4.3 SNMP Traps	54
7.5 Statistics and Events	55
7.5.1 Events	55



1 Introduction

The USP Secure Entry Server[®] appliance is a web application firewall acting as a reverse proxy with authentication and user management capability and is installed within the neighborhood of one or more target web servers.

All connections coming from the Internet addressed to one of the web servers are protected by the USP Secure Entry Server[®] appliance, which passes the requests on to the main web servers.

1.1 Purpose of Document

This guide gives a brief overview of the USP Secure Entry Server[®] appliance and its component. It describes the basic installation and configuration steps as well as how to operate the USP Secure Entry Server[®] appliance according to configuration changes, monitoring, log data analysis and more.

1.2 Target Audience

The document is intended for system administrators of the USP Secure Entry Server[®] appliance.

1.3 Glossary

Table 1: Glossary

Term	Definition
<i>SES</i>	USP Secure Entry Server [®] , the entire software suite, including the Web Application Firewall, the Authentication Service and the Administration Web GUI.
<i>WAF</i>	Web Application Firewall, the entire web application firewall part of the SES. It acts as reverse proxy and consists of the three components "HTTP Listener" (HTL), "HTTPS Listener" (HTS) and "SRManager" (SRM). The composition of these components is technically called HSP.
<i>HSP</i>	HTTP Secure Proxy, the technical name of the WAF.
<i>HTL</i>	WAF HTTP Listener, the HTTP listener component of the web application firewall.
<i>HTS</i>	WAF HTTPS Listener, the HTTPS listener component of the web application firewall.
<i>SRM</i>	WAF Request Manager, the session management component of the web application firewall.
<i>SLS</i>	Secure Login Service, the technical name of the Authentication Service component that is responsible for authenticating and authorizing end-users.
<i>IDM</i>	Identity Manager, lean turn-key ready user management system with integrated user administration frontend and directory provisioning capabilities.
<i>Target server</i>	An application backend server which is the actual target of an incoming HTTP request.



2 Overview

This chapter gives an overview of the different appliance platforms and setups of the USP Secure Entry Server[®] appliance.

2.1 Appliance Platforms

There are two main appliances platforms: [hardware appliance](#) and [virtual appliance](#).

2.1.1 MaxMind GeolP License

The USP Secure Entry Server[®] appliance provides support for using both free and commercial GeolP databases by MaxMind. The free "GeoLite" databases are provided under the so-called "Creative Commons License":

- [Creative Commons Corporation Attribution-ShareAlike 4.0 International License](#)

The details of the MaxMind licensing can be reviewed on their own website:

- [MaxMind Geolp Database EULA](#)

2.1.2 Hardware Appliance

The hardware appliance has a standard rack size form factor. Besides the common ports, the appliance offers four network interfaces. See [Interface Roles](#) section for details how these interfaces are used. To prevent service failures, the appliance supports redundant power-supplies and mirrored hard disks (RAID 1).

2.1.3 Virtual Appliance

The USP Secure Entry Server[®] can run as a virtual appliance. The functionality does not differ to the hardware appliance, except that the hardware settings can be individually adjusted to the expected needs.

The following settings are recommended for a moderate system usage:

Parameter	Minimal	Recommended
CPU cores	2	8
RAM	8 GB	32 GB
Disk size	40 GB	300 GB
Network interfaces	2	3

If the virtualization software allows to define a guest operation platform, a 64bit architecture with Linux Kernel 4.X should be used.

Note

The RAM requirements may vary considerably depending on the number of applications and concurrent users.

Note

With the minimal configuration the performance as well as the usage of different features is very limited and is not recommended for production.



The supported virtualization solutions are:

- VMware ESX/ESXi (Supported versions: 8.0, 7.0, 6.7, 6.5 and 6.0)
- Hyper-V
- Nutanix AHV



2.2 Network Environment

The USP Secure Entry Server[®] appliance is commonly run as a multi-homed server. This means that the USP Secure Entry Server[®] appliance requires at least two separate network interfaces being connected to your routers/switches/firewalls in order to be used. Each network interface has a certain role which implies some restrictions.

2.2.1 Interface Roles

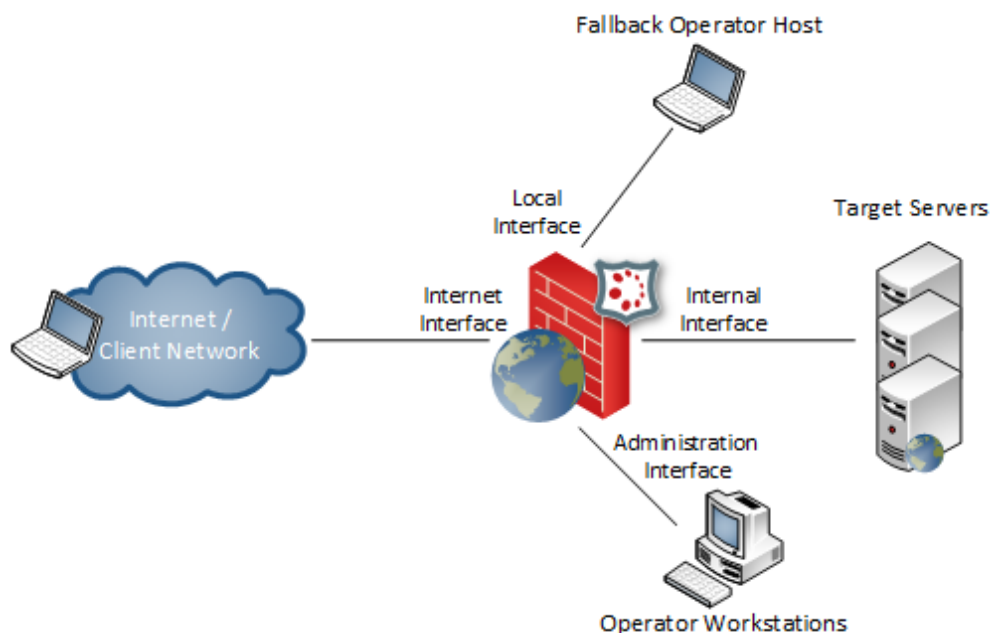


Figure 1: Network Interface Roles

Local interface The *local* (or *console*) interface is used to connect a local administrative workstation to the USP Secure Entry Server[®] appliance. The workstation may be connected using a crossed Ethernet cable. This interface is used for the initial network configuration when setting up a new USP Secure Entry Server[®] appliance. By default the interface has the IP addresses `192.168.0.1/24` and `fd12:3:4:5::/64` assigned. You can access the Administration Web GUI via this interface on port 443 or 8443 (HTTPS).



Warning

The *local* interface features a DHCP server which is enabled by default. The DHCP service is used to provide your administrative workstation with an IP address in order to connect to the Administrator Web GUI. Never connect this interface to the internal area network since the DHCP server may seriously disturb other systems connected to this network.



External interface	The <i>external</i> interface is connected to the inbound firewall (client/external network). This interface becomes the IP address which is going to be accessible from the client network, typically the Internet. Multiple IP addresses may be assigned to this interface, one for each host, but all these addresses must be within the same network segment. See section Hosts about configuring new hosts. The default route is always set to the gateway connected to this interface.
Internal interface	The <i>internal</i> (or <i>intranet</i>) interface provides connectivity to the network of target servers. Requests to target servers are always sent via this interface. You can also access the Web GUI for Administration via this interface on port 443 or 8443 (HTTPS).
Administration interface	The <i>administration</i> (or <i>operator</i>) interface is optional and may be connected to a separate network for operational purposes (access to the Web GUI of the USP Secure Entry Server [®] appliance only).

**Important**

When the *administrator* interface is enabled, access to the Web GUI via the *internal* interface is not possible anymore.

During operation the *external* interface and the *internal* interface are mandatory and must be connected to your network.

2.3 Special Setups

2.3.1 Standalone Appliance

It is possible to run the appliance in Authentication Service or Identity Manager Standalone mode. If enabled, the WAF and other service features are disabled and only the respective service is running. This setups requires at least two interface, else the Cloud Appliance mode will be enabled([Cloud Appliance](#)). Only the *internal* interface needs to be connected to the network during operation.

See [Setup Authentication Service Standalone Mode](#) section for further information how to enable e.g the Authentication Service Standalone mode. Identity Manager Standalone can be setup in the same way.

2.3.2 USP Secure Entry Server[®] Cloud Appliance

United Security Providers provides the necessary machine images to instantiate a virtual cloud appliance.

The main difference to the other setups is that only one network interface is available. The IP Address is automatically assigned by the cloud service and the administration Web GUI can only be accessed on port 8443.

2.4 High Availability Setups

The USP Secure Entry Server[®] appliance High Availability (HA) and Session Transfer facility offers two different setups:

- [Active/Passive](#) - Failover to secondary standby appliance
- [Active/Active](#) - Load distribution and failover using multiple appliances



2.4.1 Active/Passive

This High Availability setup allows a failover between two appliances.

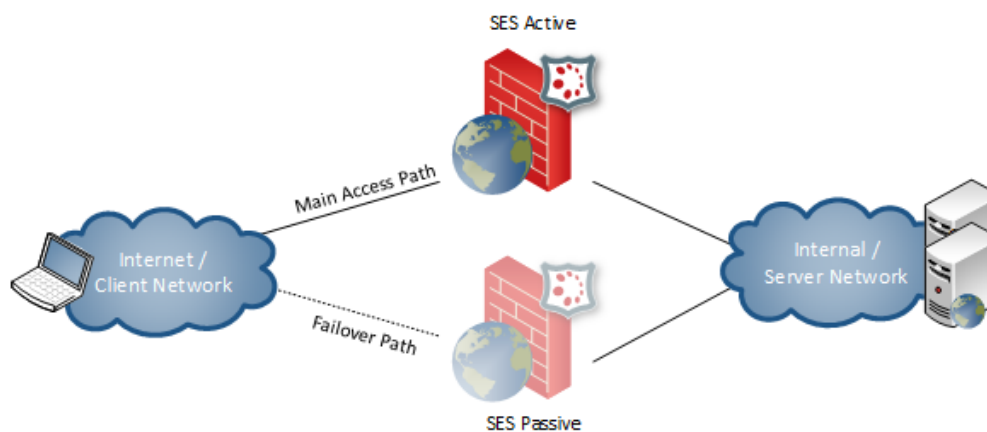


Figure 2: HA Active/Passive Setup

- One active USP Secure Entry Server[®] appliance processes client requests.
- A standby USP Secure Entry Server[®] appliance is ready to takeover the service if this becomes necessary.
- A service takeover is either initiated manually or automatically when the active server becomes unavailable.
- The configuration may be synchronized between the USP Secure Entry Server[®] appliances.
- WAF virtual host IP addresses are shared between the two nodes. The standby USP Secure Entry Server[®] appliance has disabled its *external* interface until the active server becomes unavailable.



2.4.2 Active/Active

This High Availability setup allows load distribution and failover between two or more appliances.

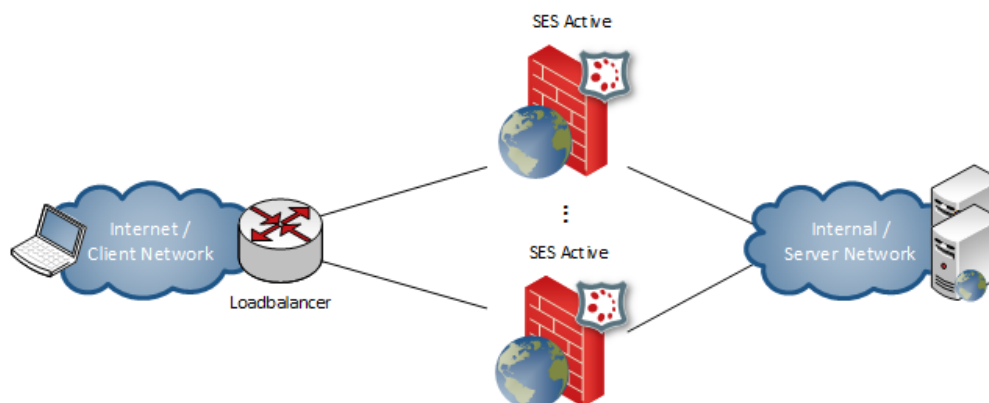


Figure 3: HA Active/Active Setup

- All active USP Secure Entry Server[®] appliance processes client requests.
- A load balancer is needed to distribute the incoming requests to the USP Secure Entry Server[®] appliances.
- One or more USP Secure Entry Server[®] appliance can be put manually offline for maintenance tasks.
- Offline USP Secure Entry Server[®] features a transfer of client sessions to the active USP Secure Entry Servers[®].
- The configuration may be synchronized between all USP Secure Entry Server[®] appliances in the active/active set.
- Each node has distinct IP addresses for its WAF virtual hosts.



3 Installation

This guide is intended if you want to install a SES appliance on a virtual environment or with a SES Hardware Appliance. It also serves for quick installation for SES testing purposes or for a SES demo environment.

See section [Connecting the Hardware Appliance](#) if you have a SES Hardware Appliance.

3.1 Installation on Virtual environment



Important

Do not start the Virtual Machine and bootable SES ISO image using **only** one network interface, otherwise the SES appliance will boot in cloud mode and would not be usable.

Prerequisites:

- SES ISO Image filename: ses-5.x.x.x-xxxx-x86_84-install.iso
- It is compatible with Hypervisor VMware ESXi, Microsoft Hyper-V, KVM (Proxmox/QEMU), Nutanix AHV, Oracle VirtualBox or with Hardware Dell PowerEdge.

3.2 System Requirements for SES Appliance

see also Appliance User Guide - section [Appliance Platforms](#)

Parameter	Minimal	Recommended
CPU cores	2	8
RAM	8 GB	32 GB
Disk size	40 GB	300 GB
Network interfaces	2	3

3.3 Create Virtual Machine template

- Start Hypervisor e.g. VirtualBox, Hyper-V etc.
- Create New Virtual Machine
- Name: SES-Appliance
- Type: Linux
- Version: Other Linux (64-bit) or Gentoo (64-bit)
- Using a BIOS VM is recommended; but if a UEFI-based setup is used, it is necessary to disable secure boot.
- Memory: e.g. 16GB (disable dynamic memory !)
- Select the first Network Adapter for the Admin Interface e.g. 192.168.56.0
- Create a virtual hard disk
- Fixed size: e.g. 50GB
- Select bootable SES ISO e.g. ses-5.x.x.x-xxxx-x86_84-install.iso

**Important**

Do NOT start the newly created VM before all network adapters have been properly set up as described in the following chapter, otherwise the SES appliance will boot in cloud mode and would not be usable.

3.4 Prepare and create Network Adapters

Start the Hypervisor application, but **IMPORTANT** leave the Virtual Machine powered **off**. It is absolutely necessary to add additional Network adapters.

