IBM® Security Access Manager v8.x Kerberos Part 2

Kerberos Single Sign On using Constrained Delegation

<u>Panelists</u>

- Gianluca Gargaro – L2 Support Engineer
- Jonathan Morrow – L2 Support Engineer
- Darren Pond – L2 Support Engineer
- Hans Vandeweghe – L2 Support Engineer
- Antti Merihaara – L2 Support Engineer

Reminder: You must dial-in to the phone conference to listen to the panelists. The web cast does not include audio.

- **USA Toll-Free: 866-803-2145**
- **USA Toll: 1-210-795-1099**
- **Participant passcode: 3353561**
- Slides and additional dial in numbers: https://ibm.biz/BdHs9G

NOTICE: By participating in this call, you give your irrevocable consent to IBM to record any statements that you may make during the call, as well as to IBM's use of such recording in any and all media, including for video postings on YouTube. If you object, please do not connect to this call.

Agenda

- Kerberos Protocol Transition and Constrained delegation concepts
- ISAM 8 Native Kerberos Junction
- ITFIM enabled Kerberos Junction
- Delegation in Multiple Active Directory Domains
- Integration with Microsoft SharePoint
- Questions

IBM Security

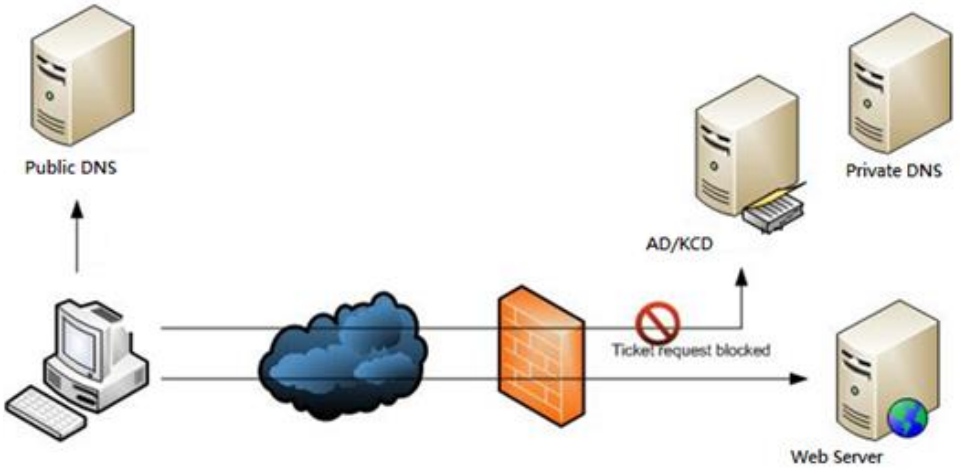
Intelligence. Integration. Expertise.

Kerberos Protocol Transition and Constrained Delegation concepts

Kerberos Protocol Transition and Constrained delegation concepts

The problem

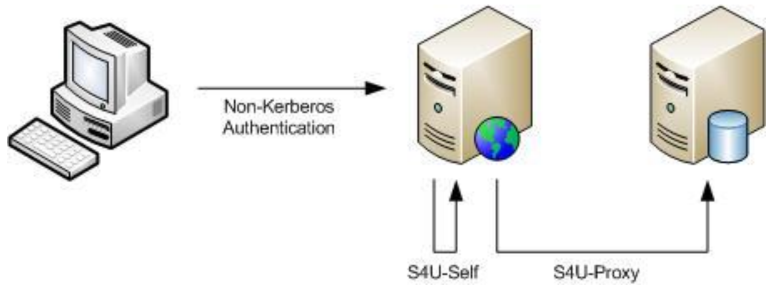
- The KDC is not exposed to internet
- Service records in internal DNS

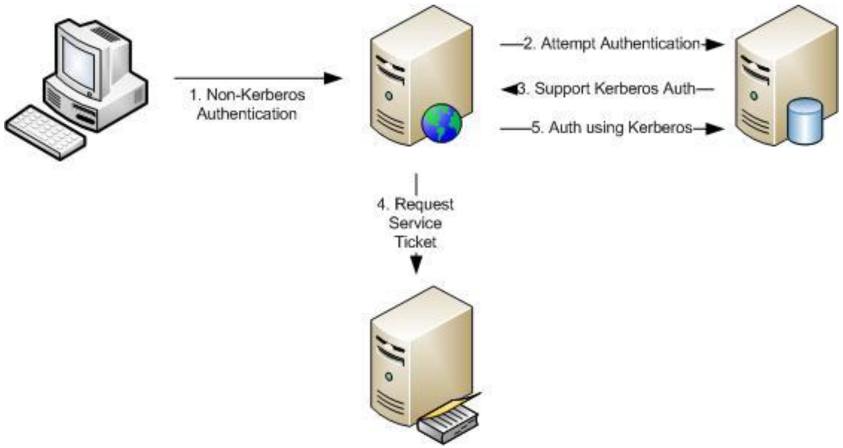


Kerberos Protocol Transition and Constrained delegation concepts

The solution

- Kerberos protocol extension
  - Services For User to Self (S4U2S)
  - Services for User To Proxy (S4UTP)




1. Non-Kerberos Authentication
2. Attempt Authentication
3. Support Kerberos Auth
5. Auth using Kerberos
4. Request Service Ticket

IBM Security

Intelligence. Integration. Expertise.

IBM

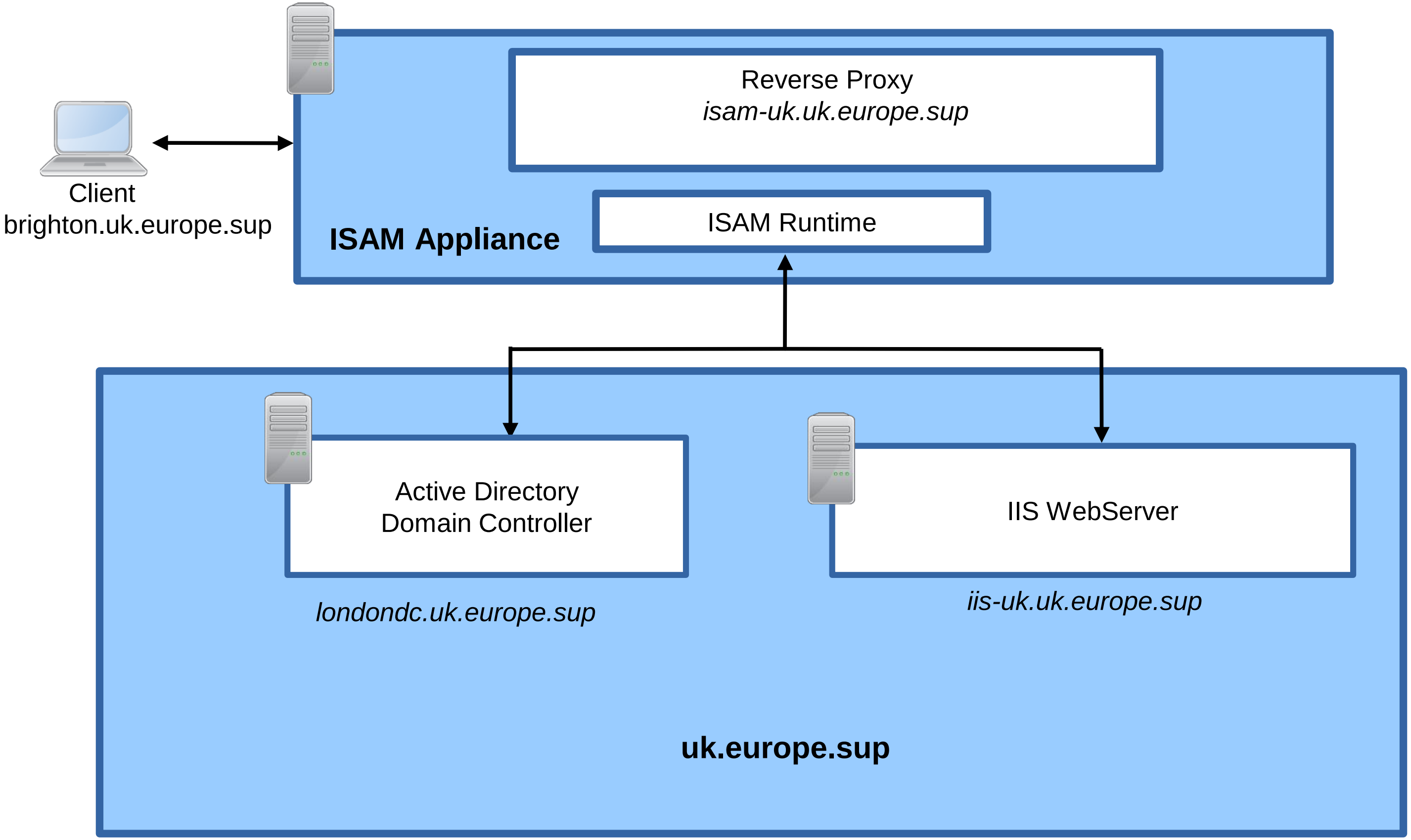
ISAM 8 Native Kerberos Junction

ISAM 8 Native Kerberos Junction

- Architecture
- Creating identities for WebSEAL and Target Service in an Active Directory domain
- Configure the Kerberos client in the appliance
- Configure WebSEAL instance
- Configure target server for Kerberos authentication
- Test functionality

