Microsoft

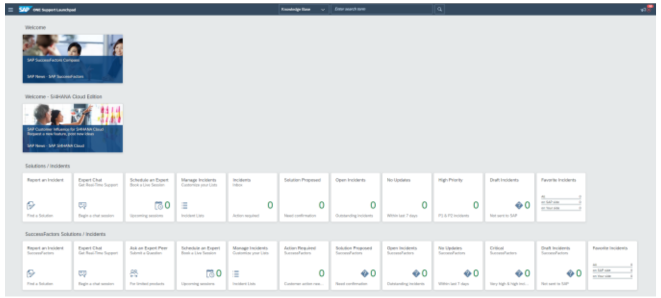
SAP Fiori Deployment on Azure

Dennis Padia

Agenda

- SAP Fiori Overview
- SAP Fiori Apps architecture and deployment on Azure
- Azure Application Gateway configuration for SAP Fiori Apps
- Single Sign On (SSO) configuration using SAML and Azure Active Directory for SAP Fiori Apps
- Troubleshooting WAF

What is SAP Fiori?



Role-based

Adaptive

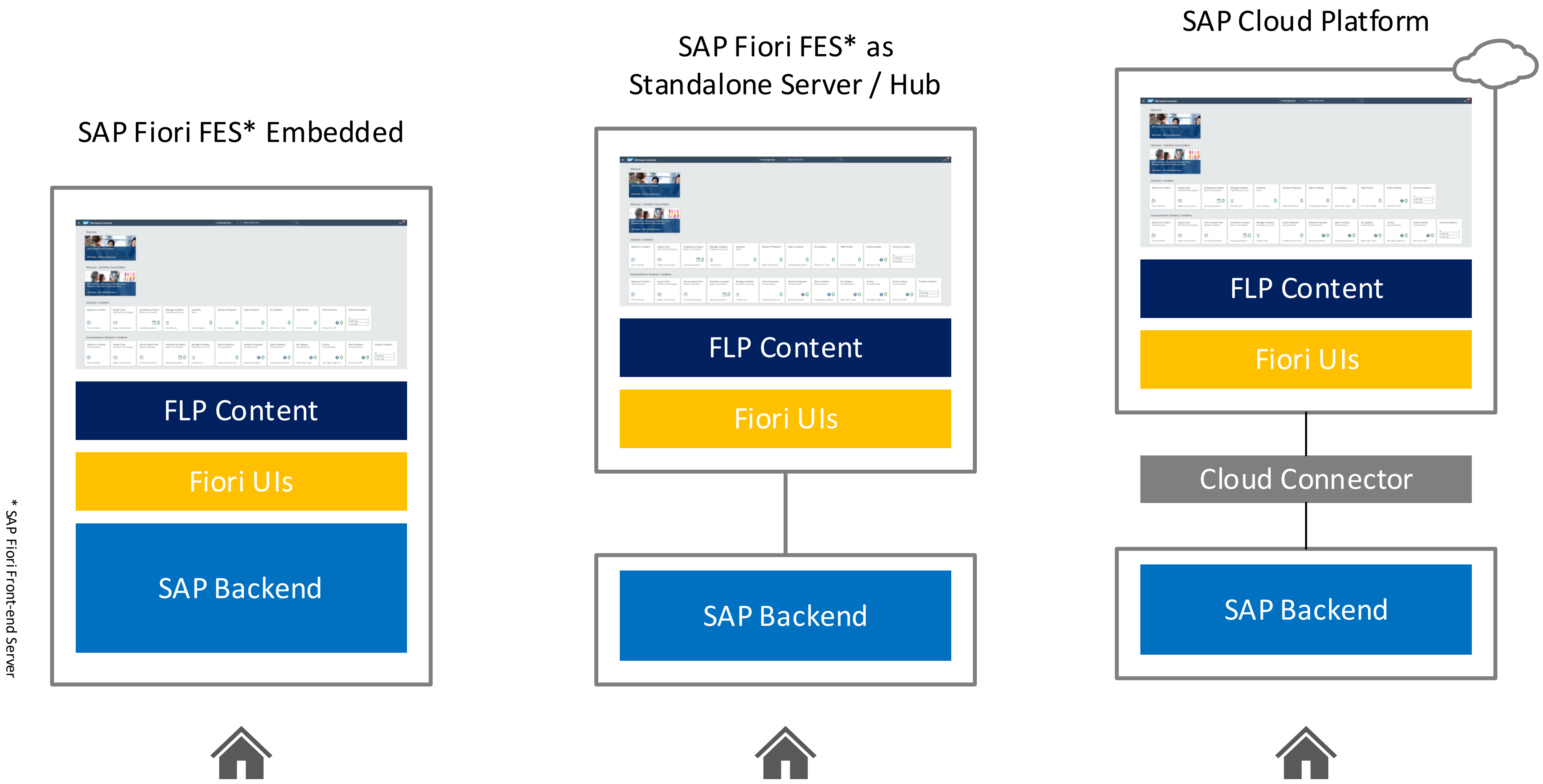
Simple

Coherent

Delightful

- SAP Fiori is a new user experience (UX) for SAP Software and applications. It is a set of apps, newly written by SAP, that address the most broadly and frequently used SAP functions.
- It provides simple and easy-to-use access across desktops, tablets and smartphones.

SAP Fiori Deployment Options



SAP Fiori FES* Embedded

FLP Content

Fiori UIs

SAP Backend

SAP Fiori FES* as Standalone Server / Hub

FLP Content

Fiori UIs

SAP Backend

SAP Cloud Platform

FLP Content

Fiori UIs

Cloud Connector

SAP Backend

* SAP Fiori Front-end Server

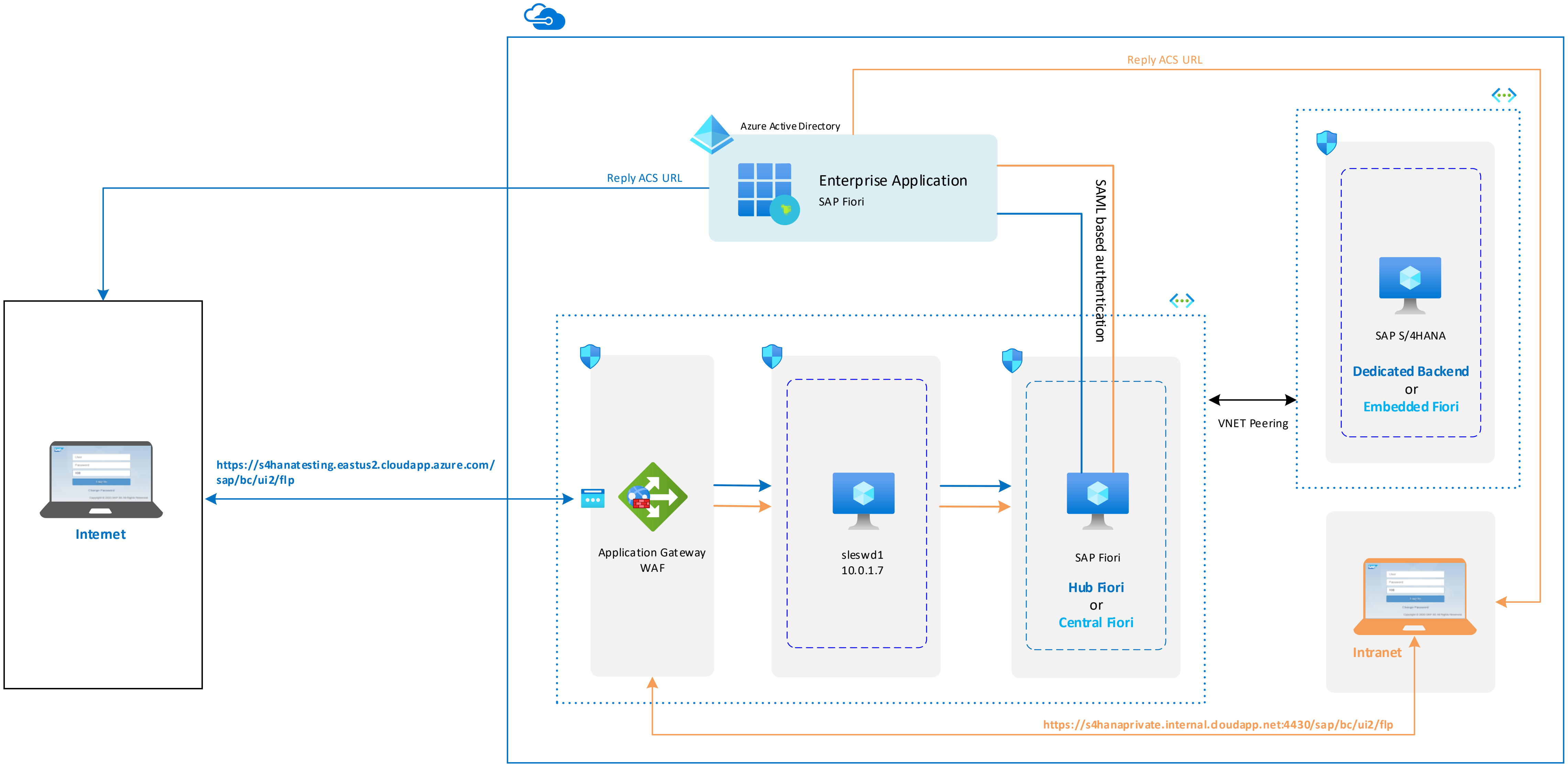
Refer SAP Fiori Deployment Options and System Landscape Recommendations for up-to-date information.