- Adapter 1: Admin Network Adapter (e.g. 192.168.56.0)
- Adapter 2: Internal Network Adapter (e.g. 10.0.2.0)
- Adapter 3: External Network Adapter (e.g. 192.168.57.0)

Select the Virtual Machine and add or edit the Network Adapters as below as example:

Admin Network Adapter

- IPv4 Address: 192.168.56.0
- IPv4 Subnet Mask: 255.255.255.0

Internal Network Adapter

- IPv4 Address: 10.0.2.0
- IPv4 Subnet Mask: 255.255.255.0

External Network Adapter

- IPv4 Address: 192.168.57.0
- IPv4 Subnet Mask: 255.255.255.0

3.5 Configure Network Interfaces on the Virtual Machine

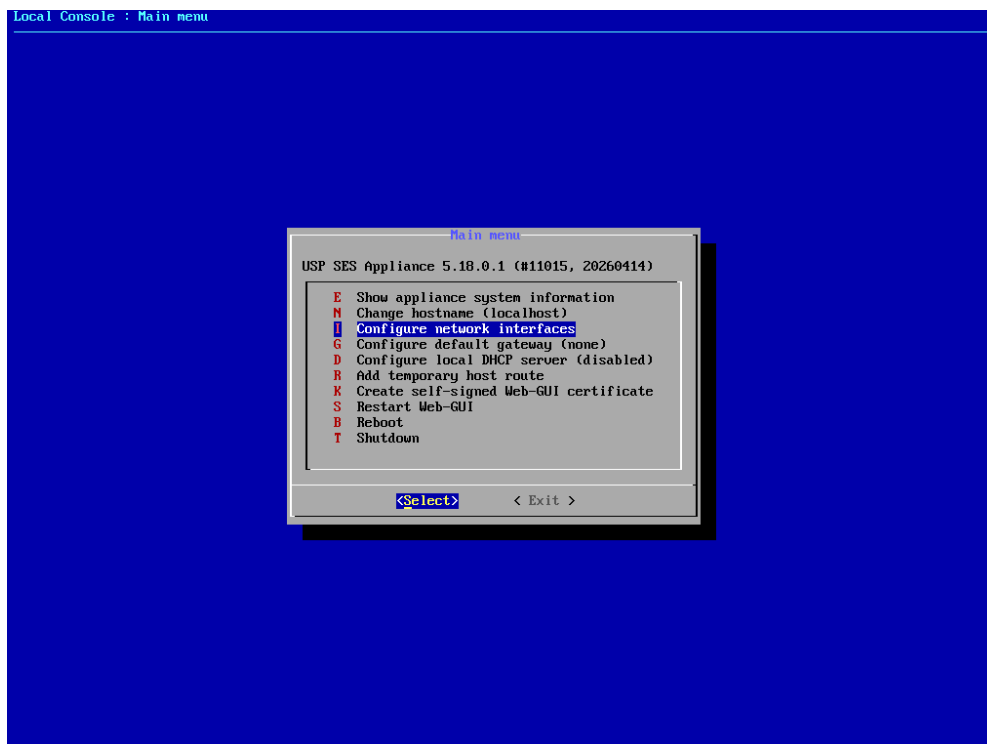
- Power on the SES-Appliance virtual machine



```
* Checking local filesystems ... [ ok ]
* Remounting filesystems ... [ ok ]
* Updating /etc/mtab ... [ ok ]
* Creating mtab symbolic link [ ok ]
* Activating swap devices ... [ ok ]
* Mounting local filesystems ... [ ok ]
* Configuring kernel parameters ... [ ok ]
* Creating user login records ... [ ok ]
* Wiping /tmp directory ... [ ok ]
Cloud-init v. 22.4 running 'init-local' at Tue, 21 Apr 2026 10:35:17 +0000. Up 4.38 seconds.
Cloud-init v. 22.4 running 'init' at Tue, 21 Apr 2026 10:35:17 +0000. Up 4.84 seconds.
ci-info: +-----+Net device info+-----+
ci-info: +-----+-----+-----+-----+-----+-----+
ci-info: | Device | Up | Address | Mask | Scope | Hw-Address |
ci-info: +-----+-----+-----+-----+-----+-----+
ci-info: | eth0 | False | . | . | . | 00:15:5d:01:37:0e |
ci-info: | eth1 | False | . | . | . | 00:15:5d:01:37:0d |
ci-info: | eth2 | False | . | . | . | 00:15:5d:01:37:0e |
ci-info: | lo | False | . | . | . | |
ci-info: +-----+-----+-----+-----+-----+-----+
ci-info:
2026-04-21 10:35:17,784 - util.py[WARNING]: No instance datasource found! Likely bad things to come! [ ok ]
* Starting USP Shared Appliance Base Boot Service ... [ ok ]
* Setting hostname to localhost from /etc/conf.d/hostname ... [ ok ]
* Setting terminal encoding [UTF-8] ... [ ok ]
* Setting keyboard mode [UTF-8] ... [ ok ]
* Loading key mappings [sg] ... [ ok ]
* Bringing up network interface lo ... [ ok ]
* Bringing up interface lo
* Caching network module dependencies
* 127.0.0.1/8 ... [ ok ]
* Adding routes
* 127.0.0.0/8 via 127.0.0.1 ... [ ok ]
* Saving key mapping ... [ ok ]
* Saving terminal encoding ... [ ok ]
* Seeding random number generator ... [ ok ]
* Saving 256 bits of creditable seed for next boot [ ok ]
* Create Volatile Files and Directories ... [ ok ]
INIT: Entering runlevel: 3
* WARNING: clock skew detected!
* Starting USP Shared Appliance Base ... [ ok ]
* Running puppet ... [ ok ]
* Starting cronie ... [ ok ]
* Starting local ... [ ok ]

USP SES Appliance 5.18.0.1 (#11015) localhost
localhost login:
```

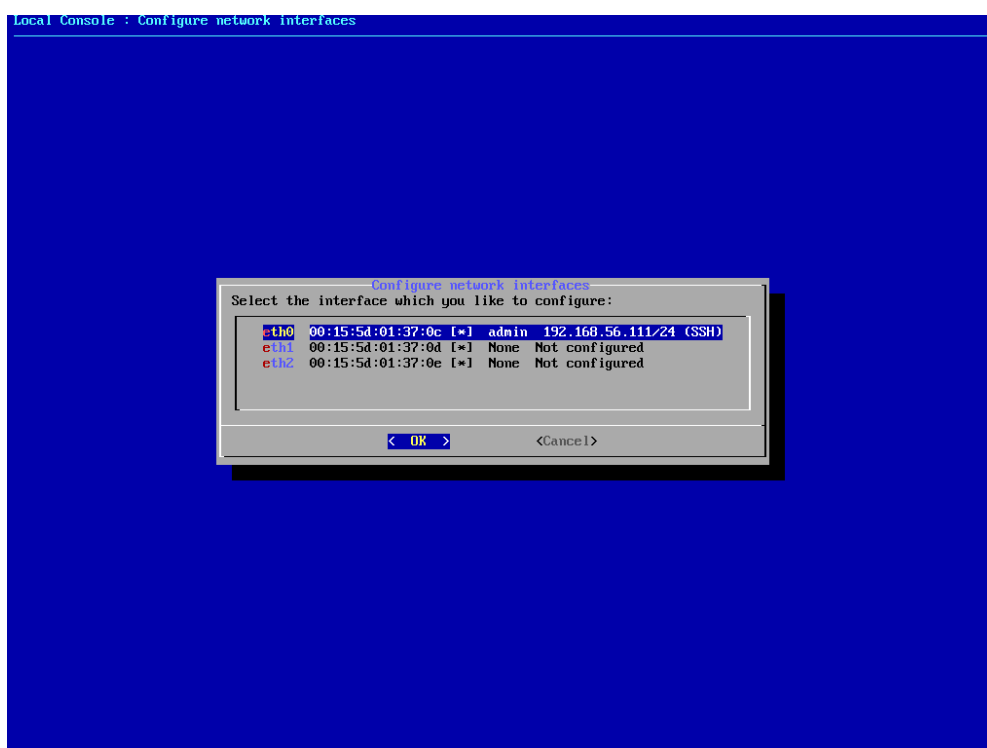
- Log in on the Virtual Machine console with the credential below:
 - Username: console
 - Password: console
- select "Configure network interfaces" in the Console Menu





The console menu provides a variety of options to configure basic USP SES Appliance settings. Here you will see the three connected network interfaces. We will now configure the admin interface. Afterward, we should be able to access the SES Admin WebGUI.

- Find the MAC address of the "Admin Network Adapter*" select the interface with the matching MAC address in "Configure network interfaces" (using the arrow keys and then click Enter).
- Select "static"
- Select "admin"
- Enter e.g. "192.168.56.111/24" in IPv4 address field
- IPv6 address field is optional



- Select "ssh" (with the spacebar)

Repeat these steps for the other two adapters (Internal Network, External Network). However, only the configured "admin" interface requires the "ssh" flag.

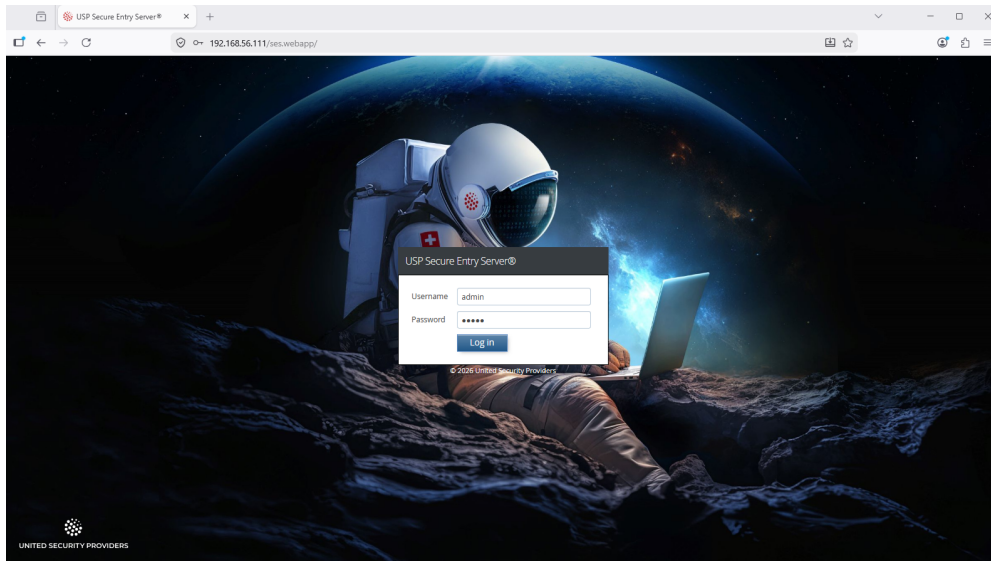
3.6 Initial SES Appliances Setup

Login to SES Admin WebGUI

- Access via Web-Browser the SES Admin WebGUI e.g. <https://192.168.56.111>
- Browser Security settings click Advanced → Proceed to unsafe access
- Login with the Admin WebGUI default credential:
 - Username: admin

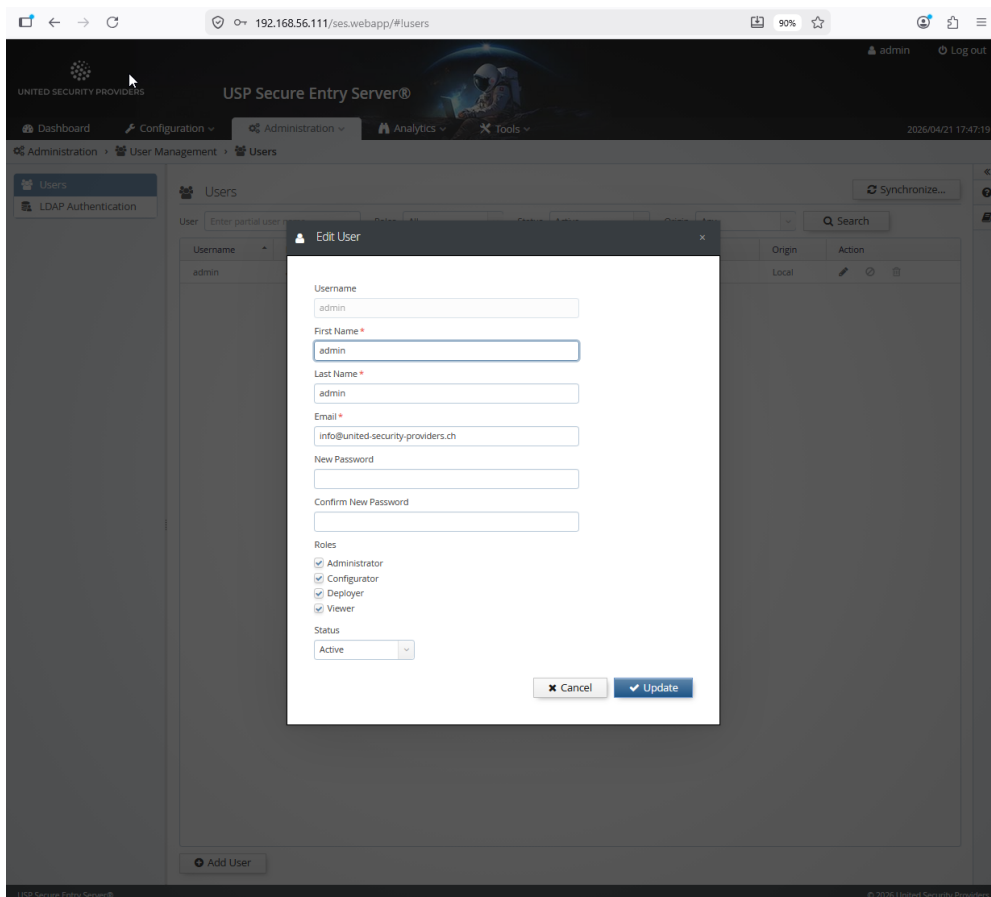


– Password: admin



Important

After the first login, the password of the "admin" user should immediately be changed to a secure new value:





- Go to the SES Admin WebGUI menu "Configuration → System Settings → Interfaces"

3.7 Interface Configuration

- Find the MAC addresses of all Network Interfaces
- **IMPORTANT:** Map the network interfaces to the right MAC addresses, but at least the "Admin Network Adapter" otherwise you lose the connection over the browser to the Admin WebGUI.
 - Local Console Network → Optional not **necessary** for VM
 - External Network Adapter → Adapter 3 (External interface)
 - Intranet Network Adapter → Adapter 2 (Internal Interface)
 - Administrator Network Adapter → Adapter 1 (Admin Interface)

Configure the WAF IP addresses below an example:

- External (Internet or DMZ Network)
 - IPv4 address: 192.168.57.222
 - Netmask: 24
 - Gateway: 192.168.57.1
- Intranet (Application or Backend Server Network)
 - IPv4 address: 10.0.2.10
 - Netmask: 24
 - Gateway: 10.0.2.1
- Administrator (Management or Operator Network)
 - Enable interface with checkbox
 - IPv4 address: 192.168.56.111
 - Netmask: 24
 - Gateway: 192.168.56.1
 - * click save

3.8 Activating the initial configuration

- Commit → Comment (with a text e.g. Network Interface configuration) → click Commit
- click Activate

If you have done it correctly, access to the SES Admin GUI e.g. <https://192.168.56.111> should still be possible after activation.

4 Connecting the Hardware Appliance

For the installation, at least the *external* and the *internal* interface must be connected to the network. For the initial setup, the *local* interface can be connected to the operator workstation with an Ethernet crossover cable.

The [interface roles](#) are per default assigned according to the order of the MAC addresses which corresponds with the physical location of the network cards on the system board. Starting with the lowest being the *local* interface, followed by *external* interface, *internal* interface, *administration* interface. Looking at the backside of the hardware appliance, the furthest interface to the left is the *local* interface.

The interface roles assignment can be changed after the initial setup when configuring the appliance with the Web GUI.



4.1 Software Installation with Hardware Appliance

The provided installation media contains an auto-installer for USP Secure Entry Server[®]. To install the software, boot the appliance from the install media (USB Stick) and start the auto-installer. No user interaction will be required. After finishing the installation, the appliance will reboot automatically and start up the USP Secure Entry Server[®] appliance.

4.2 Administration Web GUI Access

When the operator workstation is connected to the *local* interface with an Ethernet cross-over cable, the Administration Web GUI can be accessed with a browser by navigating to the address <https://192.168.0.1> or fd12:3:4:5::. The operator workstation will automatically receive an IP address from the local DHCP server running on this interface.



Important

The default user is "admin" with password "admin". **Change the default password after you have logged in!** See section [User Management](#) about managing administrative roles.

Note

If the USP Secure Entry Server[®] appliance can't be accessed via the *local* interface, see section [Console Menu](#) how to initially setup the network interfaces without Administration Web GUI access.

After the initial setup, the Administration Web GUI can be access via the *internal* interface or the *administration* interface, and always via the *local* interface. When successfully logged into Web GUI, the first step is the configuration of the network interfaces. See [Network Settings Setup](#) for further details. <<<

5 Using USP Secure Entry Server[®]

5.1 USP Secure Entry Server[®] Components

The USP Secure Entry Server[®] is the only system directly accessible and visible from the Internet. All other infrastructure components are hidden behind it. To be able to safeguard application servers and infrastructure elements, all communication terminates on the USP Secure Entry Server[®]. It establishes connections to the inner side to the target server on behalf of the clients.