ISAM 8 Native Kerberos Junction

Architecture



Client
brighton.uk.europe.sup

Reverse Proxy
isam-uk.uk.europe.sup

ISAM Runtime

ISAM Appliance

Active Directory
Domain Controller

londondc.uk.europe.sup

IIS WebServer

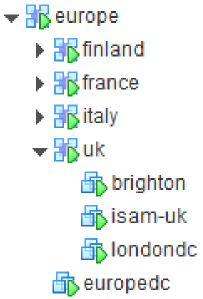
iis-uk.uk.europe.sup

uk.europe.sup

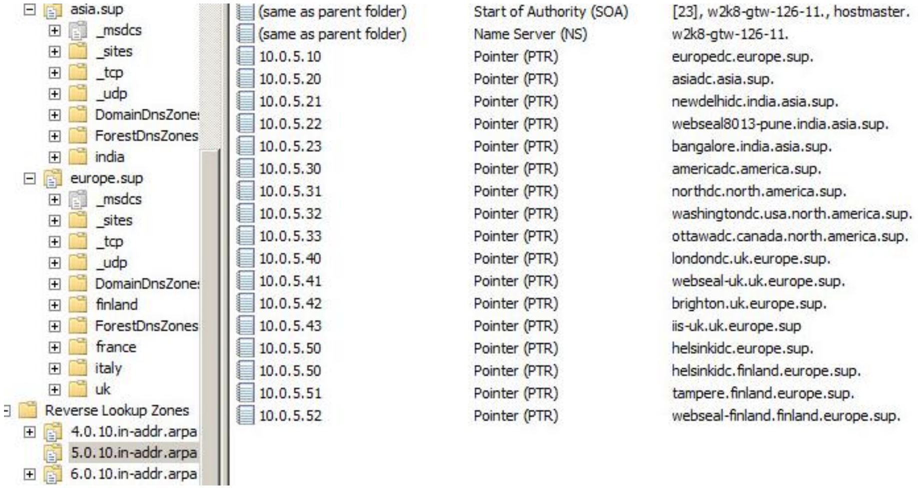
ISAM 8 Native Kerberos Junction

Architecture

- Machines must have full network connectivity
- Firewall open for KDC, DNS, HTTP
- Correct DNS, Forward and Reverse look-up.

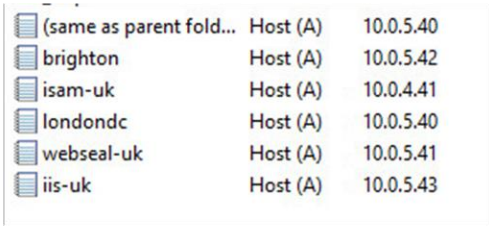


- europe
  - finland
  - france
  - italy
  - uk
    - brighton
    - isam-uk
    - londondc
  - europedc



- asia.sup
  - _msdcs
  - _sites
  - _tcp
  - _udp
  - DomainDnsZone
  - ForestDnsZones
  - india
- europe.sup
  - _msdcs
  - _sites
  - _tcp
  - _udp
  - DomainDnsZone
  - finland
  - ForestDnsZones
  - france
  - italy
  - uk
- Reverse Lookup Zones
  - 4.0.10.in-addr.arpa
  - 5.0.10.in-addr.arpa
  - 6.0.10.in-addr.arpa

(same as parent folder)	Start of Authority (SOA)	[23], w2k8-gtw-126-11., hostmaster.
(same as parent folder)	Name Server (NS)	w2k8-gtw-126-11.
10.0.5.10	Pointer (PTR)	europedc.europe.sup.
10.0.5.20	Pointer (PTR)	asiadc.asia.sup.
10.0.5.21	Pointer (PTR)	newdelhidc.india.asia.sup.
10.0.5.22	Pointer (PTR)	webseal8013-pune.india.asia.sup.
10.0.5.23	Pointer (PTR)	bangalore.india.asia.sup.
10.0.5.30	Pointer (PTR)	americadc.america.sup.
10.0.5.31	Pointer (PTR)	northdc.north.america.sup.
10.0.5.32	Pointer (PTR)	washingtondc.usa.north.america.sup.
10.0.5.33	Pointer (PTR)	ottawadc.canada.north.america.sup.
10.0.5.40	Pointer (PTR)	londondc.uk.europe.sup.
10.0.5.41	Pointer (PTR)	webseal-uk.uk.europe.sup.
10.0.5.42	Pointer (PTR)	brighton.uk.europe.sup.
10.0.5.43	Pointer (PTR)	iis-uk.uk.europe.sup
10.0.5.50	Pointer (PTR)	helsinkidc.europe.sup.
10.0.5.50	Pointer (PTR)	helsinkidc.finland.europe.sup.
10.0.5.51	Pointer (PTR)	tampere.finland.europe.sup.
10.0.5.52	Pointer (PTR)	webseal-finland.finland.europe.sup.

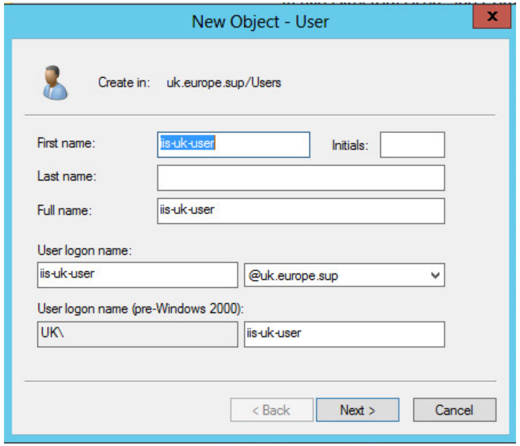


(same as parent fold...	Host (A)	10.0.5.40
brighton	Host (A)	10.0.5.42
isam-uk	Host (A)	10.0.4.41
londondc	Host (A)	10.0.5.40
webseal-uk	Host (A)	10.0.5.41
iis-uk	Host (A)	10.0.5.43

ISAM 8 Native Kerberos Junction

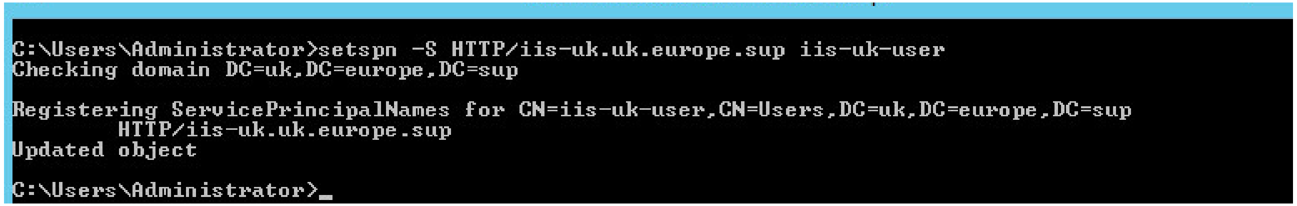
Creating Target Service identity in AD

- Create a user that represents the Target Service with a password that does not need to be changed and that never expires.
- Create a Service Principal Name for this user using setspn.