SAP Fiori Deployment Recommendation

- For **SAP S/4HANA**, the **embedded** SAP Front End Server (FES) deployment is recommended.
- For **SAP Business Suite** scenarios, SAP Front End Server (FES) as a central **hub** is still the recommended deployment.
- If **internet access is an important use case** and for security reason the backend should not be exposed, the **hub deployment might be preferable**. But in this case software lifecycle and maintenance is more complex due to dependencies of the software components

Pros & Cons of each deployment option can be found in SAP Fiori Deployment Options and System Landscape Recommendations

Internet Facing SAP Fiori Architecture on Azure



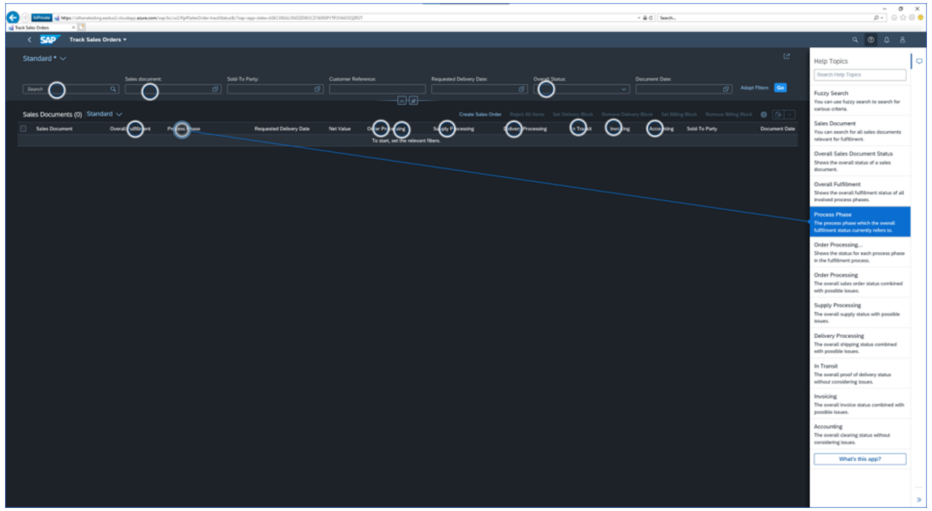
Blog by SAP: [Considerations and Recommendations for Internet-facing Fiori apps]()

Insight about exposing SAP Fiori Apps to the Internet in Azure

1. Web Application Firewall should be used for internet facing use cases of SAP Fiori Apps.
2. For SAP Fiori, it is not advisable to use Azure Application Gateway as a replacement of web dispatcher (next slide for details).
3. Standalone SAP Web dispatcher is a default option by SAP. To integrate web dispatcher with ASCS/ERS of SAP Fiori central/hub, make sure to size the VM accordingly.
4. Have SAP backend systems on separate network because in case of security breaches/attack you can anytime disconnect two peered networks, whereas restricting inbound/outbound rules in NSG within virtual network will not apply to already established connections.
5. For internet-facing use cases, it is recommended to have end-to-end HTTPS.
6. The network latency between virtual machines in peered virtual network in the same region is the same as the latency within a single virtual network.
7. The traffic between two services in peered virtual networks is routed directly through the Microsoft backbone infrastructure, not through a gateway or over the public Internet.

When Application Gateway, why SAP Web Dispatcher?

- In S/4HANA, SAP Web Dispatcher is required to enable certain features like web assistant, co-pilot.
- SAP Web Dispatcher provide features like URL filter, which help customer to restrict services based on certain conditions.
- For certain SAP Products like SAP BusinessObjects, customer can directly leverage Application Gateway.



To start, set the relevant filters.

Fuzzy Search
You can use fuzzy search to search for various criteria.

Sales Document
You can search for all sales documents relevant for fulfillment.

Overall Sales Document Status
Shows the overall status of a sales document.

Overall Fulfillment
Shows the overall fulfillment status of all involved process phases.

Process Phase
The process phase which the overall fulfillment status currently refers to.

Order Processing...
Shows the status for each process phase in the fulfillment process.

Order Processing
The overall sales order status combined with possible issues.

Supply Processing
The overall supply status with possible issues.

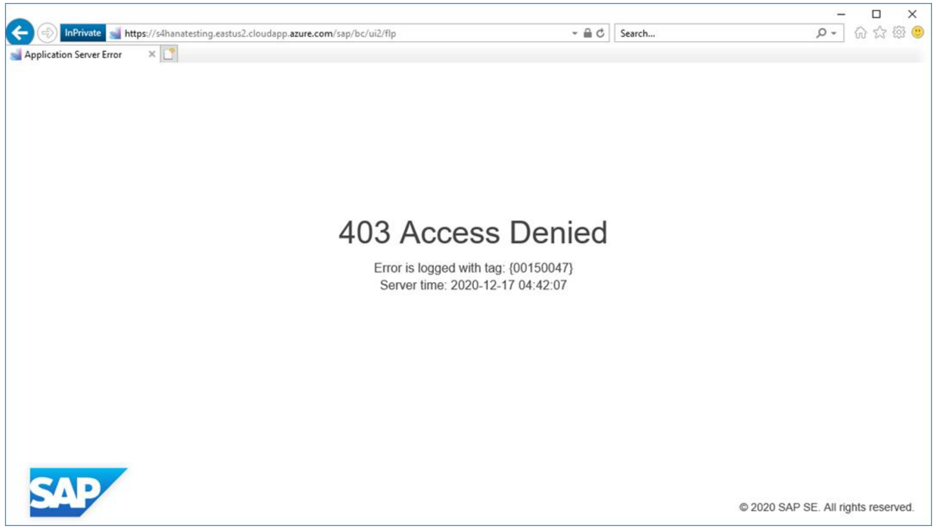
Delivery Processing
The overall shipping status combined with possible issues.

In Transit
The overall proof of delivery status without considering issues.

Invoicing
The overall invoice status combined with possible issues.

Accounting
The overall clearing status without considering issues.

Web Assistant


InPrivate
https://s4hanatesting.eastus2.cloudapp.azure.com/sap/bc/ui2/flp
Search...
Application Server Error

403 Access Denied

Error is logged with tag: {00150047}
Server time: 2020-12-17 04:42:07

© 2020 SAP SE. All rights reserved.

URL Filter

Application Gateway & its configuration options

- For application gateway, there are two SKUs that are available, and each SKU has two tiers.

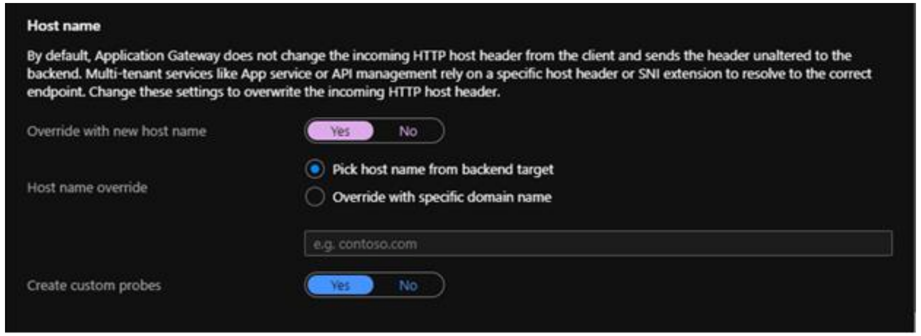
v1 SKU	v2 SKU
Standard	Standard V2
WAF	WAF V2

- v2 SKU offers performance enhancements and adds support for critical new features like autoscaling, zone redundancy and support for static VIPs. *(More Info: Feature comparison between v1 SKU and v2 SKU)*
- Each SKU has different support for Frontend IP address type. *(More Info: FAQs about Application Gateway)*