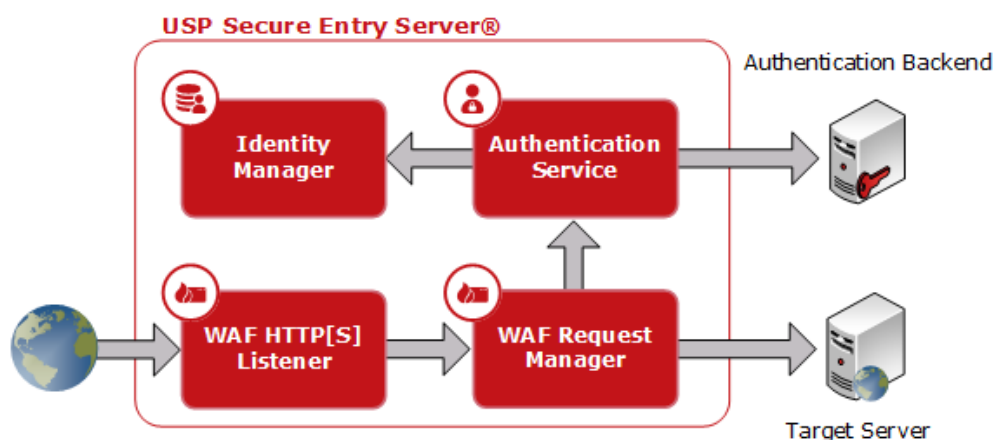


Figure 4: USP Secure Entry Server[®] components



WAF HTTP(S) Listener

The HTTPS Listener is the main entry point which terminates the TCP connection, provides filtering, policy control, content compression and request prioritization. The HTTP Listener usually only redirects to the HTTPS Listener to ensure encrypted communication.

WAF Request Manager

The Request Manager features session management, access control, fine granular policy control and target server integration with load-balancing and URL translation.

Authentication Service

The first request to a non-public URL is forwarded to the Authentication Service. After successful authentication, requests are handed over directly to applications on the target servers.

Identity Manager

Is a user directory which can be used as authentication backend by the Authentication Service. It included a user management web application and features provisioning capabilities to other directories.



5.2 Web GUI Overview

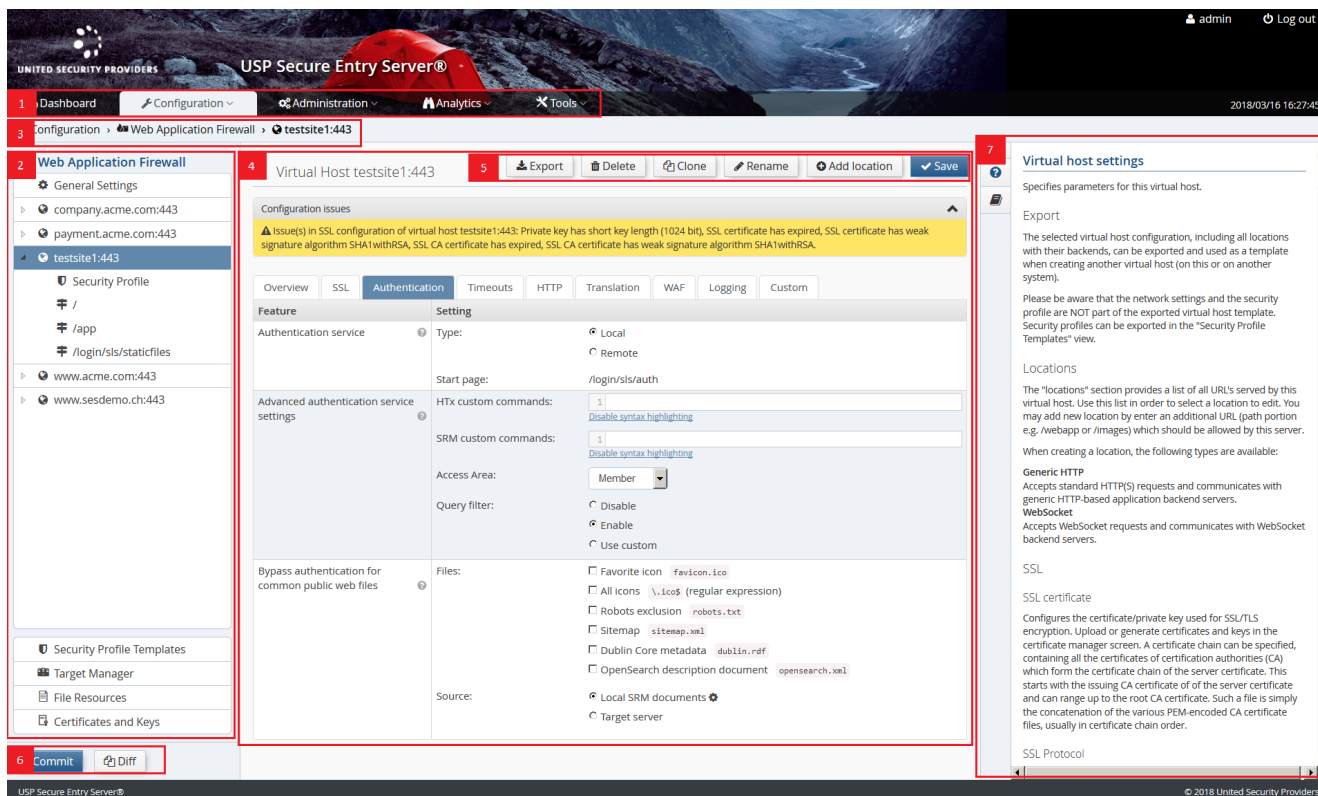


Figure 5: USP Secure Entry Server® Administration Web GUI Overview

(1) Main Navigation

Menu items to access the different configuration and administration views.

(2) Configuration (Secondary) Navigation

A more fine grained navigation for the different main navigation items. E.g. Virtual Host and Location configuration for the Web Application Firewall. This secondary navigation is not present in all views.

(3) Navigation Breadcrumb

A navigation breadcrumb showing the path of the current view and allowing to quickly navigate to the higher level views in the path.

(4) Main Configuration Content Area

The main view area.

(5) Action Area

The main actions, like save configuration or the like, are always located in the upper right corner.

(6) Configuration Deployment Shortcut

These are shortcut links to the configuration deployment actions. They only appear when uncommitted changes are present, the configuration need to be activated or synchronized.

(7) Help Sidepanel

The sidepanel provides the detailed context help as well as the list of documentation. Per default the sidepanel is hidden and can be expanded when needed by clicking the different tabs.



5.2.1 Main Navigation

Dashboard

The dashboard offers an overview of status information, statistics and performance indicators.

Configuration

The USP Secure Entry Server[®] system and component configuration. All these are included in the [configuration lifecycle](#).

Web Application Firewall

Configuration of the entire Web Application Firewall, including the WAF itself, target server management and local file resources.

Authentication Service

Authentication Service related configuration, like adapters, models, scripts, file resources and more.

Identity Manager

Configuration of the user directory structure and provisioning settings for multiple Identity Manager tenants.

NOTE: This component must be licensed separately!

System Settings

Configuration related to the appliance system, i.a. [network settings](#), [High Availability settings](#), [log management](#), remote services and more.

Manage and Deploy

View and actions related to the [configuration lifecycle](#), including management and activation of configuration and import and export of those.

Administration

Different administration tasks. This view is only accessible for users with *Administration* user role.

Users

User management and password change, see section [User Management](#).

Appliance Control

Appliance control action like shutdown and reboot and Web GUI certificate management.

Software Update

Shows detailed software version information and allows to update the appliance, see section [Appliance Update](#).

Analytics

Log Viewer

Viewer to filter and search the different log files of the components.

Log Download

Log file archive of the different SES components.

Event Viewer

List of open events reported by the different USP Secure Entry Server[®] components.

Traffic Analyzer

This screen is used to analyze the HTTP/HTTPS traffic between the USP Secure Entry Server[®] and the target servers for application integration purposes.

Tools

Reports

Provides several different reports with usage, security and support statistics.

SLS DataProtector

Tool that allows to encrypt sensitive configuration property values.



Connectivity Check

Overview of the different targets servers and facility to check if systems are reachable.

Network Tools

Tools like Ping and Traceroute, useful to analyze network problems.



5.3 Console Menu

A simple Console Menu that allows to prepare the initial access to the Web GUI. It can be started having direct access to USP Secure Entry Server® local console and log in using the user "console" with the password "console".

Table 6: Console Menu Commands

Command Key	Description
E	Shows different appliance system information, like release information, current network interface and IP address settings or routing table
N	Sets the hostname of the appliance temporarily.
I	Sets the network interface roles and IP address settings temporarily.
G	Sets the default gateway temporarily.
D	Stops or starts the DHCP server. The status change is persistent (reboot).
R	Adds a temporary route to a server. The entry gets deleted at server reboot.
K	Creates a self signed x509 certificate for the Web front-end using the servers machine name.
S	Restarts the Web GUI.
B	Reboots the appliance
T	Shutdown the appliance

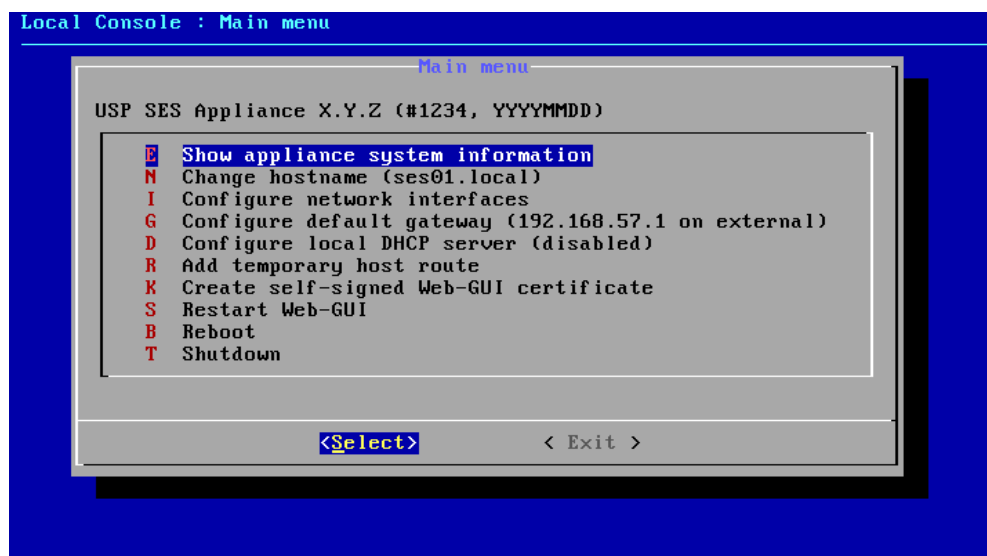


Figure 6: USP Secure Entry Server® console



5.4 Configuration Lifecycle

Configuring the USP Secure Entry Server® involves several steps. All configuration files are under revision control, which allows to have a change history, as well as the possibility to rollback the configuration to any previous state. The configuration needs to be explicitly activated before the components will apply it, so service interruptions due to required restarts of the Web Application Firewall or Authentication Service components can be planned in advance.

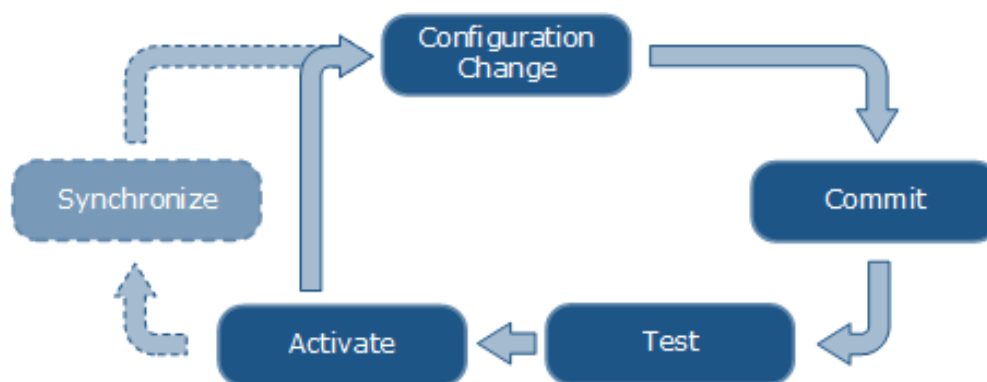


Figure 7: Configuration Lifecycle

5.4.1 Committing

Whenever one or more configuration parameters in the "System Settings", "Web Application Firewall", "Authentication Service" or "Identity Manager" section are changed, it is necessary to commit these changes. A "Commit" button will be displayed in the navigation sidebar, taking the user to the commit screen where a review of the changes to the configuration files is possible. Every commit requires a commit message, describing what has been changed, which is then added to the change history.

5.4.2 Testing

The current configuration can be tested for issues (e.g. invalid security certificates, misconfigured custom commands) by clicking on the *Test* button in the *Configuration Deployment* screen (*Configuration*→*Manage and deploy*). This will deploy the configuration to a temporary directory structure, and start the services in test mode.

The *Configuration Deployment* screen will also show warnings about obvious configuration issues. Clicking on an entry will open the related screen where the issue can be fixed.

5.4.3 Activation

Configuration activation is only possible if there are no uncommitted changes. To activate the current configuration, go to *Configuration*→*Manage and deploy*→*Configuration Deployment* screen and click on the *Activate* button. The activation process takes a while, as some services might require a restart or a reload. Services, whose configuration has not been changed, will not be restarted.

Sometimes, the activation will perform a restart of the web GUI, for example if the internal or administrative IP address has been changed. In that case, it may be necessary to reconnect to the web GUI manually after a while.

5.4.4 Synchronization

If the USP Secure Entry Server® is set up as a High Availability cluster, the configuration needs to be synchronized to the other node(s) after activation. A *Synchronize* button will be displayed in the *Configuration Deployment* screen which starts the synchronization process. <<<



6 Configuration

This chapter should give a brief overview of how to setup the different parts of the USP Secure Entry Server[®] appliance.

Detailed information about different settings and application integration are provided in the help within the Web GUI, the component Administration Guides or in the [USP Customer Knowledge Base](#).

6.1 Network Setup

To run the USP Secure Entry Server[®] appliance, some basic network settings are required. Otherwise it will not be possible to set and deploy any component configuration.

All these settings are located in *Configuration*→*System Settings*→*Network Settings*.

6.1.1 Appliance Hostname

The appliance host name helps to identify the appliance. The configuration field is located in the tab *System*.

6.1.2 Interface Settings

In the *Interface* tab, the network interface assignment as well as the IP addresses for all operational interfaces can be set.

Network Interface Roles

The roles are usually preset correctly, but can be changed if necessary. The *external* and *internal* interface roles must have an assignment (except in [Standalone Appliance mode](#), where the *external* interface is not used).

Internal IP Address

An IP address for the *internal interface* is required. An additional gateway is optional and only needed when the target servers are not in the same subnet. It is possible to specify either an IPv4 address, an IPv6 address, or both.

Administrator Interface

This interface is not in use per default. It can be enabled by checking the *Enable interface* checkbox and entering the IP address information. It is possible to specify either an IPv4 address, an IPv6 address, or both.



Important

When the *administrator* interface is enabled, access to the Web GUI via the *internal* interface is not possible anymore. After activation of the configuration, the operator must connect again to the Web GUI using the *administration interface* IP address.

6.1.2.1 NTP Server

Using an NTP (Network Time Protocol) server is recommended. Especially when having a High Availability cluster. The setting is located in the tab *Network Services*.

Multiple NTP servers can be specified for redundancy. It is possible to use both IP addresses (IPv4 and IPv6) or hostnames.



6.1.2.2 DNS Server

Using an (internal) DNS (Domain Name System) server is recommended when backend systems are configured to use hostnames. The setting is located in the tab *Network Services*.

Multiple DNS servers can be specified for redundancy. It is possible to define IPv4 and IPv6 addresses for DNS servers.