Create in: uk.europe.sup/Users

First name: iis-uk-user
Initials:
Last name:
Full name: iis-uk-user
User logon name: iis-uk-user @uk.europe.sup
User logon name (pre-Windows 2000): UK\ iis-uk-user



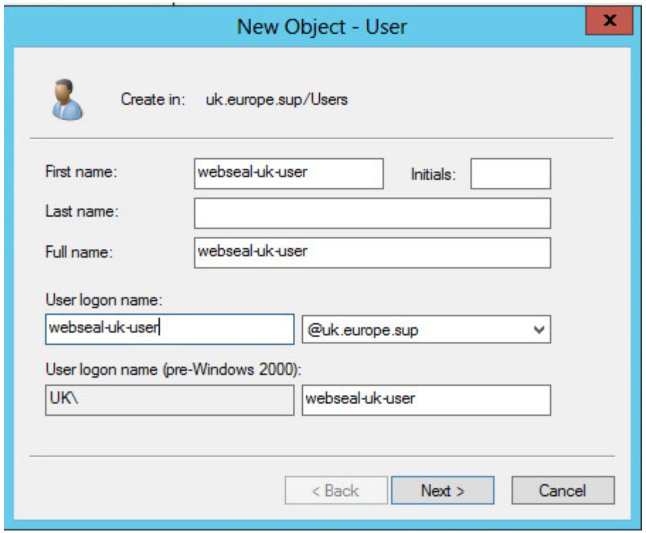
```
C:\Users\Administrator>setspn -S HTTP/iis-uk.uk.europe.sup iis-uk-user
Checking domain DC=uk,DC=europe,DC=sup

Registering ServicePrincipalNames for CN=iis-uk-user,CN=Users,DC=uk,DC=europe,DC=sup
        HTTP/iis-uk.uk.europe.sup
Updated object

C:\Users\Administrator>_
```

ISAM 8 Native Kerberos Junction

Creating WebSEAL user identity in AD

- Create a user that represents WebSEAL with a password that does not need to be changed and that never expires.

- Set the Service Principal Name (SPN) for this user on the KDC and create a keytab



Create in: uk.europe.sup/Users

First name: webseal-uk-user

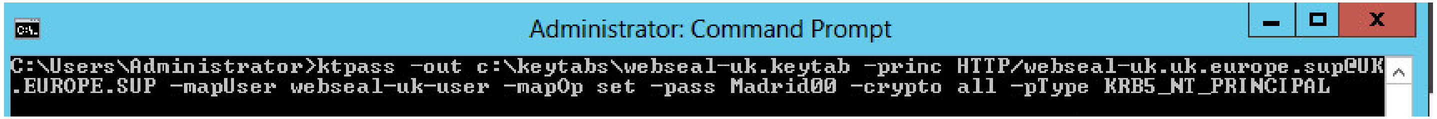
Initials:

Last name:

Full name: webseal-uk-user

User logon name: webseal-uk-user @uk.europe.sup

User logon name (pre-Windows 2000): UK\ webseal-uk-user

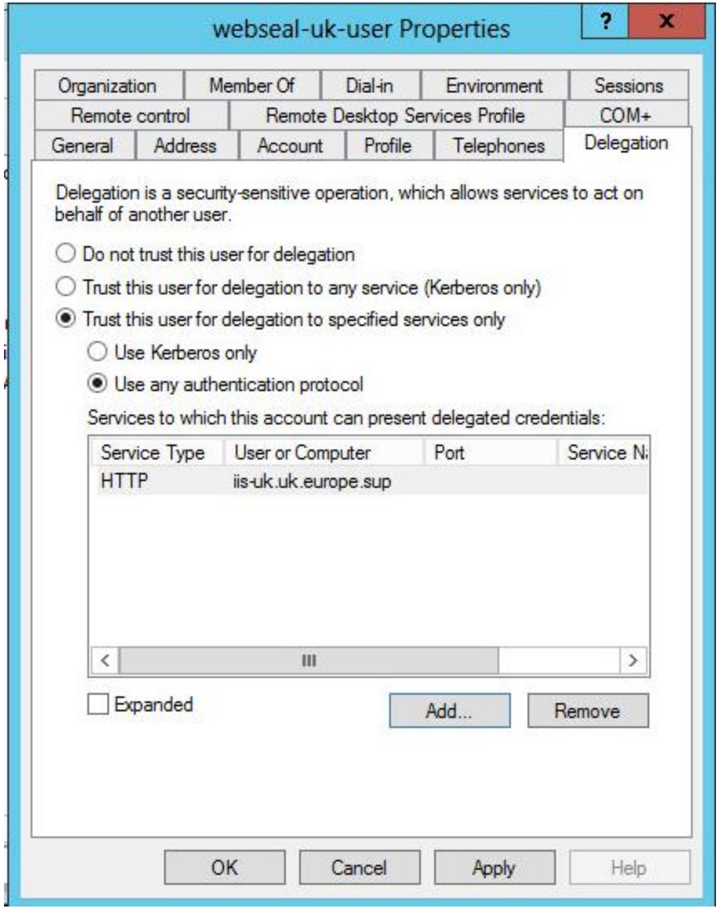


```
C:\Users\Administrator>ktpass -out c:\keytabs\webseal-uk.keytab -princ HTTP/webseal-uk.uk.europe.sup@UK
.EUROPE.SUP -mapUser webseal-uk-user -mapOp set -pass Madrid00 -crypto all -pType KRB5_NT_PRINCIPAL
```

ISAM 8 Native Kerberos Junction

Creating WebSEAL user identity in AD

- Set the WebSEAL user to be trusted for delegation to the target service user.



webseal-uk-user Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

  ○ Use Kerberos only

  ● Use any authentication protocol

Services to which this account can present delegated credentials:

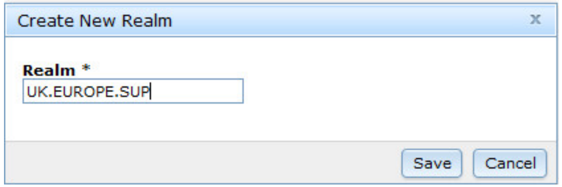
Service Type	User or Computer	Port	Service N
HTTP	iis-uk.uk.europe.sup		

☐ Expanded

ISAM 8 Native Kerberos Junction

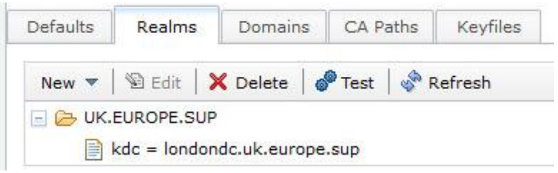
Configure the Kerberos client

- Use *Secure Web Settings > Global Settings > Kerberos Configuration* and open the *Realms* Tab and then select *New > Realm*



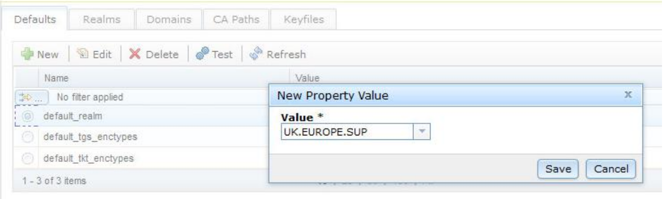
Realm *
UK.EUROPE.SUP

- Select the new realm name and use *New > Property* to select kdc and add the Active Directory KDC address



UK.EUROPE.SUP
kdc = londondc.uk.europe.sup

- On the *Defaults* tab change the default_realm to be the new realm created



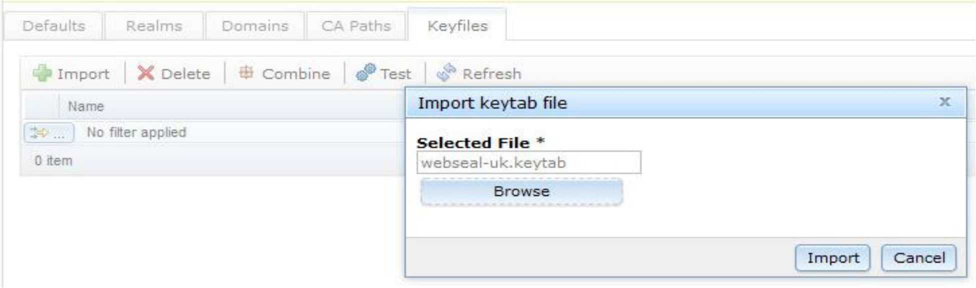
default_realm
default_tgs_enctypes
default_tkt_enctypes

Value *
UK.EUROPE.SUP

ISAM 8 Native Kerberos Junction

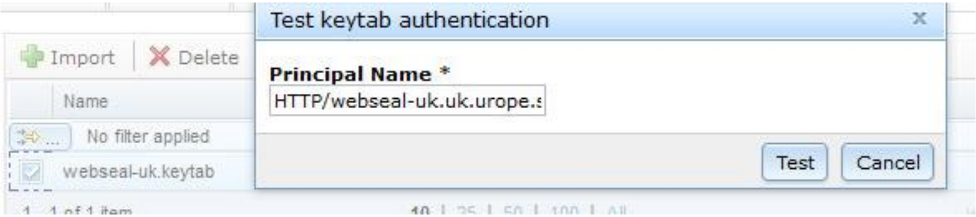
Configure the Kerberos client

- On the *Keyfiles* tab import the key table file generated for the WebSEAL user.