Application Gateway	Public	Private	Both
v1	SKU: Basic IP Assignment: Dynamic	IP Assignment: Static or Dynamic	Supported
v2	SKU: Standard IP Assignment: Static	Not Supported	Supported Private IP Assignment: Static

- Listener in application gateway cannot use the same frontend port as an existing listener. So, one URL for both public and private frontend IP is not possible.

v1 SKU vs v2 SKU

Component	v1 SKU	v2 SKU
Network	• Dedicated subnet is required. Cannot be provisioned on the same subnet of v2. • Allow incoming internet traffic on TCP ports 65503-65534.	• Dedicated subnet is required. Cannot be provisioned on the same subnet of v1 • Allow incoming internet traffic on TCP ports 65200-65535
	• Outbound internet connectivity cannot be blocked. • Traffic from the AzureLoadBalancer tag with the destination subnet as Any must be allowed.	
End-to-end TLS	• Requires authentication certificate of backend servers	• Requires root certificate (base64 encoded) of backend servers. • In addition to root certificate match, AGW v2 also validates the host setting specified in backend HTTP setting. The CN presented by backend server's TLS certificate should match with host setting. • When trying to establish a TLS connection to the backend, AGW v2 sets the Server Name Indication (SNI) extension to the Host specified in the backend http setting. When trying to establish a TLS connection to the backend, AGW v2 sets the SNI extension to the Host specified in the backend http setting.  **Host name** By default, Application Gateway does not change the incoming HTTP host header from the client and sends the header unaltered to the backend. Multi-tenant services like App service or API management rely on a specific host header or SNI extension to resolve to the correct endpoint. Change these settings to overwrite the incoming HTTP host header. Override with new host name [✓ Yes] No Host name override ● Pick host name from backend target ○ Override with specific domain name e.g. contoso.com Create custom probes [✓ Yes] No

For more details on AGW network, refer FAQs about Application Gateway
For more detail on End-to-end TLS, refer Overview of TLS termination and end to end TLS with Application Gateway
For more details on features and limitations of the v2 SKU that differ from the v1 SKU, refer Differences from v1 SKU

Web Application Firewall (WAF) on Application Gateway

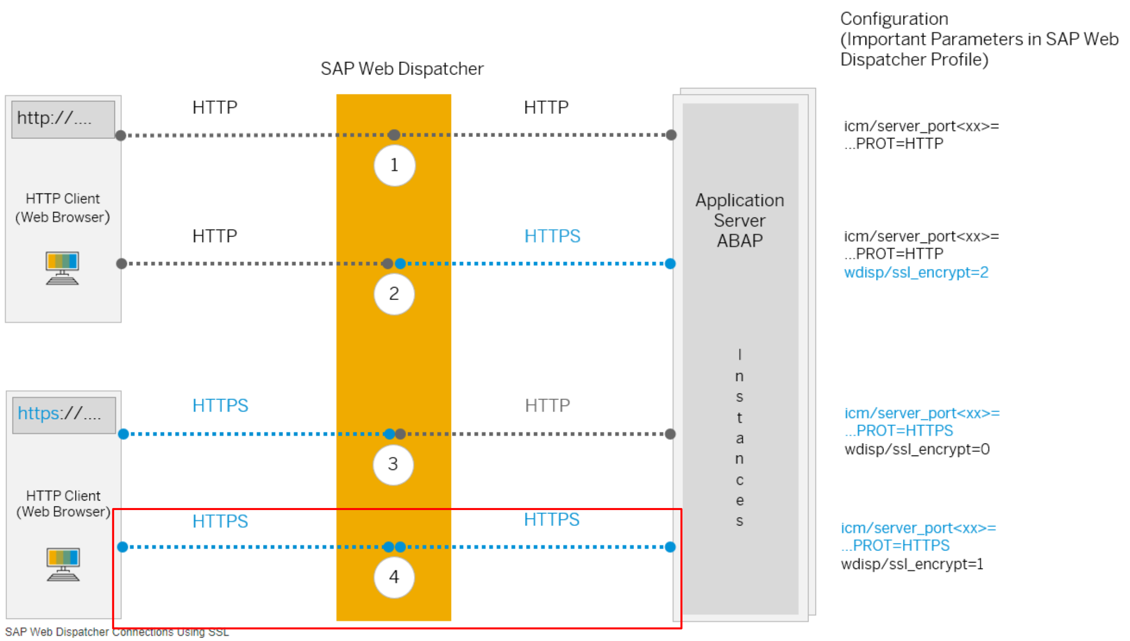
- Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities.
- WAF on Application Gateway is based on Core Rule Set (CRS) 3.2, 3.1, 3.0, or 2.2.9 from the Open Web Application Security Project (OWASP). The WAF automatically updates to include protection against new vulnerabilities, with no additional configuration needed.
- Custom policies can be created, and can be associated with an Application Gateway, to individual listeners, or to path-based routing rules on an Application Gateway.

Detection Mode	Prevention Mode
Monitor and logs all threat alerts. Web application firewall doesn't block incoming requests when it's operating in detection mode.	Block intrusions and attacks that the rules detect.

- For a newly deployed WAF, it is recommended to set the mode in Detection for a short period of time in a production environment. This provides the opportunity to obtain firewall logs and update any exceptions or custom rules prior to transition to Prevention mode. This can help reduce the occurrence of unexpected blocked traffic.

Pre-requisites

- For internet facing use case, it is recommended to have end-to-end TLS. Make sure to configure TLS on SAP Systems i.e., ABAP System and Web Dispatcher.
- TLS certificate is required, which is to be added to the Listener to enable Application Gateway to derive a symmetric key as per TLS/SSL protocol specification. The symmetric key is then used to encrypt and decrypt the traffic sent to the gateway.
- To generate Certificate Signing Request (CSR) for application gateway, you can use IIS or other third-party utility. Once the CSR is generated, get it signed from trusted CA authority based on type of frontend (Public or Private)



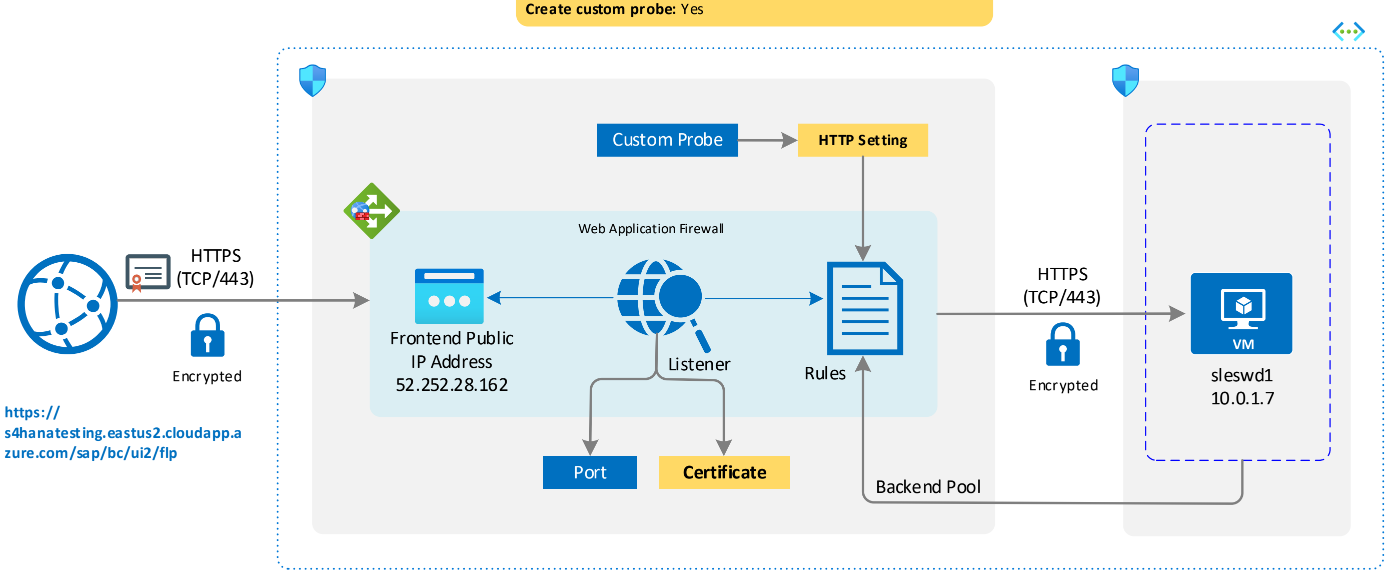
Configuration
(Important Parameters in SAP Web Dispatcher Profile)

```
icm/server_port<xx>=
...PROT=HTTP

icm/server_port<xx>=
...PROT=HTTP
wdisp/ssl_encrypt=2

icm/server_port<xx>=
...PROT=HTTPS
wdisp/ssl_encrypt=0

icm/server_port<xx>=
...PROT=HTTPS
wdisp/ssl_encrypt=1
```