Warning

Use DNS Servers with extra caution because of possible DNS attacks.

6.1.2.3 Routing

Depending on the network setup, special routing settings are required. For each target server, an automatic route will be created using the *internal interface*. Manually added routes can overwrite the automatically created routes. These will be marked accordingly.



Warning

Be cautious when adding manual routes. If misconfigured, it can lead to improper functioning of the USP Secure Entry Server[®] and even preventing operators from accessing the Web GUI. <<< == Web Application Firewall Setup

The Web Application Firewall configuration has a hierarchic structure and is divided in the three sections:

General Settings

Also called *base server settings*. These are globally applied settings like server sizing or default SSL protocols. The settings are inherited by any virtual host.

Virtual Host

A virtual host is represented by a host name and an IP address (IPv4 and/or IPv6) and other virtual host wide configuration (e.g. authentication service or SSL settings). The virtual host matching the host of the URL is selected to serve the request.

Location

Locations provide fine a grained configuration structure using the URL path. For instance, in location configurations it is defined to which target server the request should be forwarded to. A location configuration inherits the settings from its virtual host and from all its parents (in case of a sub-location).

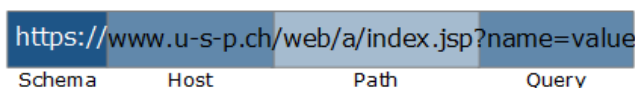


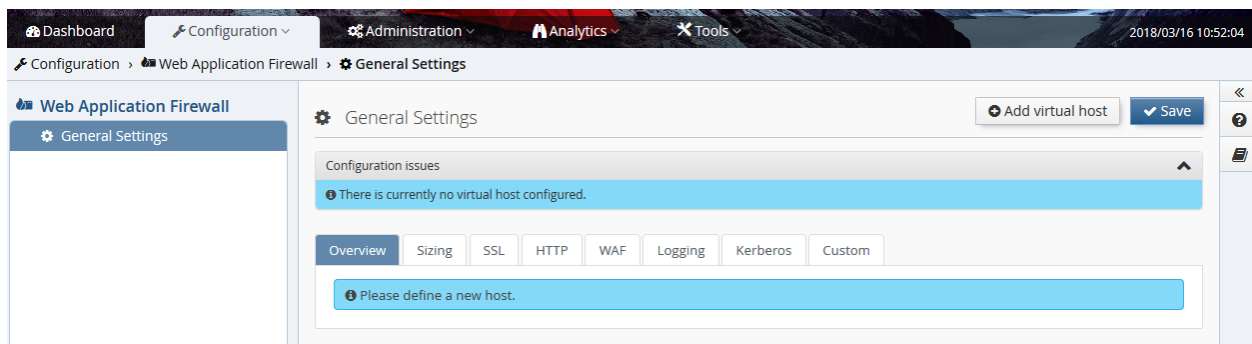
Figure 8: URL components

6.1.3 Create a new virtual host

To serve any request via USP Secure Entry Server[®] a virtual host must be created.



1. Create a new virtual host by pressing the button "Add virtual host" in the *Configuration*→*Web Application Firewall*→*General Settings* view.






2. Enter the virtual host details.



In this step it is also possible to import a configuration of another virtual host which was previously exported, for instance from another USP Secure Entry Server®. The *Security Profile* enables protection against certain attack patterns (XSS, SQL injection). You can choose to block such attacks by selecting the Mode "Prevent" or just to log it using "Detect".



3. Each virtual host must have SSL certificates. After the virtual host is created the SSL (server) certificate and the CA certificate chain must be added in the *SSL* tab of the virtual host configuration. Select the certificate from the corresponding drop-down menu.



- If new certificates must be created, change to the "Certificates and Keys" screen, either by clicking on the corresponding menu entry to the left, or by clicking the small  icon next to the certificate selection drop-down box.

Name	Private/Secret Key	Certificate	Actions
testsite1_443	Private/Secret Key Key size: 1024 (weak) Modulus: 70791672604940222519edcd29299df02224c61	Certificate X.509 Subject: EMAILADDRESS=simon.egli@u-s-p.ch, CN=Test, O=USP, L=Zurich, ST=ZH, C=CH Issuer: CN=mydemoqa, O=USP, ST=ZH, C=CH Valid from: Fri Nov 04 11:21:00 CET 2011 Valid to: Sat Nov 03 11:21:00 CET 2012 (expired) Signature Algorithm: SHA1withRSA (weak) Serial Number: 7 Fingerprint: c6:85:6b:57:c5:8c:32:e5:53:77:c2:8c:12:85:f8:9a:7c:63:1a:4c Modulus: 70791672604940222519edcd29299df02224c61	 

Name	Certificate	Actions
testsite1_443	Certificate X.509 CA (self-signed) Subject: CN=mydemoqa, O=USP, ST=ZH, C=CH Issuer: CN=mydemoqa, O=USP, ST=ZH, C=CH Valid from: Wed Aug 03 13:08:00 CEST 2016 (expired) Valid to: Wed Aug 03 13:08:00 CEST 2016 (expired) Signature Algorithm: SHA1withRSA (weak) Serial Number: 1 Fingerprint (SHA-1): 3a:5a:29:82:73:88:3a:7a:c0:1b:05:9e:14:b8:79:bd:b5:83:48:a5 Modulus: eb97963afecdf560422968759c5f71dea9d99546	 

Name	Secret Key	Actions
SES Ticket encryption key	Secret Key: TripleDES	 

This screen also shows warnings related to expired certificates, weak keys etc. The certificates and keys can be generated offline and imported as PEM encoded files. The files must be selected and uploaded by clicking the *Import file* button.

Alternatively, the private key can be generated by the USP Secure Entry Server[®] appliance. Creating a new private key and certificate consists of the following steps:

- Create a new private key on the USP Secure Entry Server[®] appliance using the *Create Key* button at the top.
- Create a Certificate Signing Request (CSR) using the *Create CSR* button at the top. Follow the instructions given by the Administration Web GUI. At the end, the CSR will be sent as a text file to the browser, so a "Save as. . ." dialog will appear that allows to store the CSR as a text file for further usage.
- Send the CSR to the certificate registration authority which will then provide you the servers certificate as well as the root CA certificates.
- Import the PEM encoded server certificate and the root CA certificate chain into the USP Secure Entry Server[®] appliance.

Alternatively, you may also create and use self-signed certificates, which is usually very useful in testing environments. To generate such certificates, click the *Create self-signed certificate* button at the top.



Warning

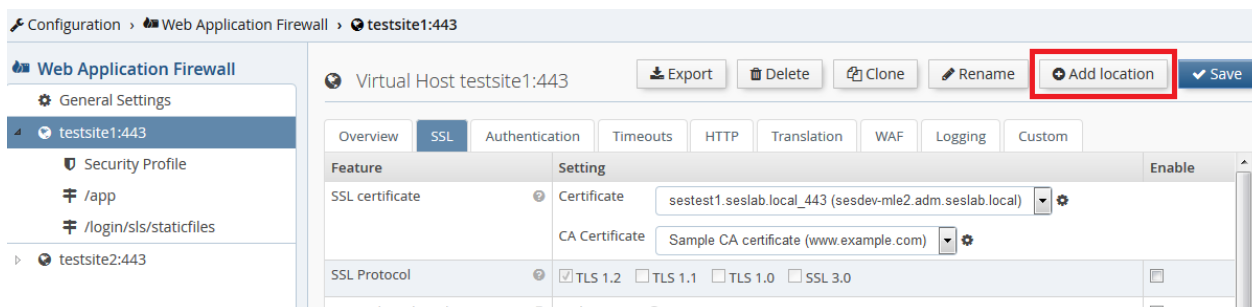
Key files are exported via the backup function, and optionally also with the configuration export function. The backup will always contain the keys, while the export will only contain them if the checkbox "Include private keys" has been checked.



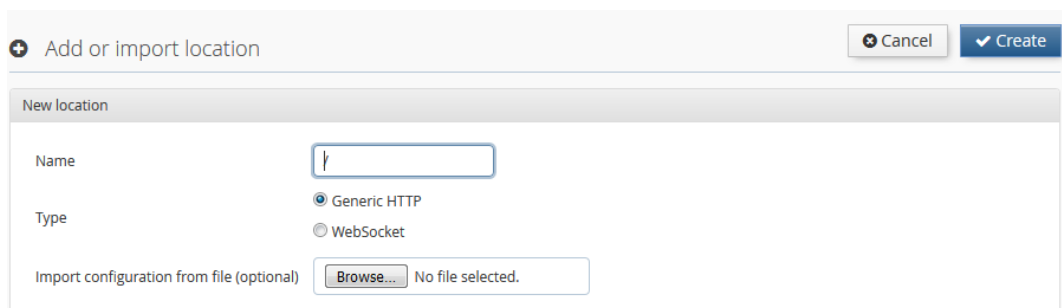
6.1.4 Create a new location

For each virtual host at least one location must be created as otherwise no target server can be served.

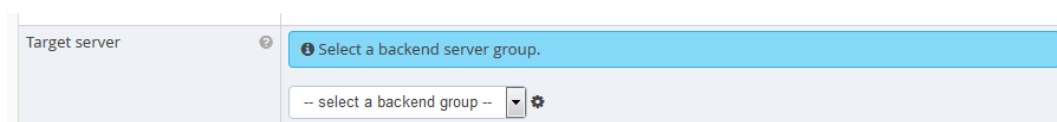
1. Create a new location by pressing the button *Add location* in the virtual host view.



2. The location name matches the request path. The name must start with /, e.g. */web/application*.



3. Each location must define a target server to which the requests are forwarded to. The target server, which must be already defined in the *Target Manager*, can be selected from the drop-down list. The target manager can be accessed either via the "Target Manager" menu item in the WAF view or by clicking icon next to the drop-down list.



4. Authentication is by default enabled for any new location and can be adjusted with the "Access Area" drop-down list. See [Access Area](#) for more details about the different authentication levels.



5. Access to the location is by default only possible using HTTPS protocol. It is possible to switch to HTTP only or using both.





6.1.4.1 Predefined Locations

Some locations are predefined by the USP Secure Entry Server[®] appliance and can not be changed or should not additionally created by the user.

- /htx-error-pages
All error documents of the WAF HTTP Listener and the WAF HTTPS Listener are available under this location.
- /srm-error-pages
The error documents of the WAF Request Manager are available under this location. These are either HTML or SHTML (using SSI, server side includes) documents.
- /cookie-check
Every browser connecting to the server gets redirected to this location where the USP Secure Entry Server[®] verifies that the client accepts HTTP cookies.
- /sil-bid-check
This location provides the JavaScript scripts used to validate the browser ID when performing session fixation.
- /login/sls
This is the location of the local Authentication Service. The Web GUI allows limited configuration changes to this location.
- /login/sls/staticfiles
Location which is used to display the images on the login page of the local Authentication Service.



6.1.5 Security Profile

Every virtual host has a Security Profile which defines the active rules to detect potential attacks. You can change the Security Profile by either applying a template or by customizing the settings manually.

Mode: The mode defines the actions to be taken when the profile is applied to traffic:

Mode	Description
Prevent	This will block traffic that is identified as suspicious by the Security Profile.
Detect	Identified suspicious traffic is logged, but no blocking will occur.
Off	Traffic is not verified with respect to the Security Profile settings.

Profile Settings: The profile settings can be edited by clicking on "Settings" in the "Profile" menu. Depending on whether your profile is based on "Lean" or on "Typical/Fully Fledged", the following settings are at your disposal:



Security Profile for sesdev-msr1.ext.seslab.local:443

This profile is a modified version of template "Fully Fledged"

Template Description:
This profile detects a broad range of attacks. It will block a request when 2 issues are found.

Mode: Prevent

Profile Settings

Enforcement: Loose Tight

Request Inspection | Response Inspection

Request Rules

- Scanner Detection
- Protocol Enforcement
- Protocol Attack
- Local File Inclusion Attack
- Remote File Inclusion Attack
- Remote Code Execution Attack
- PHP Application Attack
- Cross Site Scripting (XSS) Attack
- SQL Injection Attack
- Session Fixation Attack

Request Body Access

- Access Request Body
- Inspect Size Limit: 128.00 kB

Request Body Parsing

- Parse XML
- Parse JSON

Request Rule Exceptions ➕ Add Exception

Rule	Location	Request Part	Action
920280 Missing Host Header	/csrf	HTTP Header	
920350 Host header is not an IP address	/csrf	HTTP Header "Host"	
920440 Restrict file extensions	/bad.vbs	Tx "extension"	
930120 OS File Access		Cookie "file"	
933100 Opening/Closing PHP Tag	/customers/app	Parameter "php"	
933100 Opening/Closing PHP Tag	/members/app	Parameter "php2"	
941100 XSS Attack detection via libinjection	/customers/app	Parameter "javascri"	

Figure 9: Security Profile

6.1.5.1 Settings for "Lean"-based Security Profiles

This type of profile is based on the rules which were shipped prior to USP Secure Entry Server® 5.2.

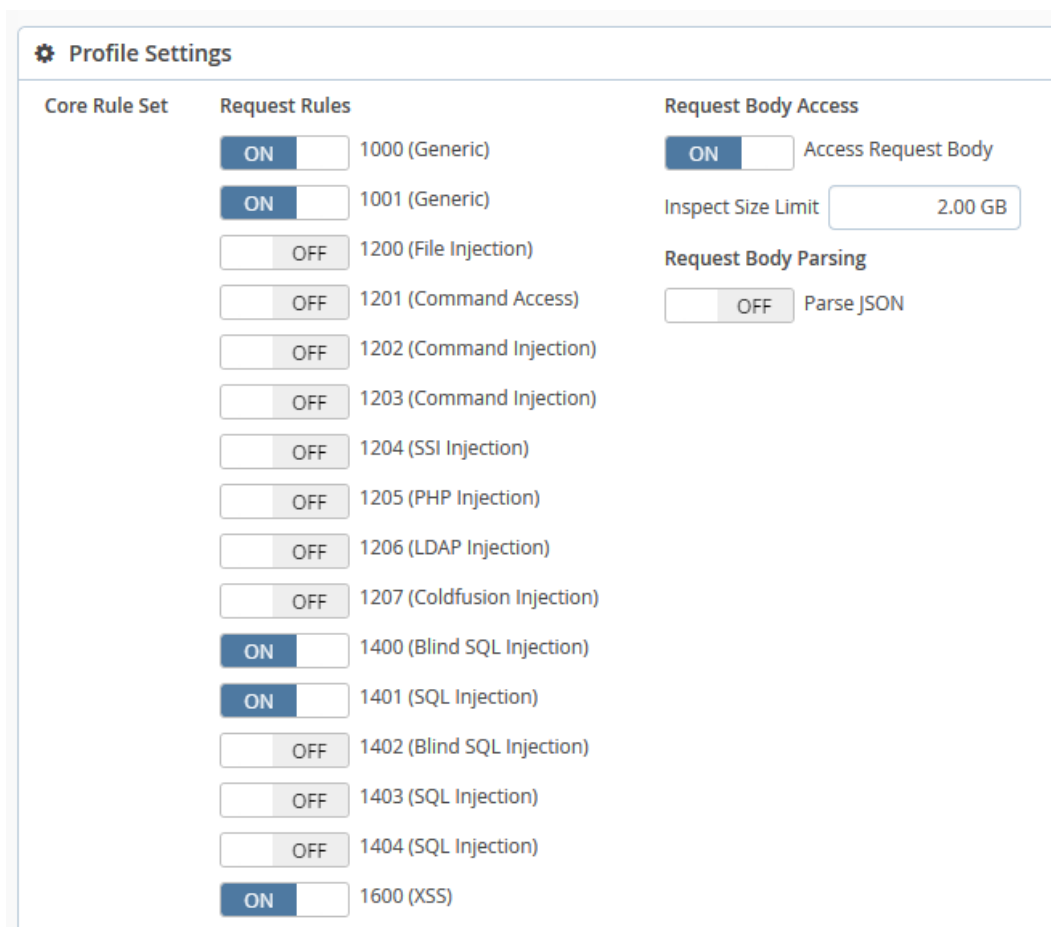


Figure 10: Settings for a "Lean"-based Security Profile

Request Rules: Every rule in this profile checks requests for a certain type of attack. You can enable or disable any of the rules. If the current mode is "Prevent" and an enabled rule detects an anomaly, the affected request is blocked. If a rule is disabled, it won't log nor block any suspicious requests.