Selected File *: webseal-uk.keytab

- Test the keytab content for the WebSEAL principal name



Principal Name *: HTTP/webseal-uk.uk.urope.s

ISAM 8 Native Kerberos Junction

Configuring WebSEAL to enable Kerberos single sign-on for a junction

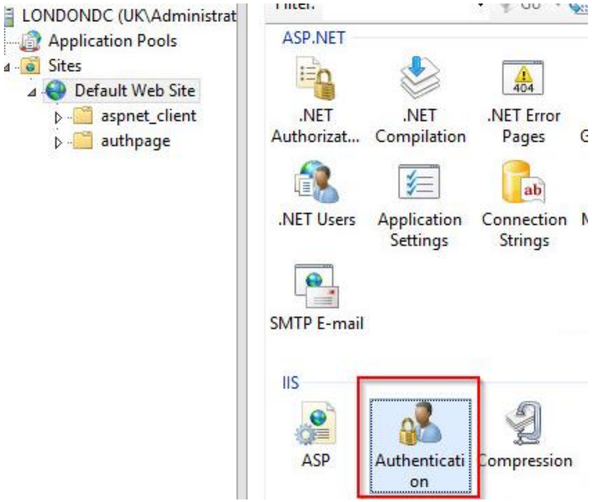
- Locate the [junction] stanza.
- Update the configuration items accordingly. For example:

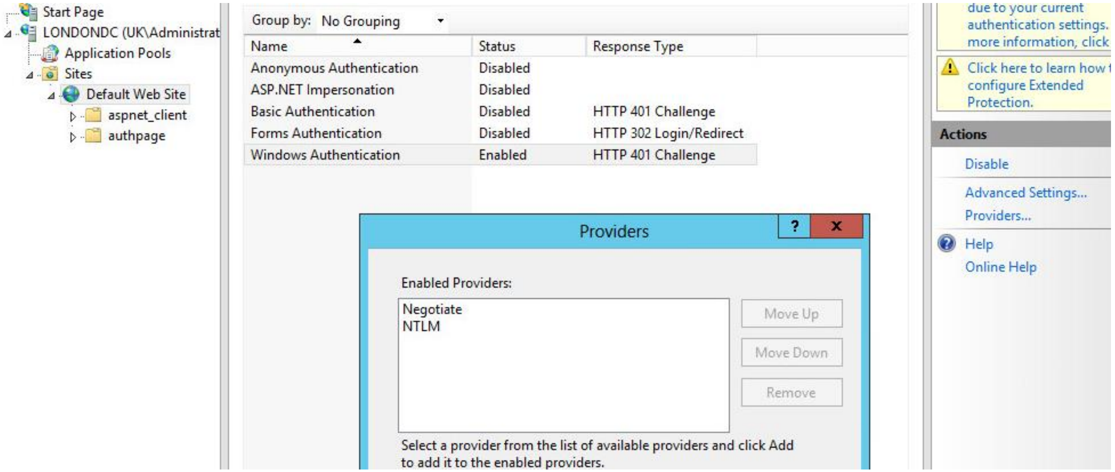
  - kerberos-sso-enable = true
  - kerberos-keytab-file = webseal-uk.keytab
  - kerberos-principal-name = HTTP/webseal-uk.uk.europe.sup@UK.EUROPE.SUP
  - kerberos-service-name = HTTP/iis-uk.uk.europe.sup@UK.EUROPE.SUP

ISAM 8 Native Kerberos Junction

Configure Target Server for Kerberos Authentication

- Enable Windows Authentication
- Disable all other authentication mechanisms
- Verify that *Negotiate* is the first provider.





Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

due to your current authentication settings. more information, click

Click here to learn how t configure Extended Protection.

Enabled Providers:

Negotiate
NTLM

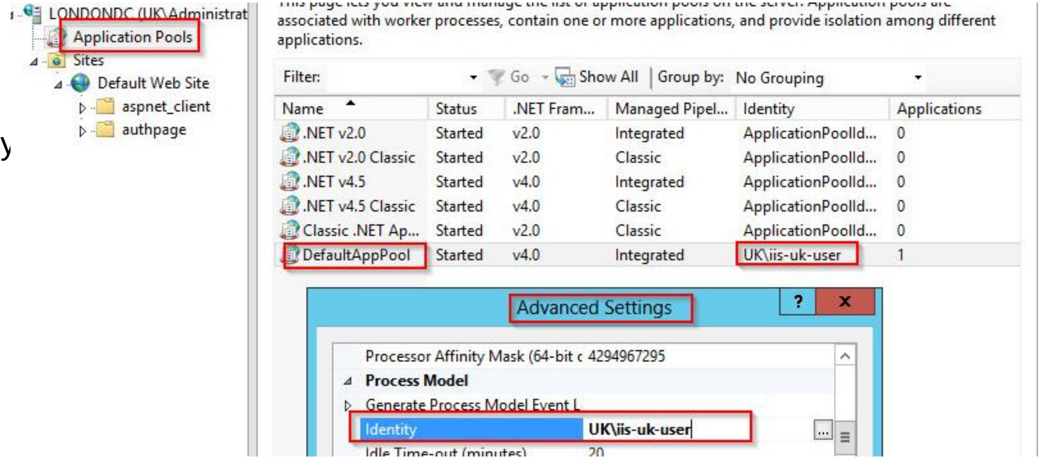
Select a provider from the list of available providers and click Add to add it to the enabled providers.

ISAM 8 Native Kerberos Junction

Configure Target Server for Kerberos Authentication

- Set iis-uk-user for the Default Application Pool identity

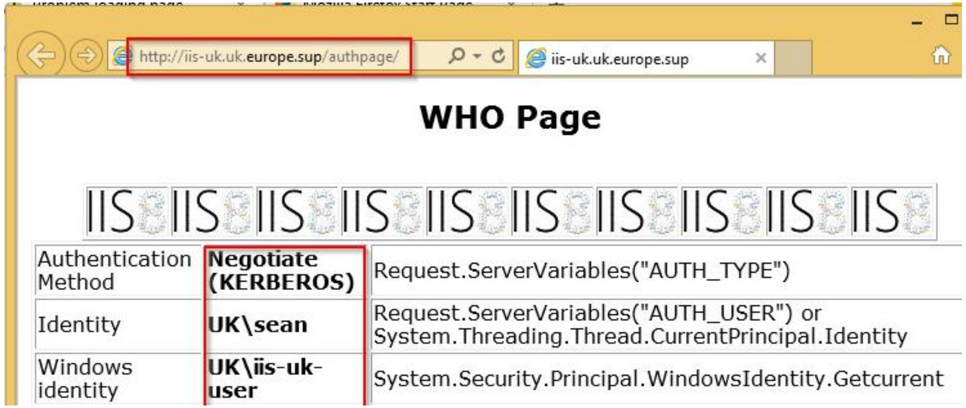
- Test Kerberos SSO directly to IIS



This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET Fram...	Managed Pipel...	Identity	Applications
.NET v2.0	Started	v2.0	Integrated	ApplicationPoolId...	0
.NET v2.0 Classic	Started	v2.0	Classic	ApplicationPoolId...	0
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolId...	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolId...	0
Classic .NET Ap...	Started	v2.0	Classic	ApplicationPoolId...	0
DefaultAppPool	Started	v4.0	Integrated	UK\iis-uk-user	1