SAP Web Dispatcher Connections Using SSL

Application Gateway WAF v2 Setup for SAP Fiori

HTTP Setting
Trusted root certificate: Upload root certificate of backend server
Override with new hostname: Yes
Host name override: Pick hostname from backend target
Create custom probe: Yes



https://s4hanatesting.eastus2.cloudapp.azure.com/sap/bc/ui2/flp

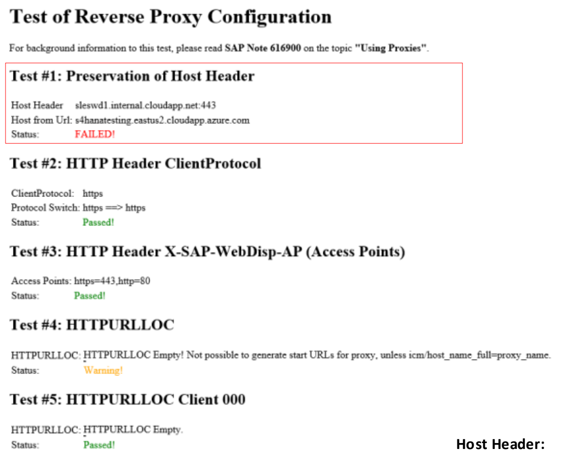
If Frontend IP address is **Public**, sign the certificate from trusted public CA authority like DigiCert, GeoTrust etc
If Frontend IP address is **Private**, sign the certificate from private CA authority like within organization

```
wdisp/system_<x> = SID=<Fiori_SID>, MSHOST=<Fiori_Msg_Server_Host>,
MSPORT=<Msg_Server_HTTP_Port>, SRCSRV=*:443, SRCURL=/sap/opu
wdisp/ssl_encrypt = 1

wdisp/ping_protocol = https
wdisp/group_info_protocol = https
wdisp/url_map_protocol = https
wdisp/server_info_protocol = https

wdisp/add_client_protocol_header = true
wdisp/handle_webdisp_ap_header = 1
wdisp/add_xforwardedfor_header = true

icm/server_port_<x> = PROT=HTTPS, PORT=443, TIMEOUT=900, PROCTIMEOUT=900,
EXTBIND=1
exe/icmbnd = $(DIR_CT_RUN)/icmbnd
```

Application Gateway Configuration Demo

Testing Proxy Configuration

Testing the Proxy Configuration:
https://s4hanatesting.eastus2.cloudapp.azure.com/sap/bc/bsp/sap/system_test/test_proxy.htm



Test of Reverse Proxy Configuration

For background information to this test, please read **SAP Note 616900** on the topic **"Using Proxies"**.

Test #1: Preservation of Host Header

Host Header   sleswd1.internal.cloudapp.net:443
Host from Url: s4hanatesting.eastus2.cloudapp.azure.com
Status: FAILED!

Test #2: HTTP Header ClientProtocol

ClientProtocol: https
Protocol Switch: https ==> https
Status: Passed!

Test #3: HTTP Header X-SAP-WebDisp-AP (Access Points)

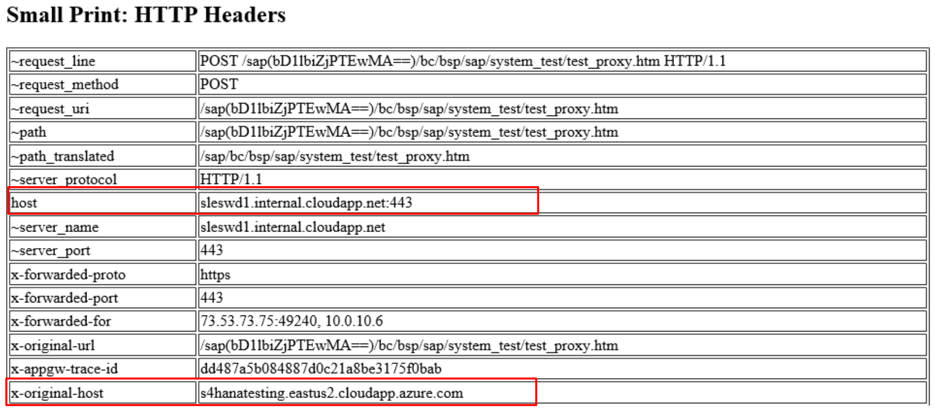
Access Points: https=443,http=80
Status: Passed!

Test #4: HTTPURLLOC

HTTPURLLOC: HTTPURLLOC Empty! Not possible to generate start URLs for proxy, unless icm/host_name_full=proxy_name.
Status: Warning!

Test #5: HTTPURLLOC Client 000

HTTPURLLOC: HTTPURLLOC Empty.
Status: Passed!

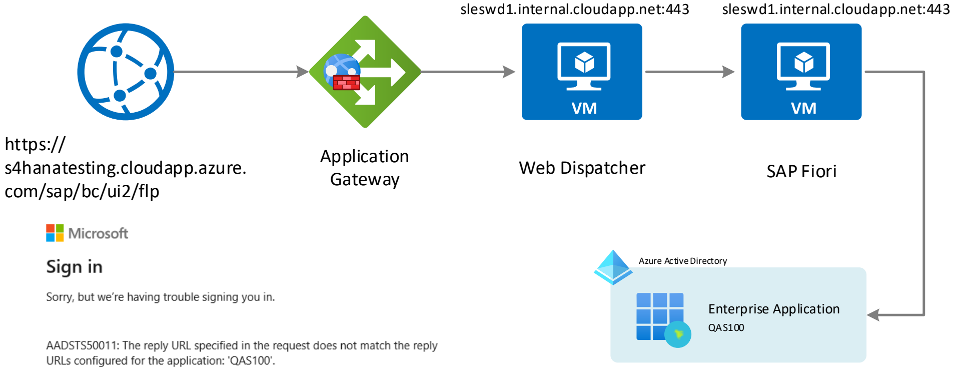


Small Print: HTTP Headers

~request_line	POST /sap(bD1lbiZjPTEwMA==)/bc/bsp/sap/system_test/test_proxy.htm HTTP/1.1
~request_method	POST
~request_uri	/sap(bD1lbiZjPTEwMA==)/bc/bsp/sap/system_test/test_proxy.htm
~path	/sap(bD1lbiZjPTEwMA==)/bc/bsp/sap/system_test/test_proxy.htm
~path_translated	/sap/bc/bsp/sap/system_test/test_proxy.htm
~server_protocol	HTTP/1.1
host	sleswd1.internal.cloudapp.net:443
~server_name	sleswd1.internal.cloudapp.net
~server_port	443
x-forwarded-proto	https
x-forwarded-port	443
x-forwarded-for	73.53.73.75:49240, 10.0.10.6
x-original-url	/sap(bD1lbiZjPTEwMA==)/bc/bsp/sap/system_test/test_proxy.htm
x-appgw-trace-id	dd487a5b084887d0c21a8be3175f0bab
x-original-host	s4hanatesting.eastus2.cloudapp.azure.com

Host Header:
sleswd1.internal.cloudapp.net:443

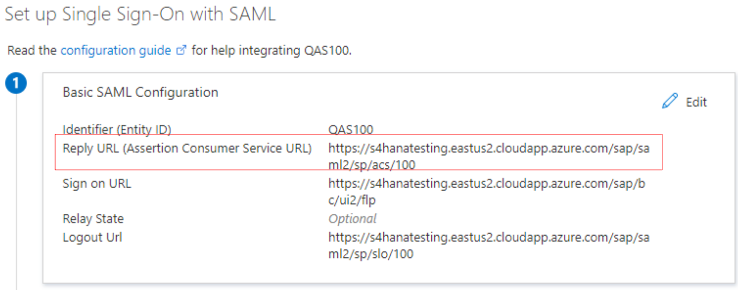
Host Header:
sleswd1.internal.cloudapp.net:443



Sign in

Sorry, but we're having trouble signing you in.

AADSTS50011: The reply URL specified in the request does not match the reply URLs configured for the application: 'QAS100'.



Set up Single Sign-On with SAML

Read the configuration guide for help integrating QAS100.