Access Request Body: Allows to choose whether to apply rules to request bodies or not. Please be aware that if this setting is disabled, POST parameters and other content submitted in the request body will *not* be inspected.

Inspect Size Limit: This puts a limit on inspecting request bodies. It is used to keep the processing load on an acceptable level. A higher limit will consume more processing time. Request bodies which are larger than this value will still be inspected, but only up to this limit. The limit can be specified in bytes (B), kilobytes (kB), megabytes (MB) or gigabytes (GB).

Parse JSON: Enabling JSON parsing will apply the rules to JSON payloads.

Validate JSON Syntax: This is a special rule which checks the syntax of JSON requests. If the syntax is invalid and the current mode is "Prevent", then such requests are blocked.

6.1.5.2 Settings for "Typical/Fully Fledged"-based Security Profiles

This type of profile comes with an enhanced, accurate rule set which was designed to detect and prevent today's sophisticated web attacks.

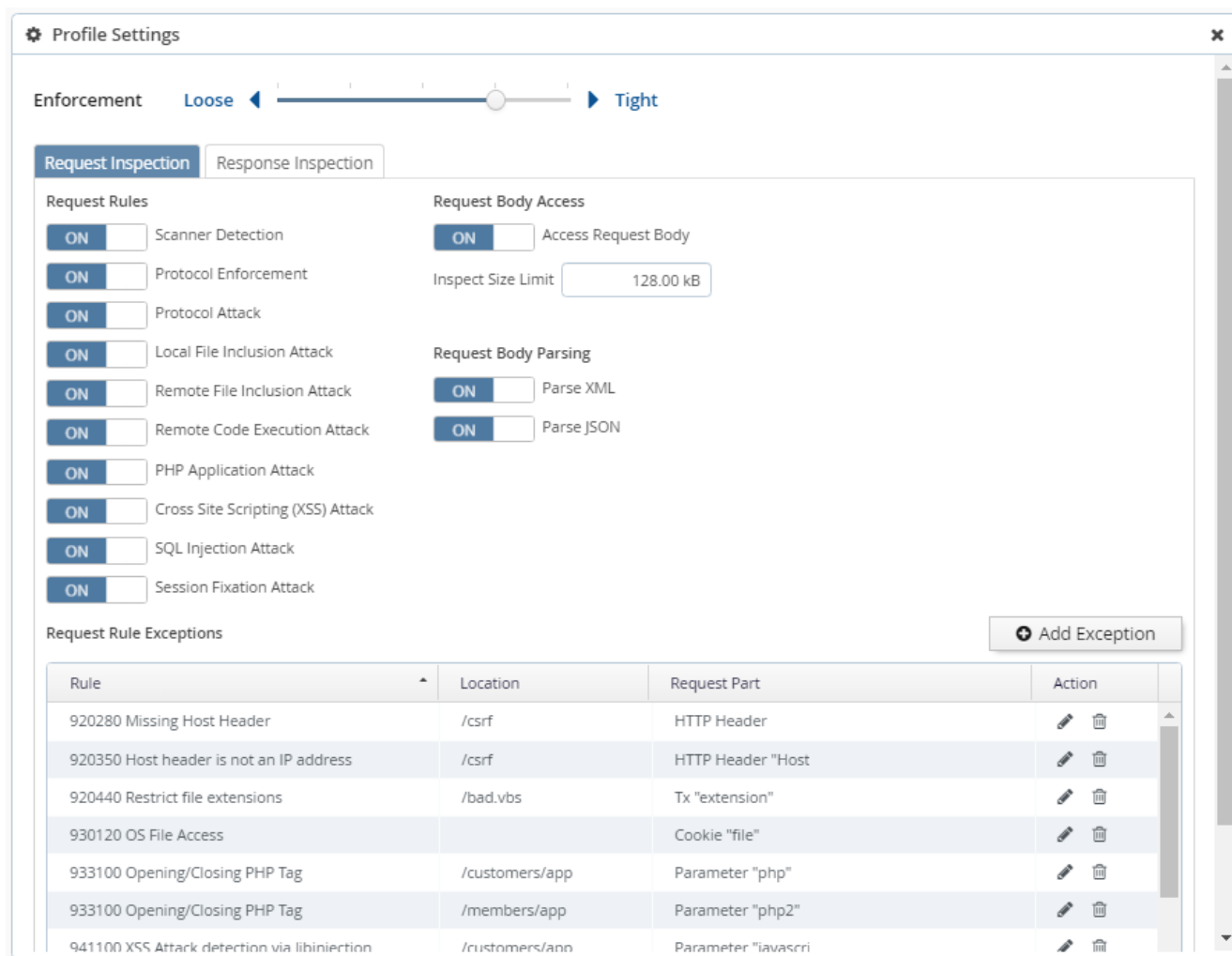


Figure 11: Settings for a "Typical/Fully Fledged"-based Security Profile

Enforcement: Enforcement defines how strictly suspicious requests will be blocked. This has only an effect if the mode is set to "Prevent". The enforcement levels behave as follows:

Level	Description
Tight: 5	Requests with one or more critical anomalies will be blocked
4	Requests with 2 or more critical anomalies will be blocked
3	Requests with 3 or more critical anomalies will be blocked
2	Requests with 5 or more critical anomalies will be blocked
Loose: 1	Requests with 10 or more critical anomalies will be blocked

Request Rules: Request rules are organized in categories. Enabling or disabling a category will enable or disable all rules contained within.

Access Request Body: Allows to choose whether to apply rules to request bodies or not. Please be aware that if this setting is disabled, POST parameters and other content submitted in the request body will *not* be inspected.

Inspect Size Limit: This puts a limit on inspecting request bodies. It is used to keep the processing load on an acceptable level. A higher limit will consume more processing time. Request bodies which are larger than this value will still be inspected, but only up to this limit. The limit can be specified in bytes (B), kilobytes (kB), megabytes (MB) or gigabytes (GB).



Parse XML: Enabling XML parsing will apply the rules to XML payloads.

Parse JSON: Enabling JSON parsing will apply the rules to JSON payloads.

Request Rule Exceptions: This table lists all request rule exceptions. A request rule exception disables a rule based on certain conditions. Conditions may include a request part (for example a HTTP header) with a specific name (for example the "User-Agent") as well as a specific location (including children thereof). Exceptions can be created either by clicking onto "Add Exception" or by using the "Advanced Learning" functionality.

By clicking onto an icon next to an exception you can invoke the following actions:

- **Edit:** Opens an editor where you can change the rule and conditions of an exception.
- **Delete:** Will delete the exception after confirmation.

Add Exception: Clicking on this button opens an editor which allows you to add a new request rule exception. The following parameters are available:

- **Rule** Choose the rule which should be disabled.
- **Request Part** Depending on the selected rule, you can specify a condition based on a request part.
- **Request Part Name** Depending on the selected request part, you can specify a name as an additional condition.
- **Location** Optionally specify a location. You can choose a defined location or enter an arbitrary one.

Response Rules: Response rules are organized in categories. Enabling or disabling a category will enable or disable all rules contained within.

Note

Enabled response rules will be applied to the response body and have a significant impact on processing load and request delay. You should enable them only selectively!

Response Rule Exceptions: This table lists all response rule exceptions. A response rule exception can disable a rule completely or just for a certain locations. Exceptions can be created either by clicking onto "Add Exception" or by using the "Advanced Learning" functionality.

By clicking onto an icon next to an exception you can invoke the following actions:

- **Edit:** Opens an editor where you can change the rule and location of an exception.
- **Delete:** Will delete the exception after confirmation.

Add Exception: Clicking on this button opens an editor which allows you to add a new response rule exception. The following parameters are available:

- **Rule** Choose the rule which should be disabled.
- **Location** Optionally specify a location. You can choose a defined location or enter an arbitrary one.

Advanced Learning: With "Advanced Learning" you can optimize the Security Profile using recorded requests. The goal is to reach the highest enforcement level without risking false positives.

Note

It is crucial that "Advanced Learning" uses only safe requests for determining false positives. Use it only in a controlled test-phase/environment or restrict it to safe requests by known client IP address or range.

**Note**

"Advanced Learning" is not available if "Advanced Log Management" is disabled or the Security Profile is based on "Lean".

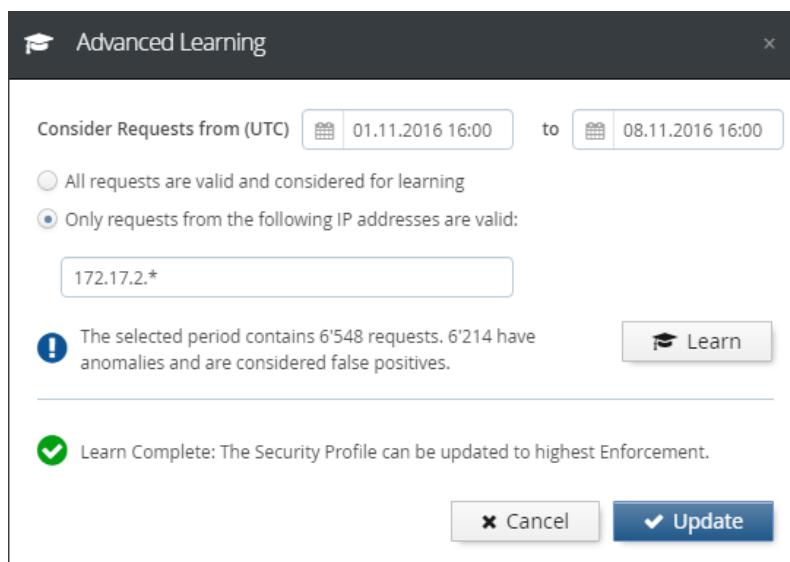


Figure 12: Advanced Learning

In the "Advanced Learning" dialog, you have the following options:

- **Consider requests from/to (UTC)** You can enter a time period for requests to be considered. If you choose a date before the first recorded request or a date after the last recorded request, it will be corrected automatically.
- **All requests are valid** Choose this option if you know that all recorded requests are safe and contain no attacks.
- **Only requests from the following IP addresses are valid** Choose this option to consider only requests which came from specific IP addresses or ranges.
- **Learn** This button triggers the Advanced Learning based on the considered requests. You can repeat the learning when you choose to use different options.
- **Update** After successful learning, you can click this button to update the current Security Profile.
- **Cancel** Closes the "Advanced Learning" dialog without changing the Security Profile.

Save as Template: Saves the current Security Profile as a template. Templates can be applied to other Virtual Hosts or exported for use in other USP Secure Entry Server[®] instances. If you use the name of a previously saved template, it will be overwritten. Overwriting a template does not modify the Security Profiles of existing Virtual Hosts. Names of built-in templates cannot be used.

Replace by Template: Replaces the current Security Profile settings with the settings from a chosen Template. Any built-in or previously saved Template can be selected.

6.1.6 Target Manager

The target server manager is located in the *Web Application Firewall* view. Any target server to which the requests should be forwarded to must be defined as a tuple of hostname and/or IP address, and port number.



The view contains a list of all backend targets:

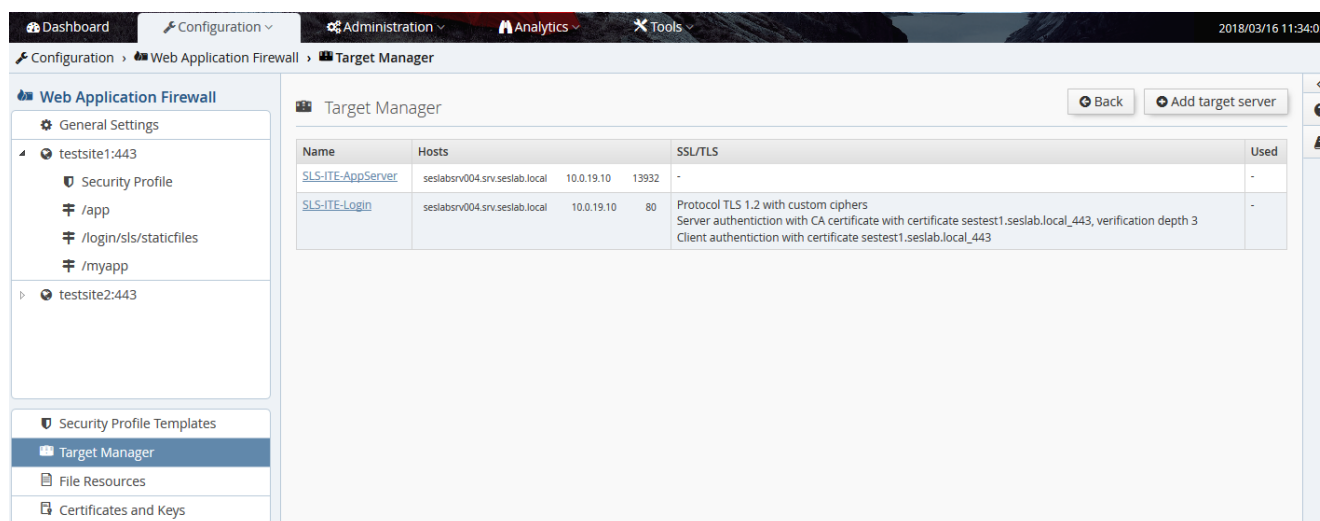


Figure 13: Target Manager

The table contains one line per target, or target group. "group" because one target can contain two or more actual backends, to provide load-balancing. The table has 3 columns:

- Name: The human-readable name assigned to the backend target. This text label will be shown in the drop-down selection box of a location in order to choose the target for that location.
- Hosts: The actual list of backend host(s), with DNS name and/or IP address, and port number.
- SSL/TLS: The TLS settings for the connection to that backend, if enabled.

To edit a target, just click on the link in the "Name" column. To add a new one, click the *Add target server* button at the top, and this screen appears:



Hostname	IP address	Port
main1.acme.com	192.168.10.15	443
main2.acme.com	192.168.10.16	443

Host header: main1.acme.com:443 main2.acme.com:443

Backends unavailable redirect: -- no redirect --

Load balance by: request count traffic byte count

Figure 14: Edit target server

This view is split into five sections:

- General Settings: Contains the input field for the text label.
- Hosts: Contains the 1-x backend target host servers. To add another host, click on the "+" icon to the right. Optionally, the host header to be sent to the target can be defined.
- Load Balancing: Load balancing between backends can be defined as soon as more than one backend has been defined. Several strategies are available, and it is possible to enable session stickiness.
- Health Check: Enable periodic availability checks for backends. Two kinds of availability checks are available: TCP connect or a configurable HTTP callout.
- SSL/TLS Settings: Configure the SSL/TLS settings to be used for the connection to the target backend.

Always click the *Save* button at the top when changing anything in this screen.

6.1.7 Security Profile Templates

On this screen you can manage the available Security Profile Templates.

**Note**

Built-in Security Profile Templates are not displayed, can't be deleted or renamed.