Processor Affinity Mask (64-bit c 4294967295
Process Model
Generate Process Model Event L
Identity UK\iis-uk-user
Idle Time-out (minutes) 20



http://iis-uk.uk.europe.sup/authpage/
iis-uk.uk.europe.sup
IIS IIS IIS IIS IIS IIS IIS IIS IIS IIS

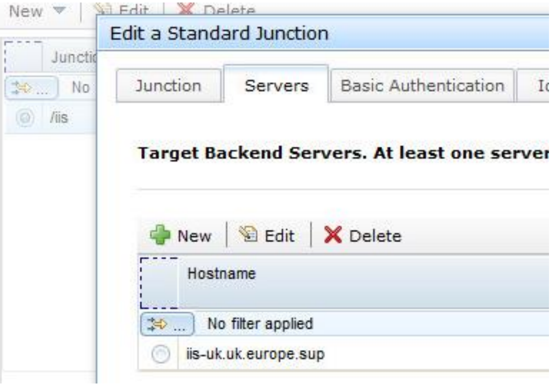
WHO Page

Authentication Method	**Negotiate (KERBEROS)**	Request.ServerVariables("AUTH_TYPE")
Identity	**UK\sean**	Request.ServerVariables("AUTH_USER") or System.Threading.Thread.CurrentPrincipal.Identity
Windows identity	**UK\iis-uk-user**	System.Security.Principal.WindowsIdentity.Getcurrent

ISAM 8 Native Kerberos Junction

Create and Test Junction

- Create a junction /iis pointing to server iis-uk.uk.europe.sup

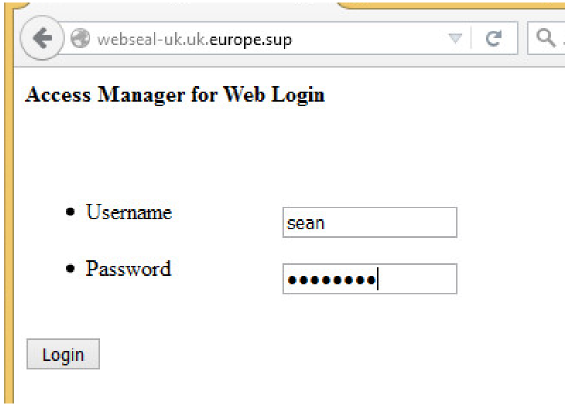


Edit a Standard Junction

Target Backend Servers. At least one server

Hostname
No filter applied
iis-uk.uk.europe.sup

- Authenticate to WebSEAL with the preferred authentication mechanism.

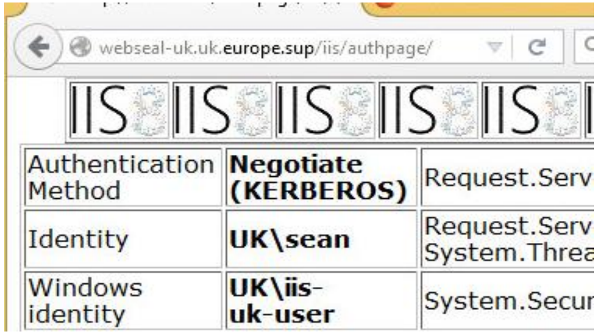


webseal-uk.uk.europe.sup

Access Manager for Web Login

- Username: sean
- Password: ••••••••

- Go to the junctioned IIS server.



webseal-uk.uk.europe.sup/iis/authpage/

Authentication Method	**Negotiate (KERBEROS)**	Request.Serv
Identity	**UK\sean**	Request.Serv System.Threa
Windows identity	**UK\iis-uk-user**	System.Secur

IBM Security

Intelligence. Integration. Expertise.

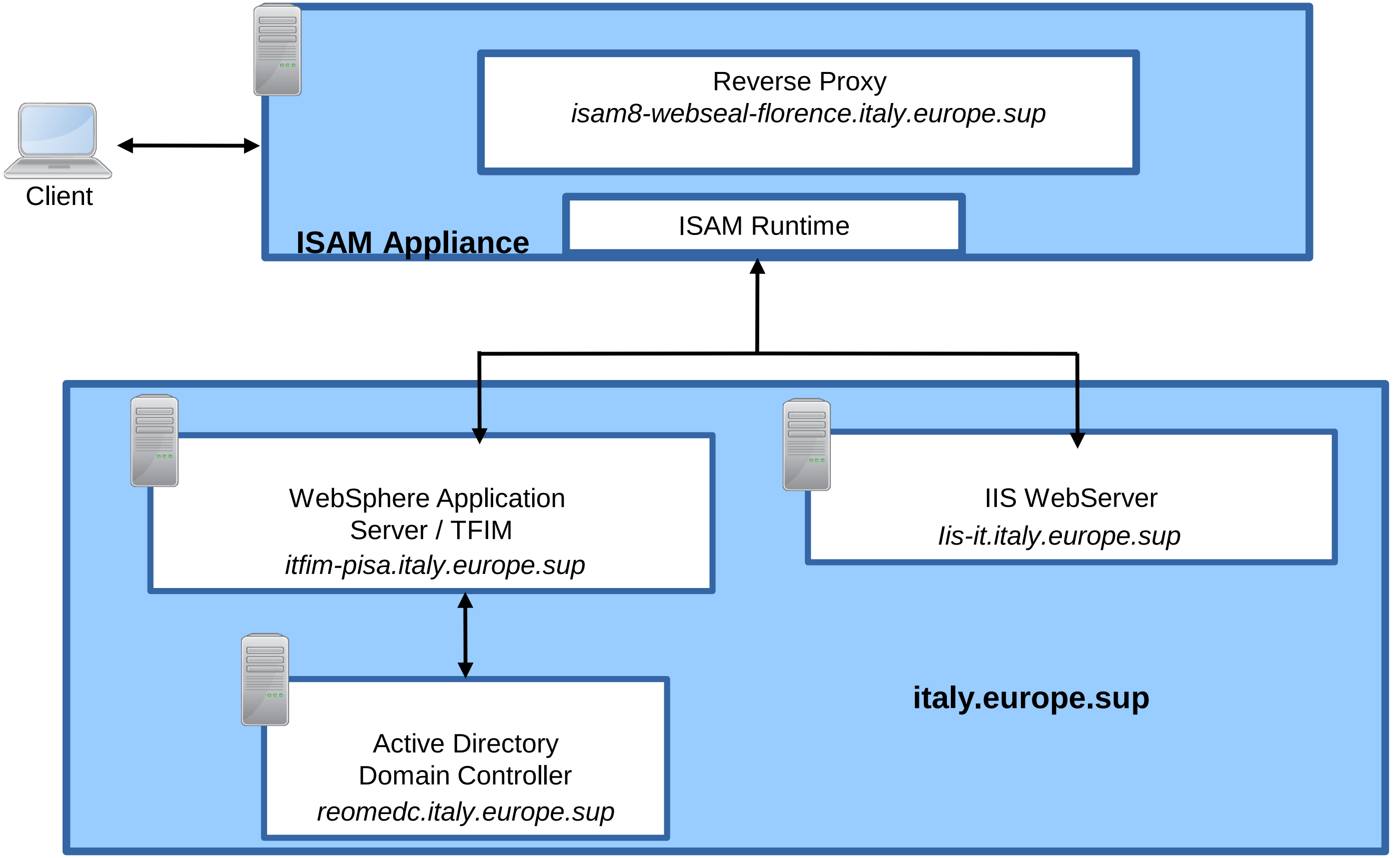
ITFIM enabled Kerberos Junction

ITFIM enabled Kerberos Junction

- Architecture Overview
- SSO flow
- WebSeal Configuration Steps
- Windows Configuration Steps
- TFIM Configuration Steps