1 Basic SAML Configuration   Edit

Identifier (Entity ID)	QAS100
Reply URL (Assertion Consumer Service URL)	https://s4hanatesting.eastus2.cloudapp.azure.com/sap/saml2/sp/acs/100
Sign on URL	https://s4hanatesting.eastus2.cloudapp.azure.com/sap/bc/ui2/flp
Relay State	*Optional*
Logout Url	https://s4hanatesting.eastus2.cloudapp.azure.com/sap/saml2/sp/slo/100

Preserve Host Header

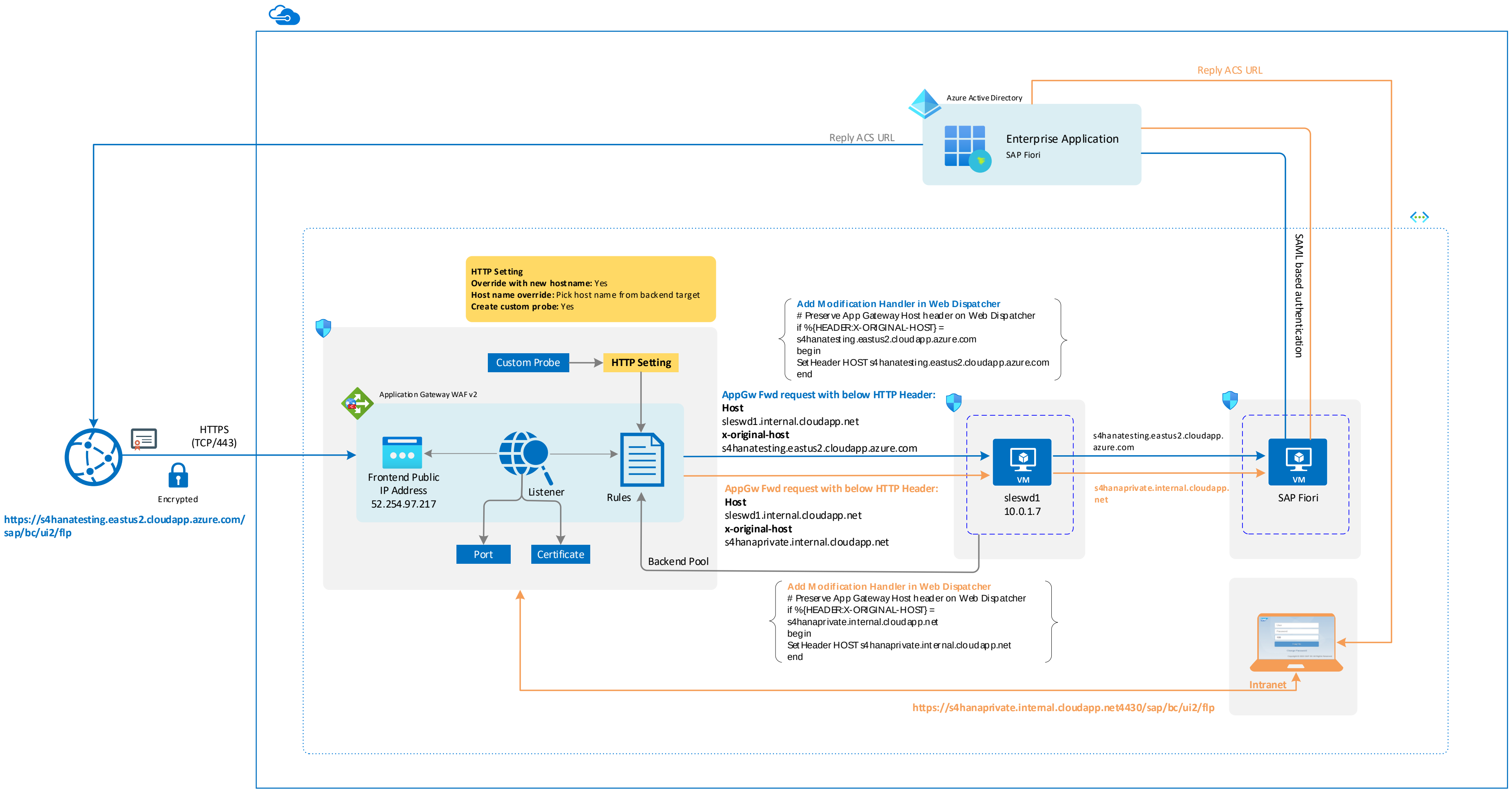
```
# vi WD1_W00_sleswd1

icm/HTTP/mod_0 = PREFIX=/, FILE=$(DIR_PROFILE)/redirect.txt

# vi /sapmnt/WD1/profile/redirect.txt

# Preserve Application Gateway Host header
if %{HEADER:X-ORIGINAL-HOST} = s4hanatesting.eastus2.cloudapp.azure.com
begin
SetHeader HOST s4hanatesting.eastus2.cloudapp.azure.com
End

# Preserve Application Gateway Host header
if %{HEADER:X-ORIGINAL-HOST} = s4hanaprivate.internal.cloudapp.net:4430
begin
SetHeader HOST s4hanaprivate.internal.cloudapp.net:4430
End
```

Manipulate Header Field

When incoming **X-ORIGINAL-HOST** is **s4hanatesting.eastus2.cloudapp.azure.com**, it will set the host header as **s4hanatesting.eastus2.cloudapp.azure.com**

Similarly, you can manipulate header field for private host **s4hanaprivate.internal.cloudapp.net** as well.

SAML SSO with Azure AD Architecture for SAP Fiori



https://s4hanatesting.eastus2.cloudapp.azure.com/sap/bc/ui2/flp

HTTP Setting
Override with new hostname: Yes
Host name override: Pick host name from backend target
Create custom probe: Yes

Add Modification Handler in Web Dispatcher

```
# Preserve App Gateway Host header on Web Dispatcher
if %{HEADER:X-ORIGINAL-HOST} =
s4hanatesting.eastus2.cloudapp.azure.com
begin
Set Header HOST s4hanatesting.eastus2.cloudapp.azure.com
end
```

AppGw Fwd request with below HTTP Header:
Host
sleswd1.internal.cloudapp.net
x-original-host
s4hanatesting.eastus2.cloudapp.azure.com

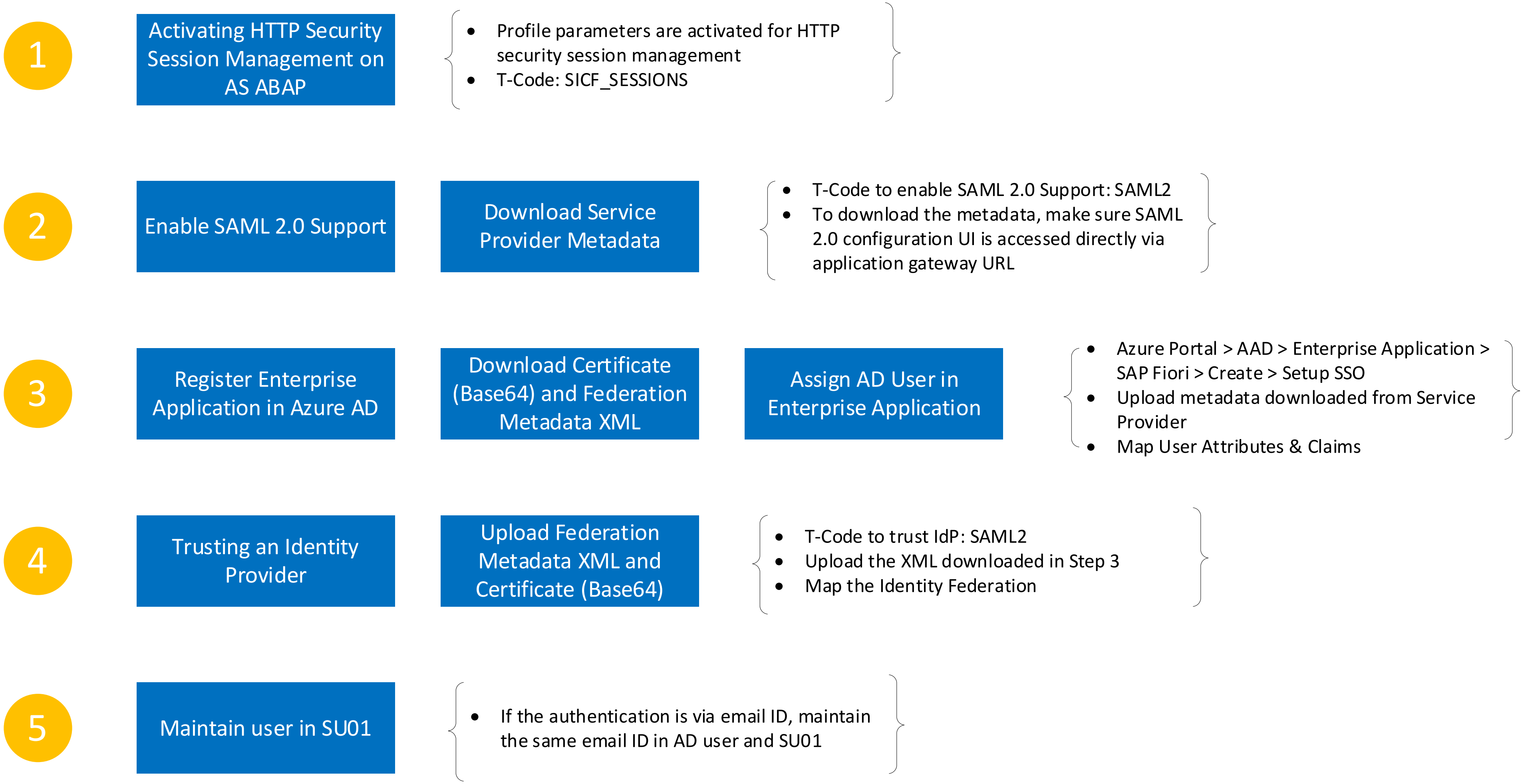
AppGw Fwd request with below HTTP Header:
Host
sleswd1.internal.cloudapp.net
x-original-host
s4hanaprivate.internal.cloudapp.net