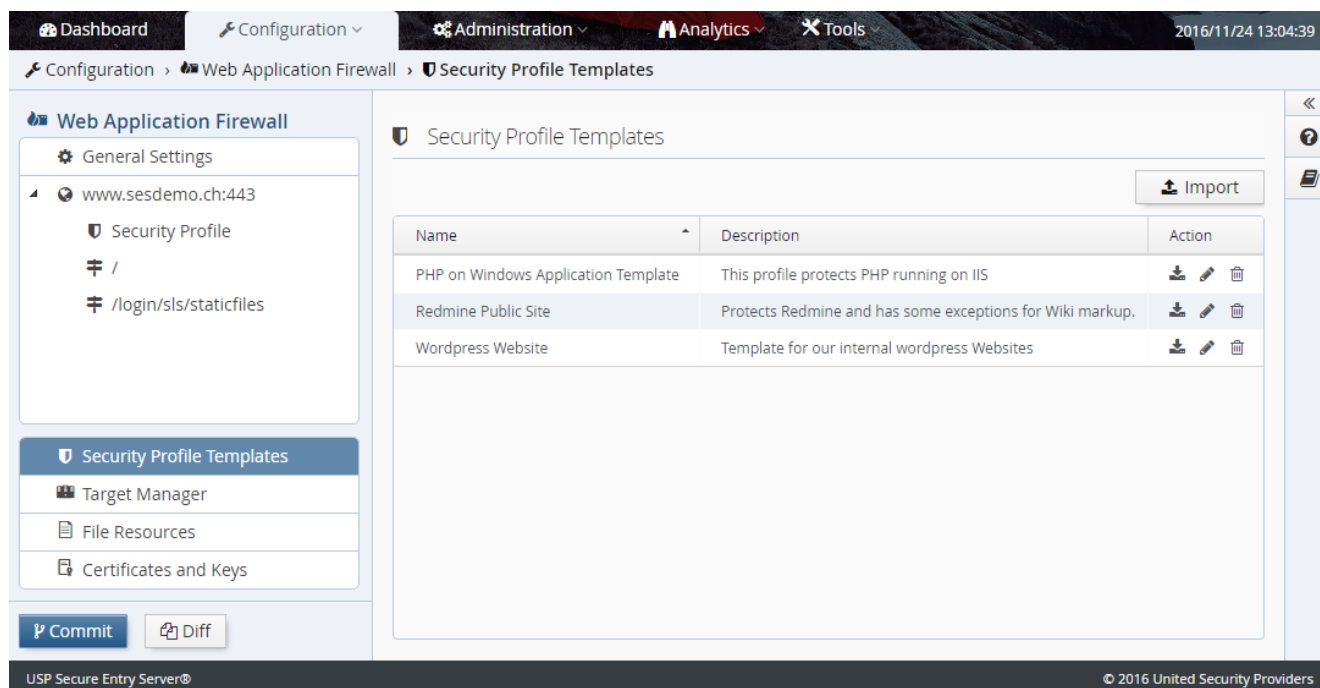


Figure 15: Security Profile Templates

Import Security Profile Template: By clicking on the "Import" button you can import a Security Profile Template which was exported on any USP Secure Entry Server® instance. If a Template with the same name already exists, an editor is opened which lets you enter a different name. If you keep the same name, the existing Template will be replaced. Replacing a Template does not modify the Security Profiles of existing Virtual Hosts. Names of built-in Templates cannot be used.

Security Profile Template Actions: By clicking on an icon of a template you can invoke the following actions:

- **Export:** Exports the selected template as a file. This file can be transferred to another USP Secure Entry Server® instances by importing it there. Exported Templates are encrypted and not intended for manual modification.
- **Edit:** Opens an editor where you can change the name and description of a Template. Names of already saved or built-in Templates cannot be used. Renaming a Template does not modify the Security Profiles of existing Virtual Hosts.
- **Delete:** Will delete the selected Template after confirmation. Deleting a Template does not modify the Security Profiles of existing Virtual Hosts.

IMPORTANT NOTE

If you use custom session cookie names, by means of custom commands, those custom session cookies might get blocked by the ModSecurity rules. In such a case, you will have to add custom exceptions to make sure your cookies will not be blocked. <<< === Authentication Service Setup

The "Authentication Service"(SLS) is a separate component on the USP Secure Entry Server® appliance.



6.1.8 Enabling / Using Authentication

Authentication can be enabled and enforced for any application location in a virtual host. In order to do this, the [Access Area Level](#) must be configured for the location.

Access Area Levels

Any location in any virtual host always has one of three "Access Area" levels:

- Public - Clients can access the location without authentication
- Member - Implies that weak authentication is required
- Customer - Implies that strong authentication is required

"Member" and "Customer" levels have a hierarchical relationship - when a user has been authenticated for a location with "Member" access level, she will still need to authenticate again for locations with "Customer" level. But a user who was already granted access to a "Customer" level location will not have to authenticate again when accessing a "Member" level location.

However, the actual strength of the authentication is defined by the settings of the authentication service. But as soon as a location has an "Access Area" level other than "Public", the WAF will enforce authentication before allowing access to the location. And choosing either "Member" or "Customer" allows to distinguish between locations with lower and higher security requirements, and implement step-up authentication procedures.

The "Access Area" level can be set in the location configuration screen of the *Web Application Firewall* part by selecting either "Member" or "Customer" in the drop-down selection box:

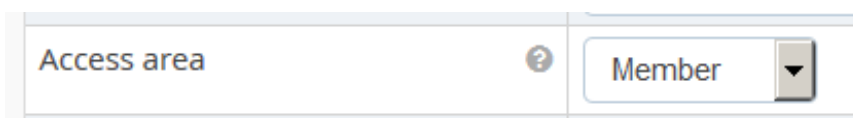


Figure 16: Enable Authentication for Virtual Host

On the virtual host screen, it is possible to define which instance of an SLS to use - either the local (by default) or a remote one. The latter allows to separate the actual WAF functionality from the authentication, by using a [Standalone Authentication Service Appliance](#) on a remote appliance:

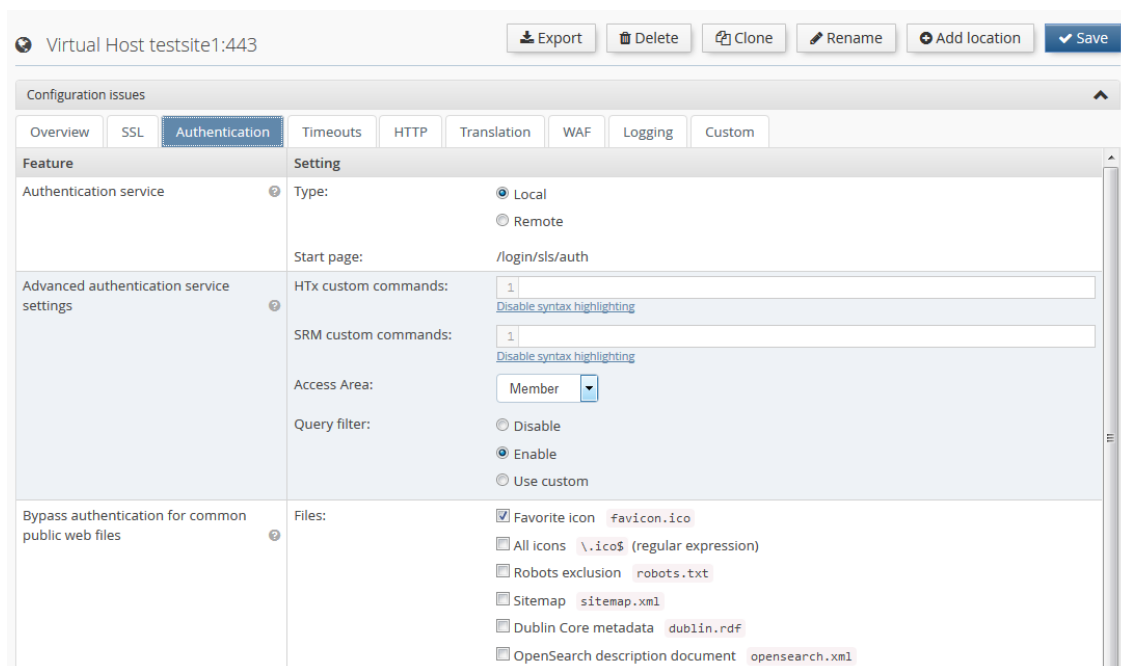


Figure 17: Configure Authentication for Virtual Host

In case of some login procedures like PKI (certificate) based login, it may be necessary to disable the query filter for the SLS, or customize the regular expression.

6.1.9 Authentication Basics

There are two important concepts in the SLS related to setting up a certain authentication flow:

- [Models](#)
- [Adapters](#)



6.1.9.1 SLS Models

A "Model" in the SLS context is a series of connected states that are processed by the SLS during a login session (what pages to show to the user, what backend calls to perform etc.) Basically the SLS is a state machine, where the steps of a login procedure can be configured in a very flexible way. Models are configured with properties, and a simple login model looks like this:

```
model.login.uri=/auth
model.login.failedState=get.cred
model.login.state.1000.name=get.cred
model.login.state.2000.name=do.auth
model.login.state.3000.name=do.success
```

The prefix of a group of properties that define a certain model is always

```
model.<model-name>.
```

followed by either global settings for the model (`uri` and `failedState`) or the various states of the model.

A short explanation of those 5 lines of model configuration:

1. `model.login.uri=/auth`: A global setting for this model. It means that this model will be triggered by a request sent to the SLS on the (default) location `/login/sls/auth`. If another (e.g. password change) model was configured with `model.changePwd.uri=/changePwd`, this flow can be triggered by using the request URI `/login/sls/changePwd`.
2. `model.login.failedState=get.cred`: Another mandatory global model setting - its basically the default error handler. In case of an error during processing the model, the SLS will switch to the `get.cred` state.
3. `model.login.state.1000.name=get.cred`: As the first step, the SLS will show the login page.
4. `model.login.state.2000.name=do.auth`: As the second step, the SLS will invoke the authentication adapter to verify the credentials posted from the login form. Which adapter is used depends on the authentication adapter configuration (see [Login Process Example](#)).
5. `model.login.state.3000.name=do.success`: This final state checks that all credentials provided by the user were actually verified by the adapter, and if so, signals successful authentication to the WAF, while redirecting the user back to the originally requested application.

The numbering in the property state names defines the order of the state. It is recommended to always leave large gaps between the numbers, so that new states can be added in the model later without having to re-number all other states.

Please refer to the "SLS Administration Guide" for more detailed information about available model states.



6.1.9.2 SLS Adapters

Certain model states like `do.auth`, `do.authresponse` or `do.ldap` invoke actions that will perform some kind of backend call (RADIUS, LDAP etc.). The SLS uses various types of adapters to support a number of different authentication standards, such as LDAP, RADIUS PKI, and for a number of different operations, such as authentication, user ID mapping, challenge/response etc. In the following is a short overview of the various adapter types and the kind of operation they support:

- Authentication
 - LDAP
 - RADIUS
 - NTLM
 - RSA (SecurID)
 - HTTP
 - PKI
 - File
- Challenge/Response
 - Simple
 - RADIUS
 - NTLM
 - Google Authenticator
 - H-Net
- Mapping
 - LDAP
 - PKI
 - File

There is also a group of "Other Adapters". Those are adapters that provide functionality that is not directly related to any of the above operations, meaning that those adapters can perform operations that will not necessarily validate any login credentials. For example, the LDAP and HTTP adapter can also be used to perform custom HTTP calls or LDAP operations.

Please refer to the "SLS Administration Guide" for more detailed information about available adapters and how to configure them.

6.1.10 Login Process Example

A typical example of this process when trying to access a web application through a browser looks like this:

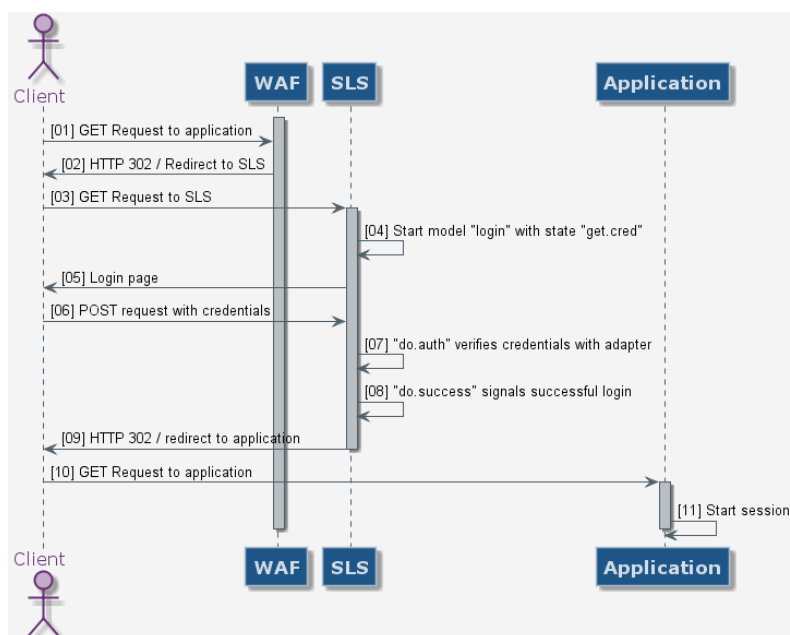



Figure 18: Simple Login Flow

The credential verification happens where the user's identity is actually confirmed by use of credentials like username, password and maybe an additional challenge-/response check with a hardware token.

LDAP Authentication Example

The following example shows which configuration screens are involved when setting up a simple LDAP-based authentication for a location:

1. Set the "Access Area Level" of the location to "Member" as described above and save in *Configuration*→*Web Application Firewall*→*Virtual Host*→*Location*→*Authentication*
2. In *Configuration*→*Authentication Service*→*Adapters*→*Authentication* choose "LDAP" in the adapter type column in the right form, and save.
3. Select *LDAP* in the navigation tree.
4. In the "LDAP Backends" section, enter 1 - n backends, either as IP address or DNS hostname. If DNS hostnames are used, DNS should be enabled in the "System Settings". Also, if multiple backends are configured, choose the target selection mode using the "Selection Mode" drop-down menu. And if the connection should be TLS protected, check the "Use TLS" checkbox.
5. In the section "LDAP Settings", enter the DN of a technical user used for lookup operations, backend-monitoring etc., and the bind DN, and save.
6. Click on *Model* in the navigation tree and select *login* - the default login model.
7. Open the Web GUI help  and copy the "default" login model example content into the model form and save.

After committing and activating the configuration the WAF will enforce LDAP authentication when accessing the application location.



6.1.11 Custom Properties

The appliance GUI does not yet support all features of the SLS authentication service. So in some cases, when a certain functionality needs to be configured as described in the "SLS Administration Guide" and no corresponding page can be found in the GUI, it may be necessary to instead configure the feature with a set of custom properties. This basically corresponds to using "Custom Commands" in the WAF part of the appliance.

So, whenever certain SLS functionality needs to be configured by hand with a few custom properties, set them by selecting the *Custom Settings* entry in the left navigation tree under *Configuration*→*Authentication Service*:

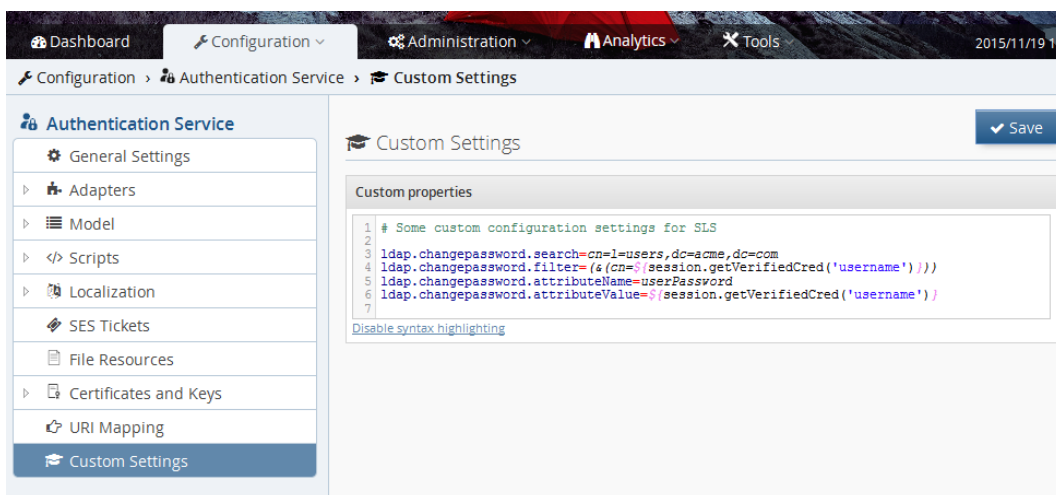


Figure 19: Setting custom properties



Warning

Properties set in the *CustomSettings* field will overwrite the same setting handled by the Web GUI! This might be desired but could also result in an unexpected behavior if used incorrectly!