ITFIM enabled Kerberos Junction

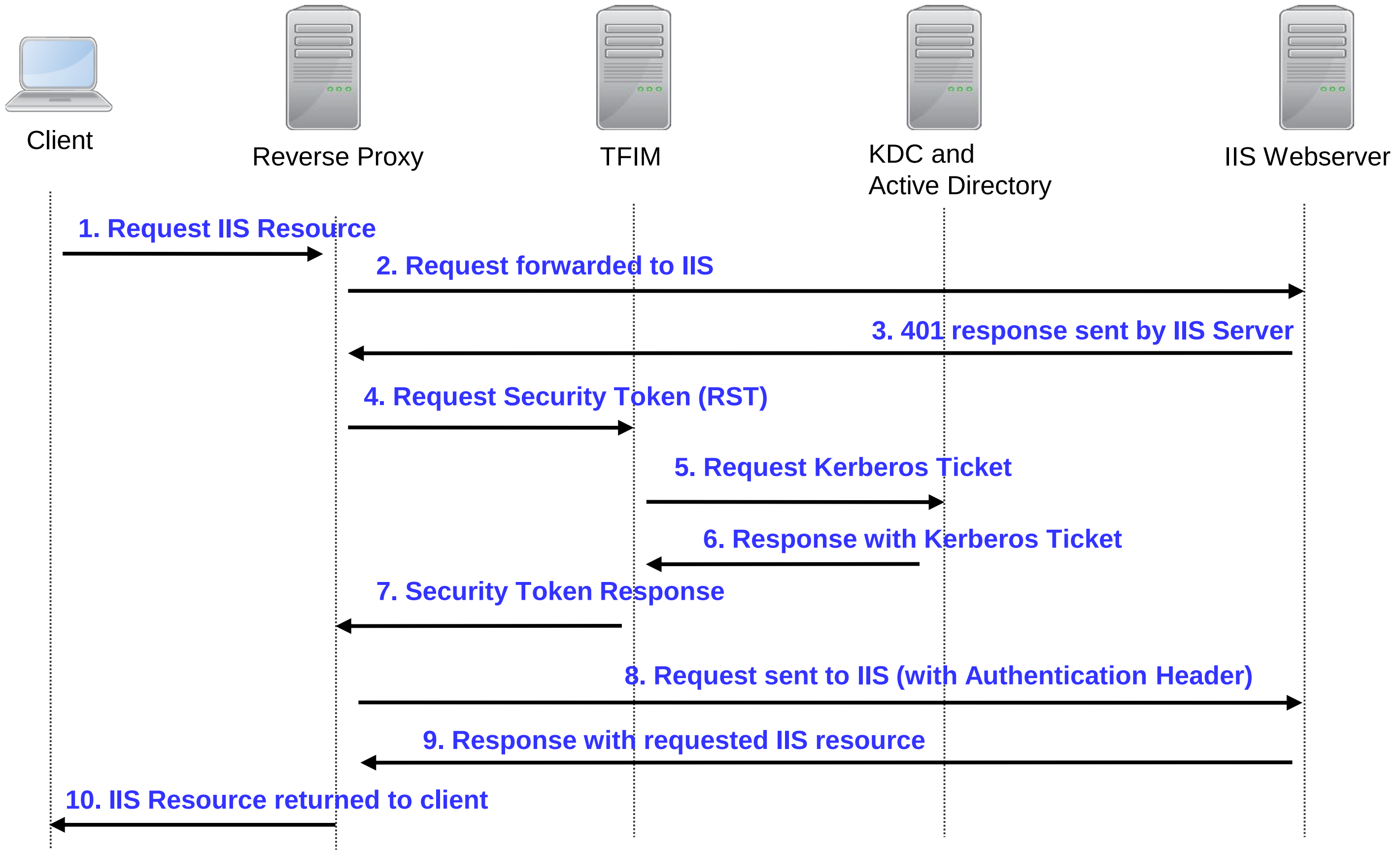
Architecture overview



Reverse Proxy
isam8-webseal-florence.italy.europe.sup
Client
ISAM Appliance
ISAM Runtime
WebSphere Application Server / TFIM
itfim-pisa.italy.europe.sup
IIS WebServer
Iis-it.italy.europe.sup
Active Directory Domain Controller
reomedc.italy.europe.sup
italy.europe.sup

ITFIM enabled Kerberos Junction

SSO Communication Flow



Client
Reverse Proxy
TFIM
KDC and
Active Directory
IIS Webserver
1. Request IIS Resource
2. Request forwarded to IIS
3. 401 response sent by IIS Server
4. Request Security Token (RST)
5. Request Kerberos Ticket
6. Response with Kerberos Ticket
7. Security Token Response
8. Request sent to IIS (with Authentication Header)
9. Response with requested IIS resource
10. IIS Resource returned to client

ITFIM enabled Kerberos Junction

WebSeal configuration steps

- Edit Reverse Proxy Configuration File
  - Create [tfimsso:/kerberossso] - Kerberos Junction configuration entry

```
[tfimsso:/kerberossso]
token-type = kerberos
applies-to = http://isam8-webseal-florence.itlay.europe.sup
service-name = HTTP/iis-it.italy.europe.sup
renewal-window = 15
one-time-token = true
preserve-xml-token = false
token-collection-size = 10
token-transmit-type = header
token-transmit-name = Authorization
always-send-tokens = true
tfim-cluster-name = tfim-pisa
```

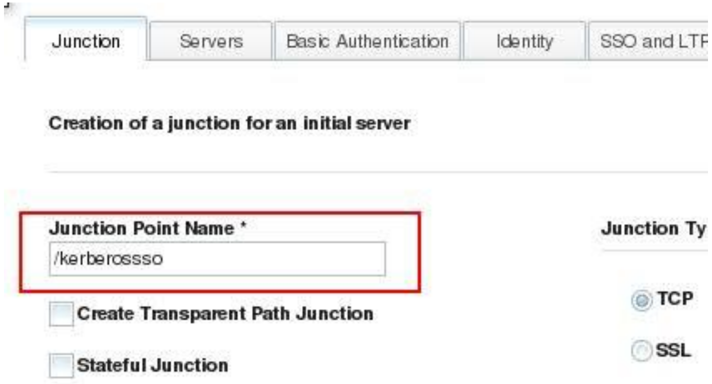
  - Create [tfim-cluster:tfim-pisa] - TFIM connection configuration entry

```
server = 9,http://itfim-pisa.italy.europe.sup:9080/TrustServerWST13/services/RequestSecurityToken
```

ITFIM enabled Kerberos Junction

WebSeal configuration steps

- Ensure junction point name matches :
  [tfimsso:/kerberossso]



Creation of a junction for an initial server

Junction Point Name *: /kerberossso

☐ **Create Transparent Path Junction**

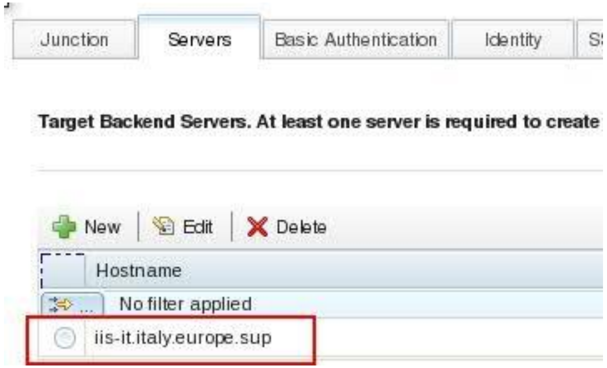
☐ **Stateful Junction**

Junction Ty

● **TCP**

○ **SSL**

- Ensure the Target Backend Server is configured for your IIS server



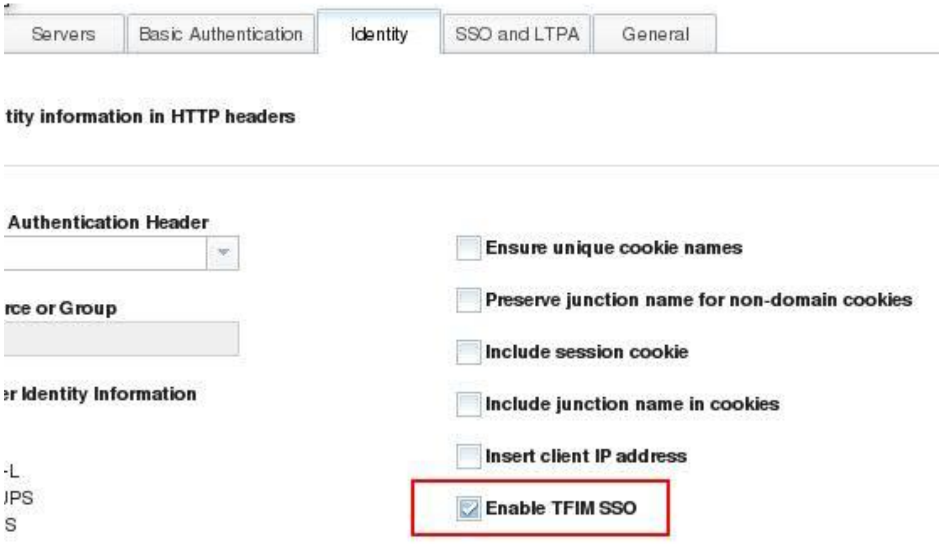
Target Backend Servers. At least one server is required to create