Add Modification Handler in Web Dispatcher

```
# Preserve App Gateway Host header on Web Dispatcher
if %{HEADER:X-ORIGINAL-HOST} =
s4hanaprivate.internal.cloudapp.net
begin
Set Header HOST s4hanaprivate.internal.cloudapp.net
end
```

https://s4hanaprivate.internal.cloudapp.net4430/sap/bc/ui2/flp

SAML SSO with Azure AD Configuration



1 Activating HTTP Security Session Management on AS ABAP

- Profile parameters are activated for HTTP security session management
- T-Code: SICF_SESSIONS

2 Enable SAML 2.0 Support — Download Service Provider Metadata

- T-Code to enable SAML 2.0 Support: SAML2
- To download the metadata, make sure SAML 2.0 configuration UI is accessed directly via application gateway URL

3 Register Enterprise Application in Azure AD — Download Certificate (Base64) and Federation Metadata XML — Assign AD User in Enterprise Application

- Azure Portal > AAD > Enterprise Application > SAP Fiori > Create > Setup SSO
- Upload metadata downloaded from Service Provider
- Map User Attributes & Claims

4 Trusting an Identity Provider — Upload Federation Metadata XML and Certificate (Base64)

- T-Code to trust IdP: SAML2
- Upload the XML downloaded in Step 3
- Map the Identity Federation

5 Maintain user in SU01

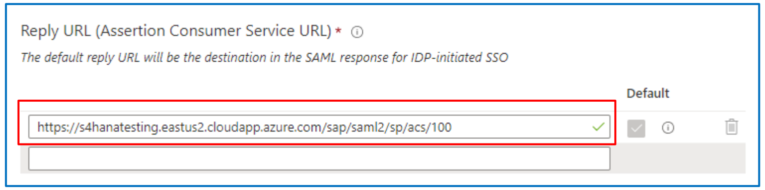
- If the authentication is via email ID, maintain the same email ID in AD user and SU01

For more information on configuration, refer below links

[*Tutorial: Azure Active Directory single sign-on (SSO) integration with SAP Fiori*]

[*SAP on Azure: Single Sign On Configuration using SAML and Azure Active Directory for Public and Internal URLs*]

Adjust SSO setup based on the Configuration

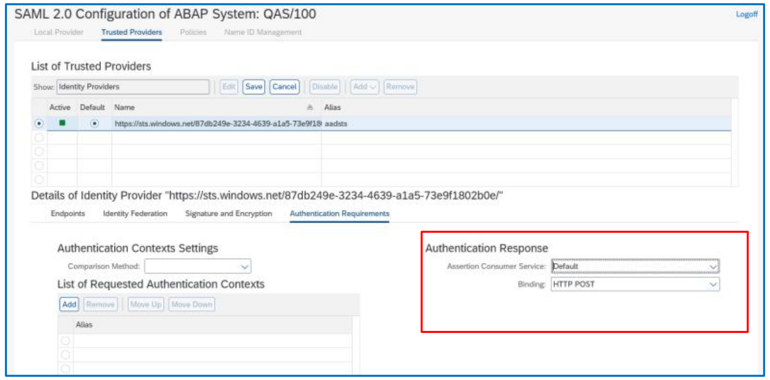


Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://s4hanatesting.eastus2.cloudapp.azure.com/sap/saml2/sp/acs/100 ✓ ☑



SAML 2.0 Configuration of ABAP System: QAS/100

List of Trusted Providers

Show: Identity Providers

Active	Default	Name	Alias
🟩	●	https://sts.windows.net/87db249e-3234-4639-a1a5-73e9f18	aadsts

Details of Identity Provider "https://sts.windows.net/87db249e-3234-4639-a1a5-73e9f1802b0e/"

Authentication Contexts Settings

Comparison Method:

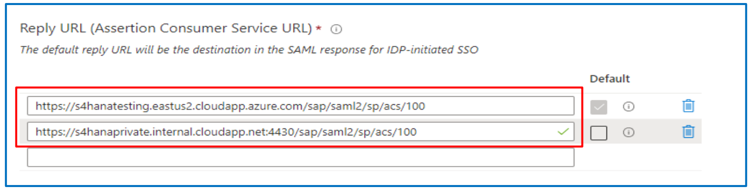
List of Requested Authentication Contexts

Authentication Response

Assertion Consumer Service: Default

Binding: HTTP POST

Single URL – Public or Private



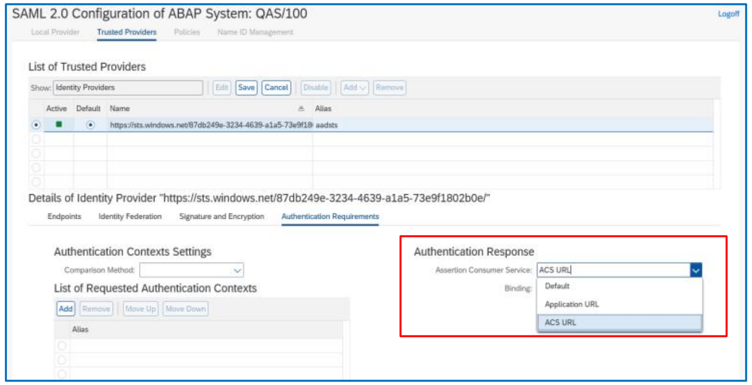
Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://s4hanatesting.eastus2.cloudapp.azure.com/sap/saml2/sp/acs/100 ☑

https://s4hanaprivate.internal.cloudapp.net:4430/sap/saml2/sp/acs/100 ✓ □



SAML 2.0 Configuration of ABAP System: QAS/100

List of Trusted Providers

Show: Identity Providers

Active	Default	Name	Alias
🟩	●	https://sts.windows.net/87db249e-3234-4639-a1a5-73e9f18	aadsts

Details of Identity Provider "https://sts.windows.net/87db249e-3234-4639-a1a5-73e9f1802b0e/"

Authentication Contexts Settings

Comparison Method:

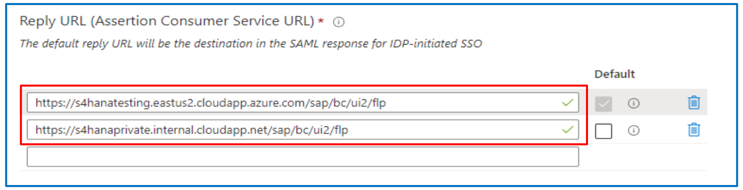
List of Requested Authentication Contexts

Authentication Response

Assertion Consumer Service: ACS URL

Binding:

Multiple URL – Public & Private



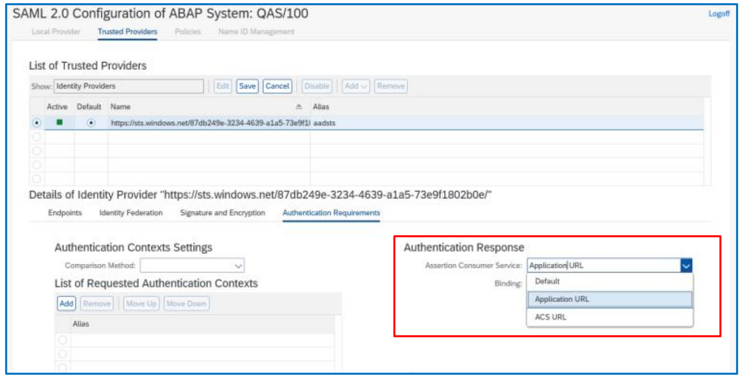
Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://s4hanatesting.eastus2.cloudapp.azure.com/sap/bc/ui2/flp ✓ ☑

https://s4hanaprivate.internal.cloudapp.net/sap/bc/ui2/flp ✓ □



SAML 2.0 Configuration of ABAP System: QAS/100

List of Trusted Providers

Show: Identity Providers

Active	Default	Name	Alias
🟩	●	https://sts.windows.net/87db249e-3234-4639-a1a5-73e9f1	aadsts