6.1.12 Setup Authentication Service Standalone Appliance

For creating an Authentication Service Standalone appliance, a fresh installed appliance is recommended. After the software installation is finished, the standalone mode must be activated first.

This is controlled in the Web GUI under *Configuration*→*Manage and Deploy*→*Enabled Services*. Only Authentication Service should be set to *on*.

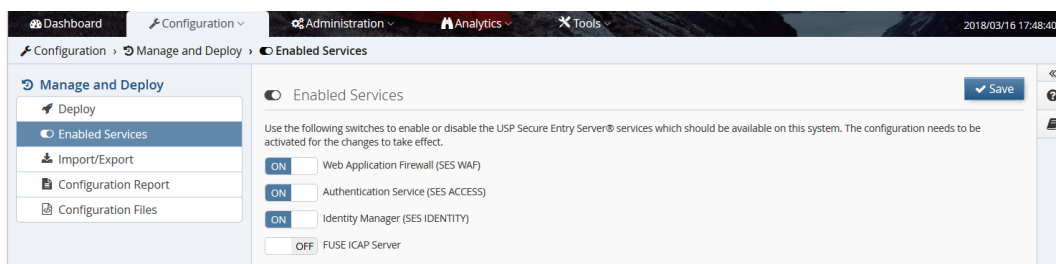


Figure 20: Enable services running on appliance



After this the Authentication Service can be configured in the usual way.

6.1.13 Connect Remote Standalone Authentication Service

To use a remote standalone authentication appliance instead of the local SLS, select "remote" in the "Authentication service" row of the *Authentication* tab in the virtual host settings:

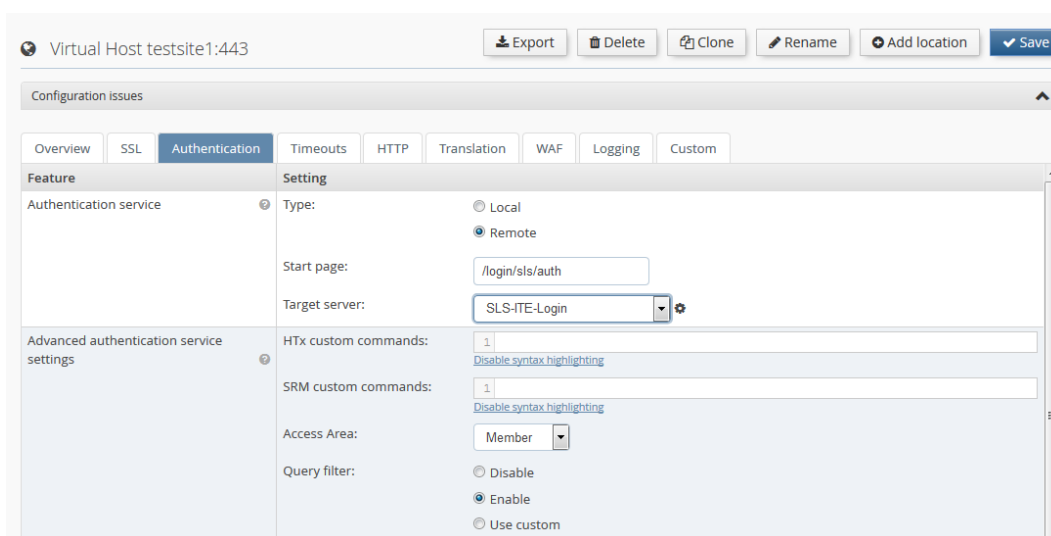


Figure 21: Configuring a Remote Authentication Service



Warning

It is recommended to protect the connection to a Remote Authentication Service with SSL. When configuring a Remote Authentication Service, the "Secure connection (SSL/TLS)" checkbox should always be enabled.

If a Remote Authentication Service is used and the local service is not needed, the local Authentication Service on the Web Application Firewall appliance can be disabled. To achieve this, the Authentication Service must be set to *off* in the *Enabled Services* view.

Note

To be able to do this, all virtual hosts in the Web Application Firewall must have a Remote Authentication Service configured.



6.2 High Availability Setup

High Availability (HA) settings are located in *Configuration*→*System Settings*→*High Availability*.

Important



Unrestricted communication between the appliances must be ensured to use the full High Availability functionality. If the *administration* interface is enabled, all communication is handled via this interface. Otherwise, the *internal* interface is used.

- The failover mechanism communicates via UDP port 6444 (Active/Passive)
 - The Session Transfer uses TCP port 6443
 - Configuration synchronization is handled via TCP ports 443/8443.
-

6.2.1 HA Active/Passive

Active/Passive requires two USP Secure Entry Server[®] appliances.

Configuration

To enable Active/Passive the following steps must be executed on both appliances:

- In the configuration screen, select mode "Active/Passive" from the drop-down list and press *Save*
- Ensure that the secret string is the same on both instances. This is used to secure the communication between the appliances.
- It is recommended to enable the "Auto Mode" checkbox. If enabled, the failover will happen automatically when the active server becomes unavailable.
- In the *Cluster Nodes* panel, the hostname and IP address of the other appliance must be added.
- Press the *Save* button again.
- The configuration must be committed and activated.
- On the *Deploy* view, the *High Availability* control panel appears - showing the status as *not running*.

Configuration Synchronization

Before activating the failover cluster, it is advised to synchronize the component configuration:

- Configure the appliance components:
 - The first appliance must be fully configured, with all virtual hosts and Authentication Service settings. The configuration must be committed and activated.
 - On the second appliance all the different virtual hosts with the **same** IP addresses as on the first appliance must be created. No certificates are required nor must the configuration be committed and activated.
- Synchronize the configuration from the first to the second appliance by pressing *Synchronize* in the *Deploy* view. When successful a message "Successfully synchronized" appears.
- On the second appliance a new entry "Configuration synchronized" is shown in the configuration revision history. No activation is needed.



Start Failover

In this last step the failover service must be activated.

- On both appliances the button *Start* must be pressed in the *High Availability* control panel in the *Deploy* view. New controls will appear.
- By pressing *Takeover* on the first appliance, the appliance will be in mode "active".

Note

On the second failover appliance the WAF HTTP[S] Listener will be shown as down - this is correct. They will start when a failover happens to this appliance.

Be aware, that stopping the HA service, as well as a shutdown or reboot of the appliance, are considered to be controlled maintenance actions, which lead to a regular exit of a node from the HA cluster. Consequently the other node is becoming active, although auto mode is turned OFF. If the auto mode is turned OFF, it will only prevent the passive node from takeover upon an uncontrolled or irregular exit, such as a power or network outage.

6.2.2 HA Active/Active

Active/Active requires at least two USP Secure Entry Server[®] appliances.

Configuration

To enable Active/Active the following steps must be executed on all appliances:

- In the configuration, select mode "Active/Active" from the drop-down list and press *Save*
- Ensure that the secret string is the same on both instances. This is used to secure the communication between the appliances.
- In the *Cluster Nodes* panel, all other HA nodes must be added.
- Press the *Save* button again.
- The configuration must be committed and activated.
- On the *Deploy* view, the *High Availability* control panel appears.

Configuration Synchronization

Before the High Availability cluster is fully functional, the configuration should be synchronized between all nodes:

- Configure the appliance components:
 - The first appliance must be fully configured, with all virtual hosts and Authentication Service settings. The configuration must be committed and activated.
 - On the other appliances all the different virtual hosts with their **own** IP addresses must be created. No certificates are required nor must the configuration be committed and activated.
- Synchronize the configuration from the first to the other appliances by pressing *Synchronize* in the *Deploy* view. When successful a message "Successfully synchronized" appears.
 - On the other appliances a new entry "Configuration synchronized" is shown in the configuration revision history. No activation is needed.



6.2.3 Session Transfer





Session Transfer allows to request session data from another USP Secure Server[®] appliance in the same High Availability cluster. This happens when an user request is served by another appliance which did not initiate the users session.

The sessions are only transferred by request and not automatically distrusted. Therefore when an appliance is taken offline due to maintenance reasons, it should not be restarted/updated until the client session inactivity timeout has passed. Otherwise user session data might be lost.

Session Transfer is by default disabled in an Active/Active setup. It can be enabled in the *Deploy* view, pressing the *Enable Session Transfer* button in the *High Availability* control panel. The load balancer in front of the HA cluster should enforce session-stickiness, otherwise the sessions are transferred unnecessarily often.

6.2.4 High Availability Status

On the dashboard, the status of each HA appliance node is shown. The status are:

-  **Active**: the node is up and running, ready to serve requests.
-  **Offline**: the node is down, either in maintenance or a failure occurred.
-  **Standby**: the failover appliance in a Active/Passive mode is standby ready to take over.
-  **Unknown**: the status of the node can not be identified.



6.3 Automatic Certificate Management Environment (ACME)

The ACME protocol defines the communication protocol between the CA and the web server, allowing to automatically deploy TLS certificates and eases the pain of the certificate issuing and renewing process. The ACME protocol has been introduced by the Internet Security Research Group (ISRG) with RFC 8555 and pushed with their own non-profit CA "Let's Encrypt™".

This mechanism can be used in the USP Secure Entry Server® to automatically manage and renew the certificates for WAF virtual hosts.

6.3.1 Preconditions

- An additional license must be obtained to be able to use the ACME feature - contact your account manager.
- Any virtual host using ACME must be accessible by the CA over TLS on port 443
- The USP Secure Entry Server® appliance must be able to connect defined CA AMCE API endpoint (DNS & routing)

For high availability setups Active/Passive and Active/Active:

- The appliances within the cluster must be able to connect to each other on TCP port 22 via the admin interface resp. internal interface if no admin interface is configured.

6.3.2 Limitations

- Only challenge type TLS-ALPN-01 is supported.
- Other ports than 443 for virtual hosts are not supported by the ACME protocol
- Wildcard certificates are not supported (requires DNS challenge)
- EAB or other authorization means are not supported

6.3.3 Migration to ACME managed certificates

When you migrate your self-managed certificate setup to ACME, we recommend you to do a step by step vhost migration and validation. This is due the rate limiting which are enforced by the CAs. Check the rate limiting documentation of the CA in use.

For "Let's Encrypt™" the rate limiting documentation you can find under <https://letsencrypt.org/docs/rate-limits/>

6.3.4 Configuration

The main configuration tab is located under *Configuration*→*Web-Application Firewall*→*Certificates and keys*→*Automatic Certificate Management (ACME)*. *



Certificates and Keys

Certificates and Keys Automatic Certificate Management (Acme)

Certificate Authority	<input type="text" value="https://boulder-ait.company.com/"/>
CA Certificate	<input type="text" value="boulder-AIT-ca (boulder)"/>
Challenge Type	<input type="text" value="http-01"/>
Contact Email	<input type="text" value="admin@company.com"/>
Http Proxy	<input type="text"/>
External Account Binding (EAB)	Key ID <input type="text"/>
	HMAC Key <input type="text"/>
Graceful Cron Timer	<input type="text" value="daily"/> at <input type="text" value="00:00"/>

In this tab you have the possibility to enter the "Certificate Authority URL" endpoint and your contact email address. The API endpoint for "Let's Encrypt™" is documented under <https://letsencrypt.org/docs/acme-protocol-updates/>

The CA Certificate is used to validate the certificate of the CA URL endpoint. For "Let's Encrypt™" the validation certificate is available by default. If you are using another CA, then please upload the corresponding CA certificate for validation under "Certificate and keys" and select it in the dropdown list.

There are two supported types of ACME challenge used to prove domain ownership. If "http-01" is selected, the SES must be reachable from the Internet on port 80.

Renewed certificates are not automatically active and the WAF must do a graceful restart first. The "Graceful cron time" defines a time schedule when the WAF HTS is automatically gracefully restarted. It is recommended to choose a regular frequency (e.g. once a day or once a week).

The other option is to disable the automatically restart, but then the graceful restart must be triggered manually as soon as new certificates are available.

In a HA Active/Active setup it's important that only one cluster node triggers the renewal process. The "Master ACME Node" flag indicates which node carries the responsibility for this. As the renewal process happens early enough before the certificate expiry, it's also not a problem if the selected master node is not available during a short period in time due to maintenance or failure and the flag must not necessarily be changed. Should the master node be offline for a long period of time, the fallback process on the second node will try to renew the certificates at a later stage.

6.3.5 Enable ACME for a vhost

To enable ACME on a vhost you must select the checkbox "Automatic certificate management (ACME)" *Vhost*→*SSL*→*SSL Certificate* *

Virtual Host acme.renewal1.gg:443

Overview **SSL** Authentication Maintenance Timeouts HTTP Translation WAF Logging Custom

Feature	Setting	Enable
SSL certificate	Certificate <input type="text" value="Sample certificate (www.example.com)"/>	<input type="checkbox"/>
	CA Certificate <input type="text" value="Sample CA certificate (www.example.com)"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/> Automatic certificate management (Acme)	<input type="checkbox"/>



It's possible to define specific certificates from the drop-down list in combination with ACME. The certificates are used till the ACME process for the vhost is finished and graceful restart is completed.

If no certificate is selected, the ACME module will use automatically generated fallback certificates. Until the ACME process is finished, and a graceful restart was triggered, the access to this vhost is blocked with a 503 HTTP response code.

6.3.6 Config Export & Backup ACME

ACME certificates and keys are not part of the configuration export or backup. In case a backup is restored, new certificates are requested from the CA.

6.4 User Management

The USP Secure Entry Server[®] appliance uses its own user management. For each operator, an individual user account should be added for auditing changes done in the configuration.

Only a user with administration role can add, edit or delete users. The user management is located under *Administration* → *Users*. Each user can change its password and some other user details by opening the *Account* view - the link is located next to the *Log out* button.

Note

The user management is not included in the configuration lifecycle, reloading an old configuration will not restore old user account or passwords. However, the user accounts are included in the full system backup. After restoring an old backup, the old user accounts and passwords are active.

A user can be set to status *inactive*, disallowing logins until the user is reactivated again.

6.4.1 User Roles

There are four different roles:

Administrator

Having full access to the system and is allowed to change or update the appliance system.

Configurator

Is allowed to update the configuration of the components, but can not activate it.

Deployer

Can not change the configuration, but is allowed to activate a certain committed configuration.

Viewer

Can not change or activate configuration, but can view the configuration and analyze log files.

Table 9: User role permissions

Permission	Administrator	Configurator	Deployer	Viewer
View dashboard	✓	✓	✓	✓
View configuration	✓	✓	✓	✓
Change and save configuration	✓	✓	✗	✗
Commit configuration	✓	✓	✗	✗
Activate configuration	✓	✗	✓	✗



Table 9: (continued)

Permission	Administrator	Configurator	Deployer	Viewer
View and edit users	✓	✗	✗	✗
Appliance control actions	✓	✗	✗	✗
Invoke appliance update	✓	✗	✗	✗
View and download logs	✓	✓	✓	✓
View events	✓	✓	✓	✓
View traffic analyzer	✓	✓	✓	✓
Use SLS Data Protector	✓	✓	✓	✓
Use connectivity check	✓	✓	✓	✓

7 Operation

7.1 Configuration Backup & Recovery

There are two types of configuration backups. They differ in the files included in the backup archive:

- **Configuration Export**: containing only the latest configuration (WAF, SLS, IDM and System).
- **Full System Backup**: is a full system backup, including configuration commit history, server private keys and certificates.

7.1.1 Configuration export

A configuration export will provide a tar archive for downloading. The default file name contains prefix "*sesconfig*" with the hostname and the date. The archive can be downloaded in the Administration GUI *Configuration*→*Manage and Deploy*→*Import/Export* by pressing the *Export* button.

7.1.2 Configuration import

The import can be initiated in the same view as the export. After importing the archive the configuration is marked as "uncommitted" and must be committed and activated to apply the changes.

7.1.3 System backup

A system backup will provide a tar archive for downloading. The default file name contains prefix "*sesbackup*" with the hostname and the date. The archive can be downloaded in the Administration GUI *Configuration*→*Manage and Deploy*→*Import/Export* pressing the *Backup* button. This action is only available for users with administration privileges.