Hostname
No filter applied
○ iis-it.italy.europe.sup

ITFIM enabled Kerberos Junction

WebSeal configuration steps

- Ensure on Identity Tab TFIM SSO is selected



tity information in HTTP headers

Authentication Header

rce or Group

er Identity Information

-L
IPS
S

☐ Ensure unique cookie names

☐ Preserve junction name for non-domain cookies

☐ Include session cookie

☐ Include junction name in cookies

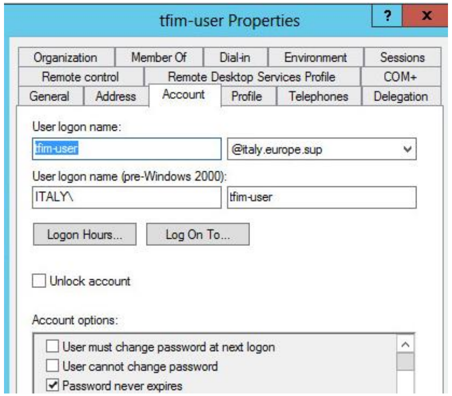
☐ Insert client IP address

☑ Enable TFIM SSO

ITFIM enabled Kerberos Junction

Windows configuration steps

- Create a tfim user in AD



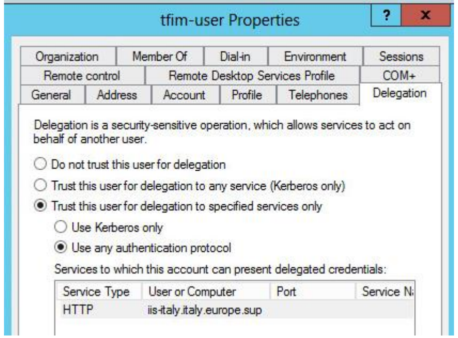
User logon name:
tfim-user @italy.europe.sup

User logon name (pre-Windows 2000):
ITALY\ tfim-user

☐ Unlock account

Account options:
☐ User must change password at next logon
☐ User cannot change password
☑ Password never expires

- Set delegation



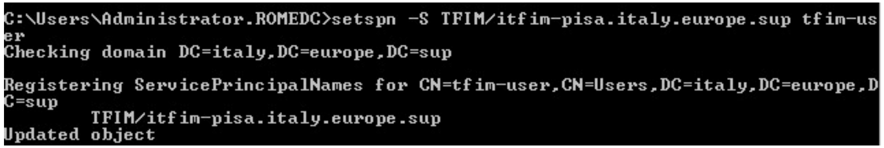
Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation
○ Trust this user for delegation to any service (Kerberos only)
● Trust this user for delegation to specified services only
  ○ Use Kerberos only
  ● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
HTTP	iis-italy.italy.europe.sup		

- Run setspn against this user

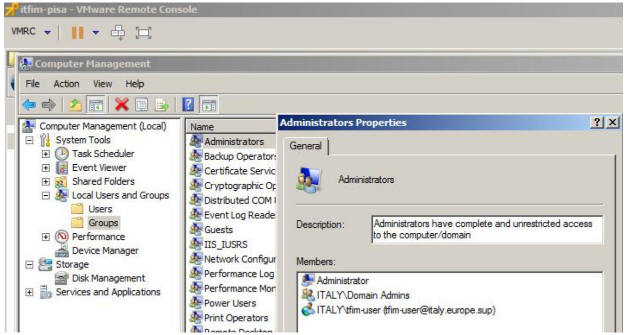


```
C:\Users\Administrator.ROMEDC>setspn -S TFIM/itfim-pisa.italy.europe.sup tfim-us
er
Checking domain DC=italy,DC=europe,DC=sup

Registering ServicePrincipalNames for CN=tfim-user,CN=Users,DC=italy,DC=europe,D
C=sup
        TFIM/itfim-pisa.italy.europe.sup
Updated object
```

ITFIM enabled Kerberos Junction

Windows configuration steps (cont)

- Add the user to the local *Administrators* group

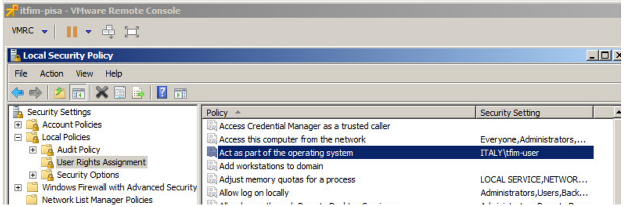


Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

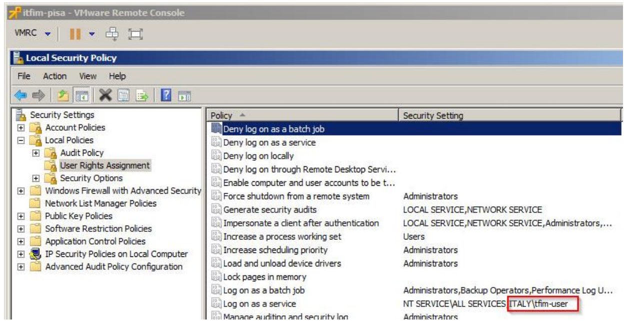
Members:
Administrator
ITALY\Domain Admins
ITALY\tfim-user (tfim-user@italy.europe.sup)

- Grant the Act as part of the operating system privilege on the local machine



Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators,...
Act as part of the operating system	ITALY\tfim-user
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWOR...
Allow log on locally	Administrators,Users,Back...

- Grant the Log on as a service privilege on the local machine.

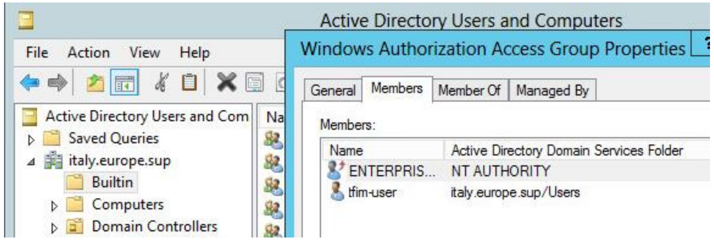

itfim-pisa - VMware Remote Console
VMRC
Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Deny log on through Remote Desktop Servi...	
Enable computer and user accounts to be t...	
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication	LOCAL SERVICE,NETWORK SERVICE,Administrators,...
Increase a process working set	Users
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	Administrators,Backup Operators,Performance Log U...
Log on as a service	NT SERVICE\ALL SERVICES,ITALY\tfim-user
Manage auditing and security log	Administrators

ITFIM enabled Kerberos Junction

Windows configuration steps (cont)

- Add the user Windows Authorization Access Groups object on the AD machine

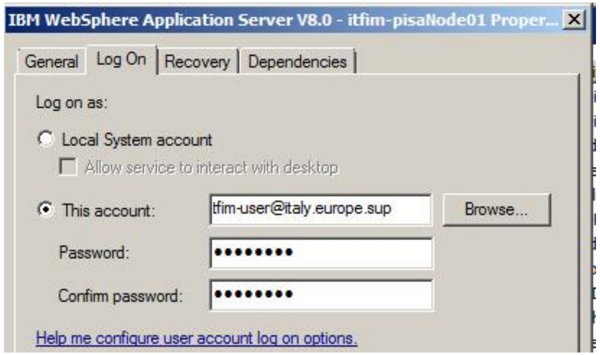


Members:

Name	Active Directory Domain Services Folder
ENTERPRIS...	NT AUTHORITY
tfim-user	italy.europe.sup/Users

- If not yet done enable the WebSphere process to run as a Windows service by executing the *wasservice* command

- Change WAS service to start as tfim user


IBM WebSphere Application Server V8.0 - itfim-pisaNode01 Proper...
General
Log On
Recovery
Dependencies
Browse...