Details of Identity Provider "https://sts.windows.net/87db249e-3234-4639-a1a5-73e9f1802b0e/"

Authentication Contexts Settings

Comparison Method:

List of Requested Authentication Contexts

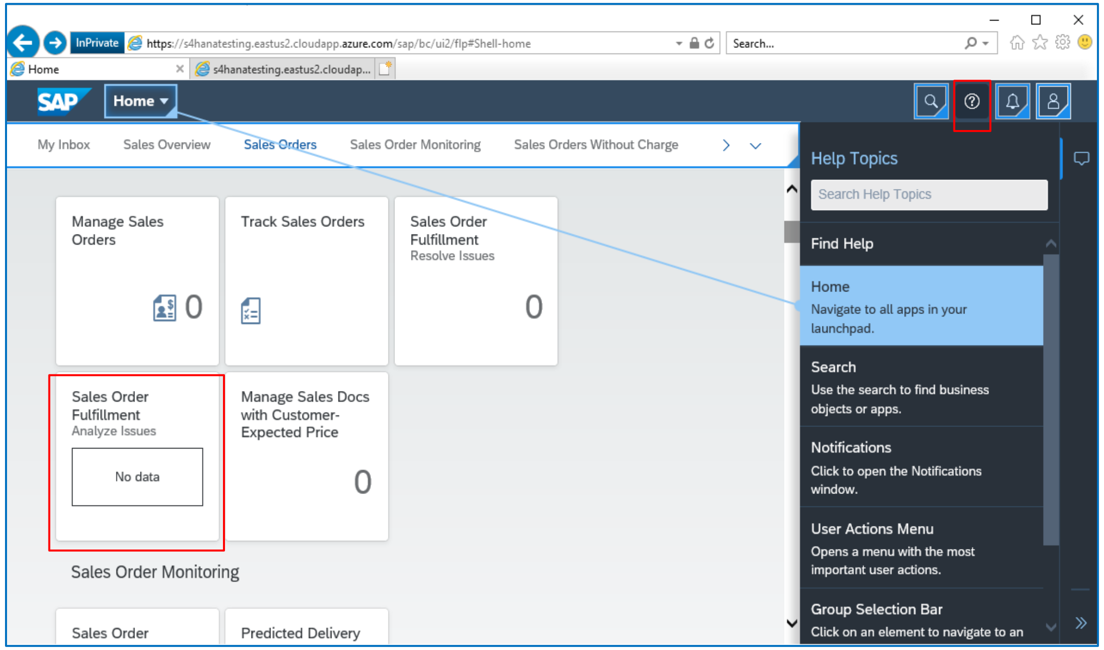
Authentication Response

Assertion Consumer Service: Application URL

Binding:

Multiple URL – Public & Private

Troubleshooting WAF Modes



Home
Navigate to all apps in your launchpad.

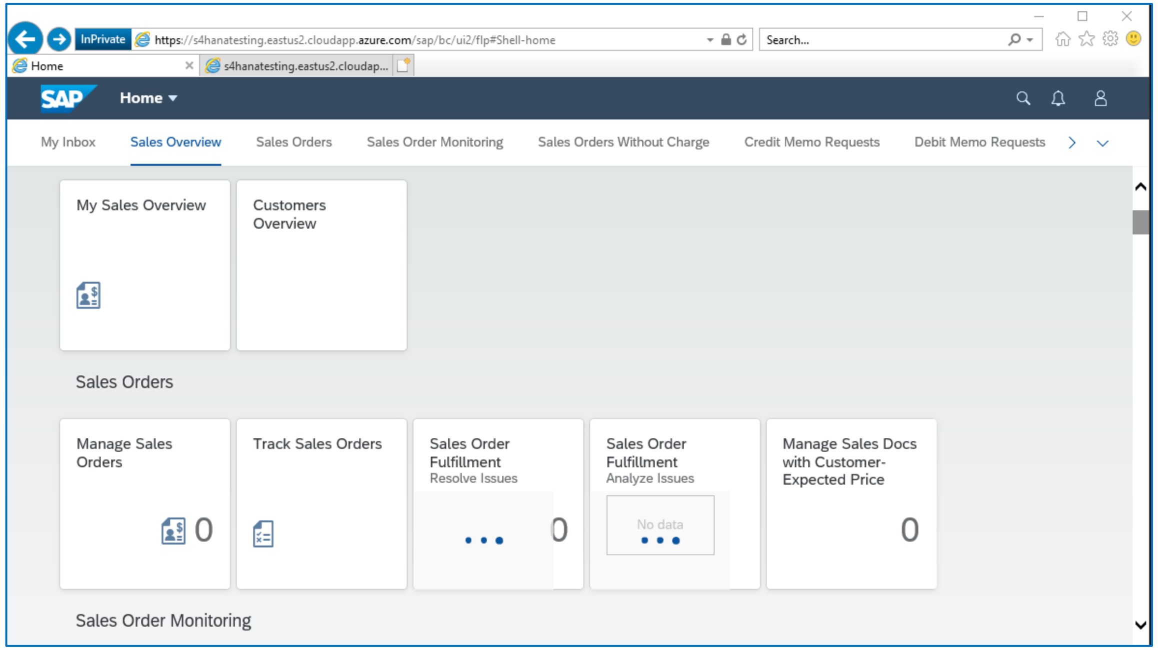
Search
Use the search to find business objects or apps.

Notifications
Click to open the Notifications window.

User Actions Menu
Opens a menu with the most important user actions.

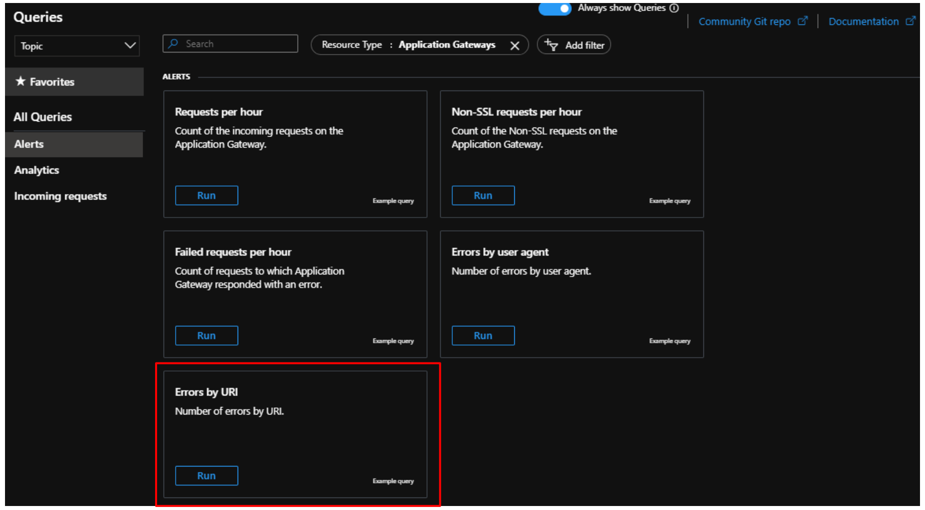
Group Selection Bar
Click on an element to navigate to an

WAF Mode: Detection



WAF Mode: Prevention

Continued...



Queries

Topic

★ Favorites

All Queries

Alerts

Analytics

Incoming requests

Always show Queries ⓘ | Community Git repo | Documentation

Search | Resource Type : **Application Gateways** ✕ | Add filter

ALERTS

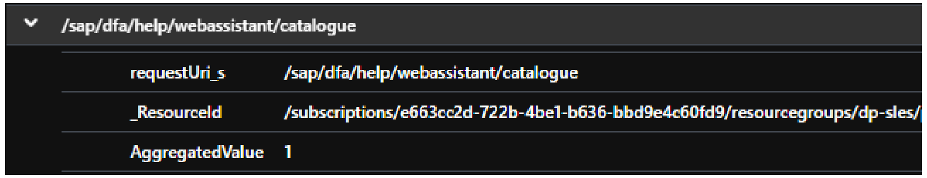
Requests per hour
Count of the incoming requests on the Application Gateway.
Run — Example query

Non-SSL requests per hour
Count of the Non-SSL requests on the Application Gateway.
Run — Example query

Failed requests per hour
Count of requests to which Application Gateway responded with an error.
Run — Example query