7.1.4 System recovery

A system recovery process includes the following steps:

1. Upload a tar archive to the server using the *Recover* button in the same view as the system backup.
2. This task loads the backup data into the server. Even if the recovered settings have not been activated yet, the server has now recovered its user management configuration.
3. To finish the recovery process, the configuration must be activated again in the *Deploy* view.



7.1.5 Automated remote backup

Backup archives can be automatically pushed to a remote server, either on a daily or weekly basis, or based on a custom schedule. If the "custom" scheduling option is selected, the backup interval must be configured with the common CRON job syntax in the text input field. The backup files are copied using the SCP protocol.

Automatic backup can be enabled by configuring the remote backup server in the *Remote Backup* tab under *Configuration*→*System Settings*→*Network Settings*:

IP address

IP address of the server used for storing the backups.

Gateway

Gateway router IP address; the default value is the gateway address of the internal interface.

User name

User which is used to login on the remote server.

Directory path

Absolute directory path where the backup files will be stored. Needs to be writable by the user specified above.

Scheduling

Daily (at 4:00AM every day), weekly (at 4:00AM on Saturdays) scheduling or a custom setting option that allows to define the schedule in a common CRON job notation.

After activating the modified configuration, a SSH public key will be presented in *Configuration*→*Manage and Deploy*→*Import/Export*→*Remote Backup*. This key must be registered on the remote backup server so that logins using public/private keys are possible. If using OpenSSH, the key must be added to the file `~/.ssh/authorized_keys`. Set the permissions of the `~/.ssh` directory and its containing files so that they may be only accessed by the current user.

Click on the button *Execute* to manually start the backup process, and verify that the backup is copied to the remote backup server.

7.2 Appliance Update

United Security Providers AG publishes regularly software updates for the USP Secure Entry Server®. This so called update image can be downloaded from the customer portal.



Important

United Security Providers AG recommends to keep the USP Secure Entry Server® always up to date! It is advised to create a [full system backup](#) before installing a new appliance release.

The update file must be downloaded to the operator machine and can then be applied using the Administration GUI. In the screen *Administration*→*Software Update*, the file can be selected and uploaded using the *Import* button. After the upload is completed, a new button *Install & Reboot* appears. Clicking on this button will actually install the new USP Secure Entry Server® release. To complete the installation, the appliance will reboot automatically.

The update can apply automatic configuration updates, which will also automatically be committed, but not activated. Therefore, after the appliance has restarted, the updated configuration must always be manually activated.

Note

Some updates need manual configuration changes by the operator. Such changes are generally documented in the migration guides provided with the new release.



Should the update process fail under any unforeseen circumstances and access to the Administration GUI can not be restored, the appliance must be reinstalled with the previous USP Secure Entry Server® version and the system configuration must be restored using the [system recovery](#) process.

7.3 Log Management and Analysis

7.3.1 Log Management

The log files are crucial for analyzing any problems or incidents. Depending on the load which is processed by the USP Secure Entry Server® the log file can grow very big. As the disk space is limited the log files must be properly managed.

The log management is located under *Configuration*→*System Settings*→*Log Management*.

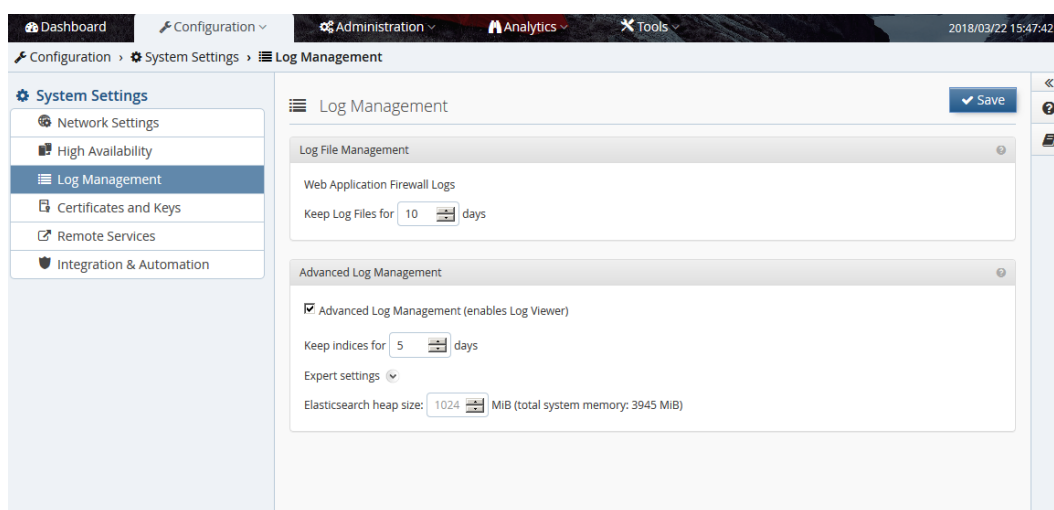


Figure 22: General log management settings

Log File Management

The Web Application Firewall log are kept several days. The number of days how long the log files should be kept can be defined here. The log files are rotated daily.

Advanced Log Management

The advanced log management allows to aggregate log data from different sources with the [Log Viewer](#) and can make it easier to locate problems in the overall processing chain.



Warning

High values are not recommended, as disk storage on the system has limited capacity and, depending on web traffic, the amount of log information will exceed the disk storage capacity rather quickly. If available disk storage drops below a certain value, old log information will be automatically removed to prevent the system to prematurely run out of disk storage. Nevertheless, up-to-date log information will still be available.

When disabling this feature completely, the possibility to aggregate the log data is lost. The components will only write the normal log files.



7.3.2 Log Message forwarding

Log messages from the WAF and Authentication Service can be forwarded to an external SIEM infrastructure or syslog server over UDP or TCP.

To configure a remote syslog server, go to *Configuration*→*System Settings*→*Network Settings*→*Monitoring/Alerting*→*Syslog Server* and enter the IP address, gateway, port and select the protocol to be used. It's possible to select between four different formats, how the message are forwarded:

- **Elastic Common Schema (ECS) with USP Extension:** json based log messages following the Elastic Common Schema(ECS) standard
- **USP SES Standard Log (Key/Value):** log messages are forwarded in a key/value structure. Servers having this output format defined, will receive all WAF and Authentication Service log messages!
- **Common Event Format (HP ArcSight):** log messages are transformed and forwarded in Common Event Format (CEF) supported by e.g. HP Arcsight. Servers having this output format defined, will receive all WAF and Authentication Service log messages!
- **Native Logfiles:** log messages are forwarded in the native format as they appear in the log file.

Native logfile forwarding

For Syslog servers having *Native Logfiles* output format selected, it's must be configured which logs will be forwarded for each component:

- **Web Application Firewall** Go to *Configuration*→*Web Application Firewall*→*General Settings* or *any virtual host*→*Logging*. In section *Syslog native log format forwarding* the logfiles to forward can be selected. Log messages from the Web Application Firewall will have the facility *local7* and a tag of the form *<VIRTUAL_HOST_ID>_<SUB_COMPONENT>*. Access log messages will have the *info* severity, and error log messages will have the *warn* severity.

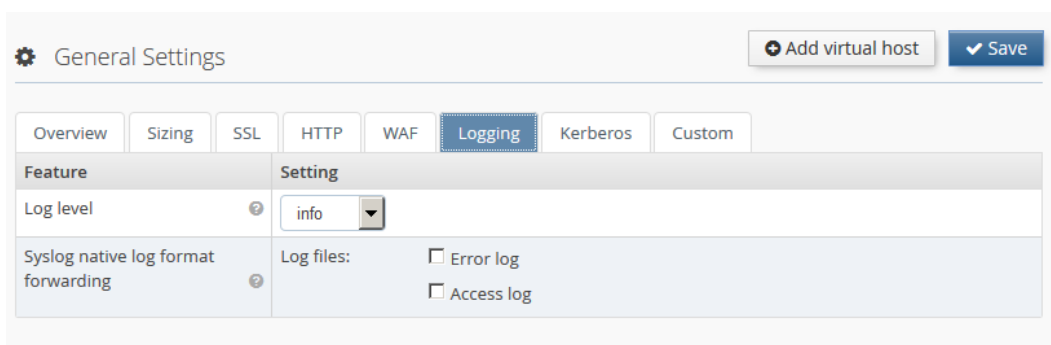


Figure 23: WAF native log file forwarding

- **Authentication service** Go to *Configuration*→*Authentication Service*→*General Settings*→*Miscellaneous Features*→*Forward log to syslog server* and select any log files which should be forwarded. Log messages from the Authentication Service will have the facility *local7* and tag *SLS*.

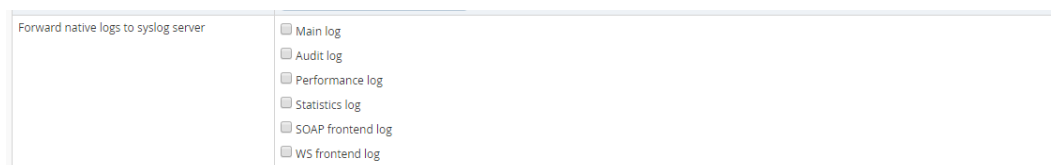


Figure 24: Authentication service native log format forwarding



Secure log message forwarding with SSL/TLS

Log messages can be transported securely using SSL/TLS. In the *Syslog Server* settings panel, select *TLS* in the list of protocols. Click on the *Manage certificates* icon to go to the *Certificates and keys* screen, where you can upload your SSL/TLS CA certificate for the selected syslog server. For proper validation of the server certificate, ensure that the *subject alternative name* field includes the IP address of the syslog server.

A client certificate & private key pair can be uploaded and specified *Syslog Server* settings panel if the server requires client authentication.

7.3.3 Log Viewer

Analytics → *Log Viewer* is only accessible when *Advanced Log Management* is enabled. This log viewer will allow to aggregate the different log sources and provides an extended search and filter mechanism.

Time (UTC)	Component	Virtual Host	Log Type	Request Method	Request Path	Response Code	Request Correlator
19.11.2015 12:51:13.000	SRM	www.sesdemo.ch:443	access	GET	/form/form.php?qwer=yxcv	200	7f0100-4274-2015.11.19_1251.13.405-001
19.11.2015 12:51:11.000	SRM	www.sesdemo.ch:443	access	GET	/form/form.php?adf=Q-pomLnbNuGN5hRehJFg8pFz4VCM6WB&qwer=yxcv	403	7f0100-4274-2015.11.19_1251.11.635-001
19.11.2015 12:51:08.000	SRM	www.sesdemo.ch:443	access	GET	/form/form.php?qwer=yxcv	200	7f0100-4274-2015.11.19_1251.08.508-001
19.11.2015 12:51:07.000	SRM	www.sesdemo.ch:443	access	GET	/form/	200	7f0100-4274-2015.11.19_1251.07.537-001
19.11.2015 12:51:05.000	SRM	www.sesdemo.ch:443	access	POST	/form/form.php	500	7f0100-4274-2015.11.19_1251.05.232-001

Figure 25: Log viewer

Consult the context help in the Web GUI for details how the different filter and search mechanism are working.

Alternative Log Viewer

When the *Advanced Log Management* is disabled, an alternative view exists to analyze the log files. In *Analytics* → *Log Download* each log file can be viewed separately by clicking **Q**. Basic filtering is possible, but only the log entries of the current log rotation generation can be viewed.

7.3.4 Traffic Analyzer

The traffic analyzer is used for debugging purposes when integrating new applications. It records detailed request and response data during different processing steps.



Warning

This feature must not be enabled on a productive server since it can record clear text user authentication data. In addition, it generates high data volume which can fill up the hard disk of the system.

Configuration

This feature can be enabled on virtual host level in the tab *Logging*. By specifying a certain URL path, an client IP address or a specific user-agent regular expression pattern, only matching requests will be captured. This will limit the amount of recorded data and will simplify the analysis.

Analysis

The captured request data can be analyzed with the build in Traffic Analyzer found under *Analytics* → *Traffic Analyzer*.



7.4 Monitoring

7.4.1 System health status

The [Dashboard](#) provides an overview of the usage of system resources like CPU usage, memory, swap and disk space. Clicking on the *System* menu item in the navigation opens a screen containing time-based charts of the system resource usage, as well as network and disk performance.

7.4.2 Local SNMPD Server

The USP Secure Entry Server® features a local SNMP service which can be accessed by external monitoring solutions to obtain system status, configuration and health information.

The local SNMP service can be configured by navigating to *Configuration*→*System Settings*→*Network Settings*→*Monitoring/Alerting*→*Local SNMPD Server*. Entering a community string and activating the configuration will enable the SNMP service, which can be accessed on port 161 using SNMP protocol version 2c.

In addition to the standard MIB-2 information, it is possible to query USP Secure Entry Server® specific information like virtual host usage, component service status, appliance release or system health information. You can download the related MIB files by clicking the *Get MIB* button in the *Network Settings* screen.

7.4.3 SNMP Traps

If the monitoring system detects an event (for example, an unexpected stop of a service, memory or hard disk filling up, errors reported by the WAF or Authentication Service), it can inform the operator by sending an SNMP trap message to a monitoring system which supports receiving SNMP traps.

SNMP trap receivers can be configured by navigating to *Configuration*→*System Settings*→*Network Settings*→*Monitoring/Alerting*→*SNMP Server*. Adding multiple SNMP servers, with individual community strings, is possible.

The structure of the SNMP trap message is defined in the *USP-SES-TRAP-MIB* file, which can be downloaded by clicking the *Get MIB* button in the *Network Settings* screen.



7.5 Statistics and Events

The [Dashboard](#) shows current and long term statistic data. The data of the last hour or up to the last year can be shown.

Besides selecting the period it is also possible to drill down into the different virtual hosts and the different locations for the long term statistic charts.

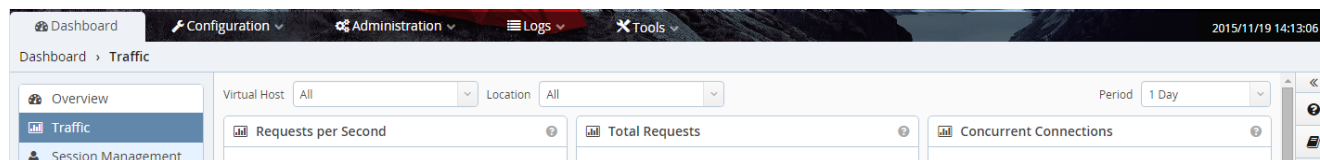


Figure 26: Dashboard drill-down

For details about the different charts see the context help in the Web GUI.

7.5.1 Events

The various components of the USP Secure Entry Server[®] generate events. These events provide consistent, uniformly structured information related to monitoring the status of various components and services in all USP products. With this structured information, a user is able to perform meaningful analysis of issues of any kind (using drill-down or statistical methods).

7.5.1.1 Event Viewer

The event viewer (*Analytics*→*Events*) is a flexible tool to analyze various occurred events on the USP Secure Entry Server[®]. Events keep track of relevant security issues like "Suspicious Access Attempt" and operational issues like "Available disk space is running low.". For a complete list of all Events consult the **USP Event Documentation**.

The event viewer offers several predefined views for a quick access to important events. Note that some views are only available with the appropriate license!

Filters will help you narrow the events list down. Note that only the latest 500 events will be displayed in the table. If the wanted events are not within this batch, you must refine your filter criteria. Available filters can be added either by choosing the desired criteria from the dropdown menu or by right-clicking on any column in the event view and selecting the menu item "Set as filter". Using the context menu will reset any previously selected filter of the same type to the exact selected value. To remove it, click on the remove-icon (x) of a criteria field. To change a criteria value click on the value of a criteria field.

7.5.1.2 Event Forwarding

Events can be forwarded to a syslog server or SIEM solution using the *Remote Syslog Server* configuration (*Configuration*→*System Settings*→*Network Settings*). This works the same way as forwarding WAF or Authentication Service logs. Tick the event forwarding checkbox(es) in the *Remote Syslog Server* configuration panel to enable event forwarding.