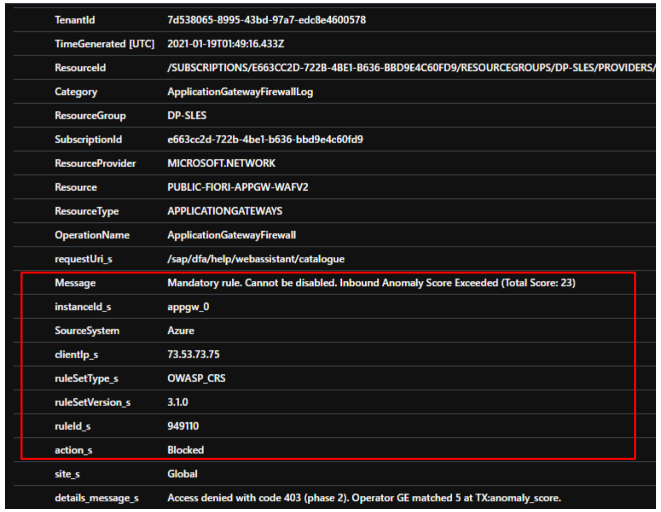
Errors by user agent
Number of errors by user agent.
Run — Example query

Errors by URI
Number of errors by URI.
Run — Example query

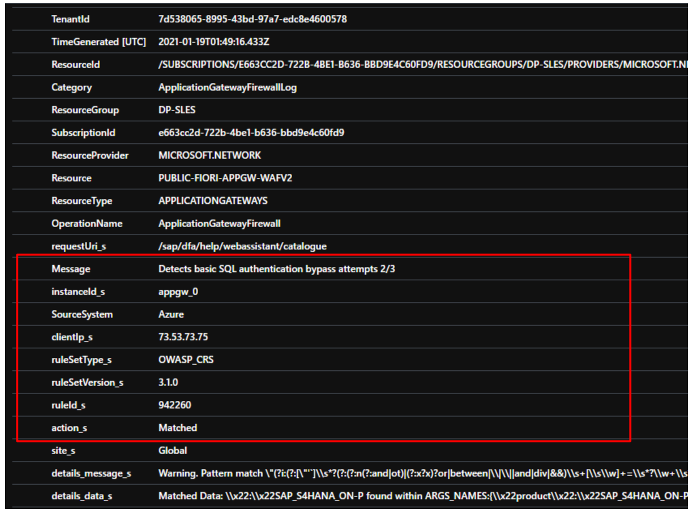


/sap/dfa/help/webassistant/catalogue	
requestUri_s	/sap/dfa/help/webassistant/catalogue
_ResourceId	/subscriptions/e663cc2d-722b-4be1-b636-bbd9e4c60fd9/resourcegroups/dp-sles/
AggregatedValue	1

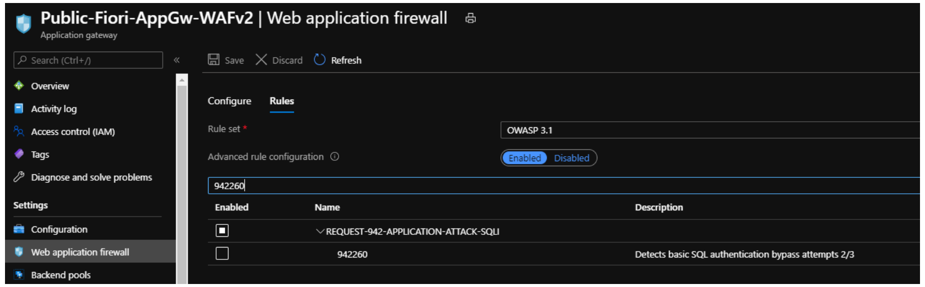
```
# Logs are stored in three tables - AzureActivity, AzureDiagnostics &
AzureMetris

# Run below command based on the requestUri_s that is being blocked

AzureDiagnostics
| where ResourceType == "APPLICATIONGATEWAYS" and
requestUri_s == "/sap/dfa/help/webassistant/catalogue"
```



TenantId	7d538065-8995-43bd-97a7-edc8e4600578
TimeGenerated [UTC]	2021-01-19T01:49:16.433Z
ResourceId	/SUBSCRIPTIONS/E663CC2D-722B-4BE1-B636-BBD9E4C60FD9/RESOURCEGROUPS/DP-SLES/PROVIDERS/
Category	ApplicationGatewayFirewallLog
ResourceGroup	DP-SLES
SubscriptionId	e663cc2d-722b-4be1-b636-bbd9e4c60fd9
ResourceProvider	MICROSOFT.NETWORK
Resource	PUBLIC-FIORI-APPGW-WAFV2
ResourceType	APPLICATIONGATEWAYS
OperationName	ApplicationGatewayFirewall
requestUri_s	/sap/dfa/help/webassistant/catalogue
Message	Mandatory rule. Cannot be disabled. Inbound Anomaly Score Exceeded (Total Score: 23)
instanceId_s	appgw_0
SourceSystem	Azure
clientIp_s	73.53.73.75
ruleSetType_s	OWASP_CRS
ruleSetVersion_s	3.1.0
ruleId_s	949110
action_s	Blocked
site_s	Global
details_message_s	Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score.



TenantId	7d538065-8995-43bd-97a7-edc8e4600578
TimeGenerated [UTC]	2021-01-19T01:49:16.433Z
ResourceId	/SUBSCRIPTIONS/E663CC2D-722B-4BE1-B636-BBD9E4C60FD9/RESOURCEGROUPS/DP-SLES/PROVIDERS/MICROSOFT.N
Category	ApplicationGatewayFirewallLog
ResourceGroup	DP-SLES
SubscriptionId	e663cc2d-722b-4be1-b636-bbd9e4c60fd9
ResourceProvider	MICROSOFT.NETWORK
Resource	PUBLIC-FIORI-APPGW-WAFV2
ResourceType	APPLICATIONGATEWAYS
OperationName	ApplicationGatewayFirewall
requestUri_s	/sap/dfa/help/webassistant/catalogue
Message	Detects basic SQL authentication bypass attempts 2/3
instanceId_s	appgw_0
SourceSystem	Azure
clientIp_s	73.53.73.75
ruleSetType_s	OWASP_CRS
ruleSetVersion_s	3.1.0
ruleId_s	942260
action_s	Matched
site_s	Global
details_message_s	Warning. Pattern match \"(?i:(?:[\"'`]\\s*?(?:(?:n(?:and|ot)|(?:x?x)?or|between|\\\|\\\||and|div|&&)\\s+[\\s\\w]+=\\s*?\\w+\\s
details_data_s	Matched Data: \\x22:\\x22SAP_S4HANA_ON-P found within ARGS_NAMES:{\\x22product\\x22:\\x22SAP_S4HANA_ON-P



Public-Fiori-AppGw-WAFv2 | Web application firewall
Application gateway

Search (Ctrl+/) | Save | Discard | Refresh

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Web application firewall
Backend pools

Configure | **Rules**

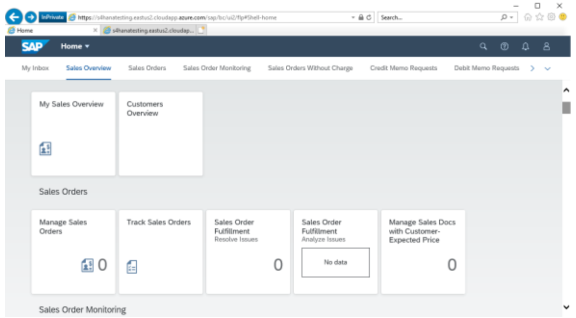
Rule set * : OWASP 3.1

Advanced rule configuration ⓘ : [✓ Enabled] Disabled

942260

Enabled	Name	Description
■	REQUEST-942-APPLICATION-ATTACK-SQLI	
□	942260	Detects basic SQL authentication bypass attempts 2/3

Some of the firewall rule cannot be disabled. This is often due to one or more previous issues with the request which cause other rules to be triggered. It is those earlier rules customers should examine or disable to mitigate this issue being triggered.



References

SAP Blogs and Documents

- Considerations and Recommendations for Internet-facing Fiori apps
- SAP Fiori Deployment Options and System Landscape Recommendations
- SAP Web Dispatcher
- Using Proxies

Application Gateway and SSO Configuration for SAP Fiori – Documents

- SAP on Azure: Application Gateway Web Application Firewall (WAF) v2 Setup for Internet facing SAP Fiori Apps
- SAP on Azure: Single Sign On Configuration using SAML and Azure Active Directory for Public and Internal URLs
- Tutorial: Azure Active Directory single sign-on (SSO) integration with SAP Fiori

Application Gateway Documents

- What is Azure Web Application Firewall on Azure Application Gateway?
- Autoscaling and Zone-redundant Application Gateway v2
- Overview of TLS termination and end to end TLS with Application Gateway
- FAQs about Application Gateway

Microsoft

Thank you !