Log on as:

○ Local System account

☐ Allow service to interact with desktop

● This account: tfim-user@italy.europe.sup

Password: ••••••••

Confirm password: ••••••••

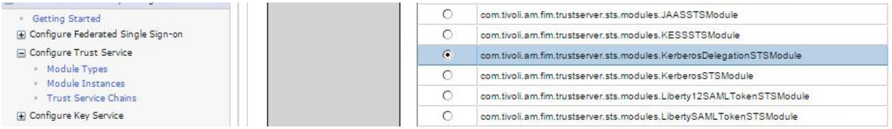
Help me configure user account log on options.

ITFIM enabled Kerberos Junction

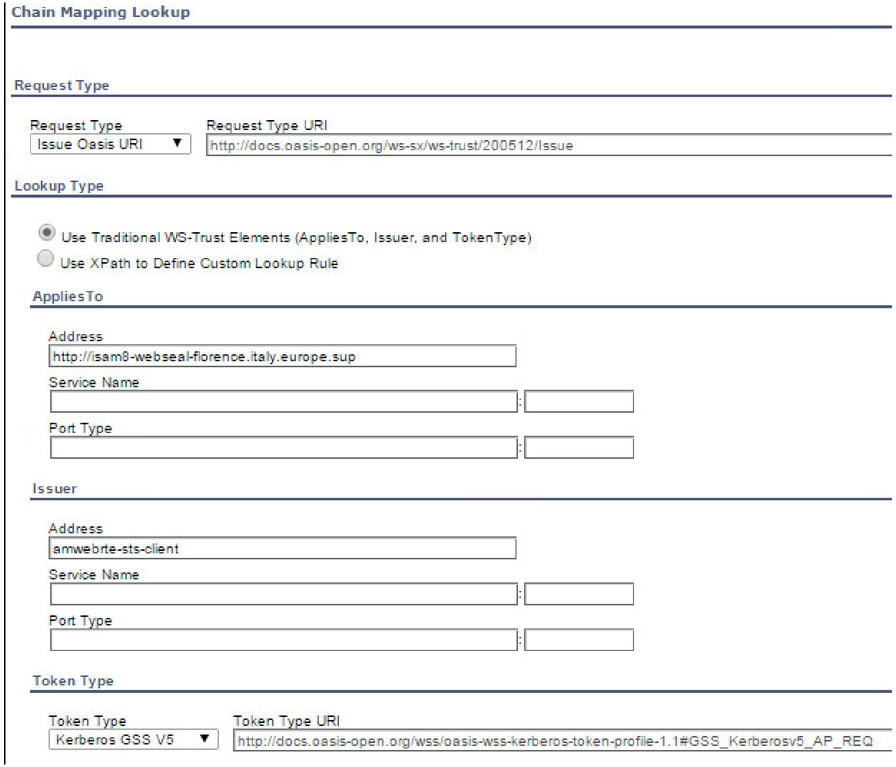
ITFIM configuration steps

- Create an instance in Kerberos delegation module

- Create a tfim trust chain



○ com.tivoli.am.fim.trustserver.sts.modules.JAASSTSModule
○ com.tivoli.am.fim.trustserver.sts.modules.KESSSTSModule
● com.tivoli.am.fim.trustserver.sts.modules.KerberosDelegationSTSModule
○ com.tivoli.am.fim.trustserver.sts.modules.KerberosSTSModule
○ com.tivoli.am.fim.trustserver.sts.modules.Liberty12SAMLTokenSTSModule
○ com.tivoli.am.fim.trustserver.sts.modules.LibertySAMLTokenSTSModule



Chain Mapping Lookup

Request Type

Request Type: Issue Oasis URI
Request Type URI: http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue

Lookup Type

● Use Traditional WS-Trust Elements (AppliesTo, Issuer, and TokenType)
○ Use XPath to Define Custom Lookup Rule

AppliesTo

Address: http://isam8-webseal-florence.italy.europe.sup
Service Name:
Port Type:

Issuer

Address: amwebrte-sts-client
Service Name:
Port Type:

Token Type

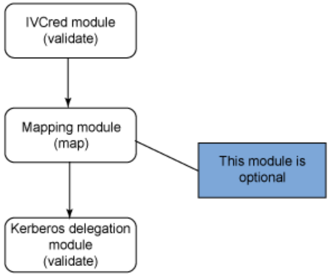
Token Type: Kerberos GSS V5
Token Type URI: http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ

ITFIM enabled Kerberos Junction

ITFIM configuration steps (cont)

- Minimal Chain composed by 2 modules

- Optional map modules :
  - Default map module
  - Directory Integrator map module
  - Custom map module

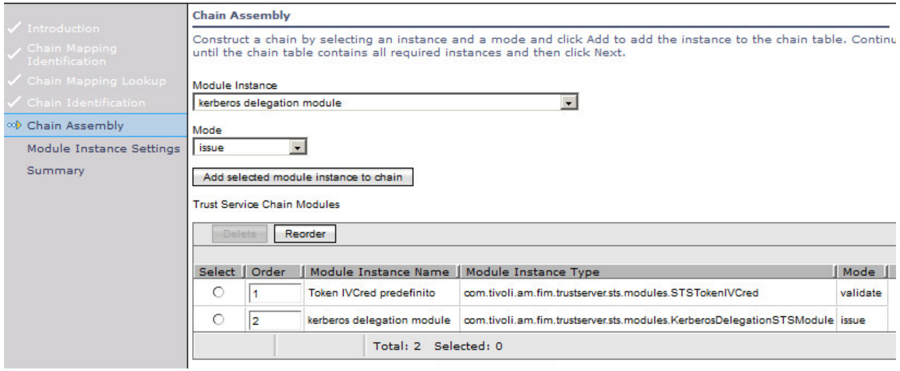


IVCred module (validate)

Mapping module (map)

This module is optional

Kerberos delegation module (validate)



Chain Assembly

Construct a chain by selecting an instance and a mode and click Add to add the instance to the chain table. Continu until the chain table contains all required instances and then click Next.

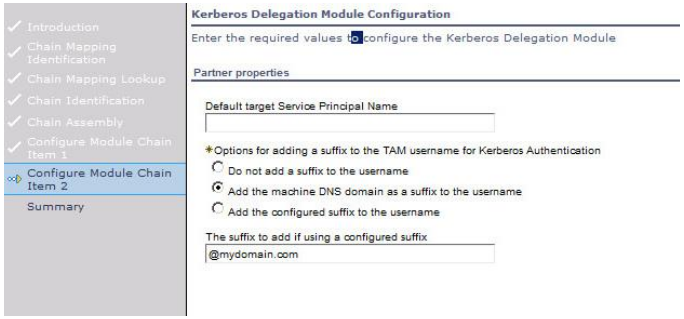
Module Instance: kerberos delegation module

Mode: issue

Trust Service Chain Modules

Select	Order	Module Instance Name	Module Instance Type	Mode
○	1	Token IVCred predefinito	com.tivoli.am.fim.trustserver.sts.modules.STSTokenIVCred	validate
○	2	kerberos delegation module	com.tivoli.am.fim.trustserver.sts.modules.KerberosDelegationSTSModule	issue

Total: 2 Selected: 0


Introduction
Chain Mapping Identification
Chain Mapping Lookup
Chain Identification
Chain Assembly
Configure Module Chain Item 1
Configure Module Chain Item 2
Summary

Kerberos Delegation Module Configuration

Enter the required values to configure the Kerberos Delegation Module

Partner properties

Default target Service Principal Name

*Options for adding a suffix to the TAM username for Kerberos Authentication
○ Do not add a suffix to the username
● Add the machine DNS domain as a suffix to the username
○ Add the configured suffix to the username

The suffix to add if using a configured suffix: @mydomain.com

IBM Security

Intelligence. Integration. Expertise.

Delegation in Multiple Active Directory Domains

Delegation in Multiple Active Directory Domains

- Multi-Domain Kerberos SSO support
- Architecture Domains and Trusts
- Leveraging Federated Directories and Basic User Support
- Kerberos User Identity Rule
- Shortcut Trusts

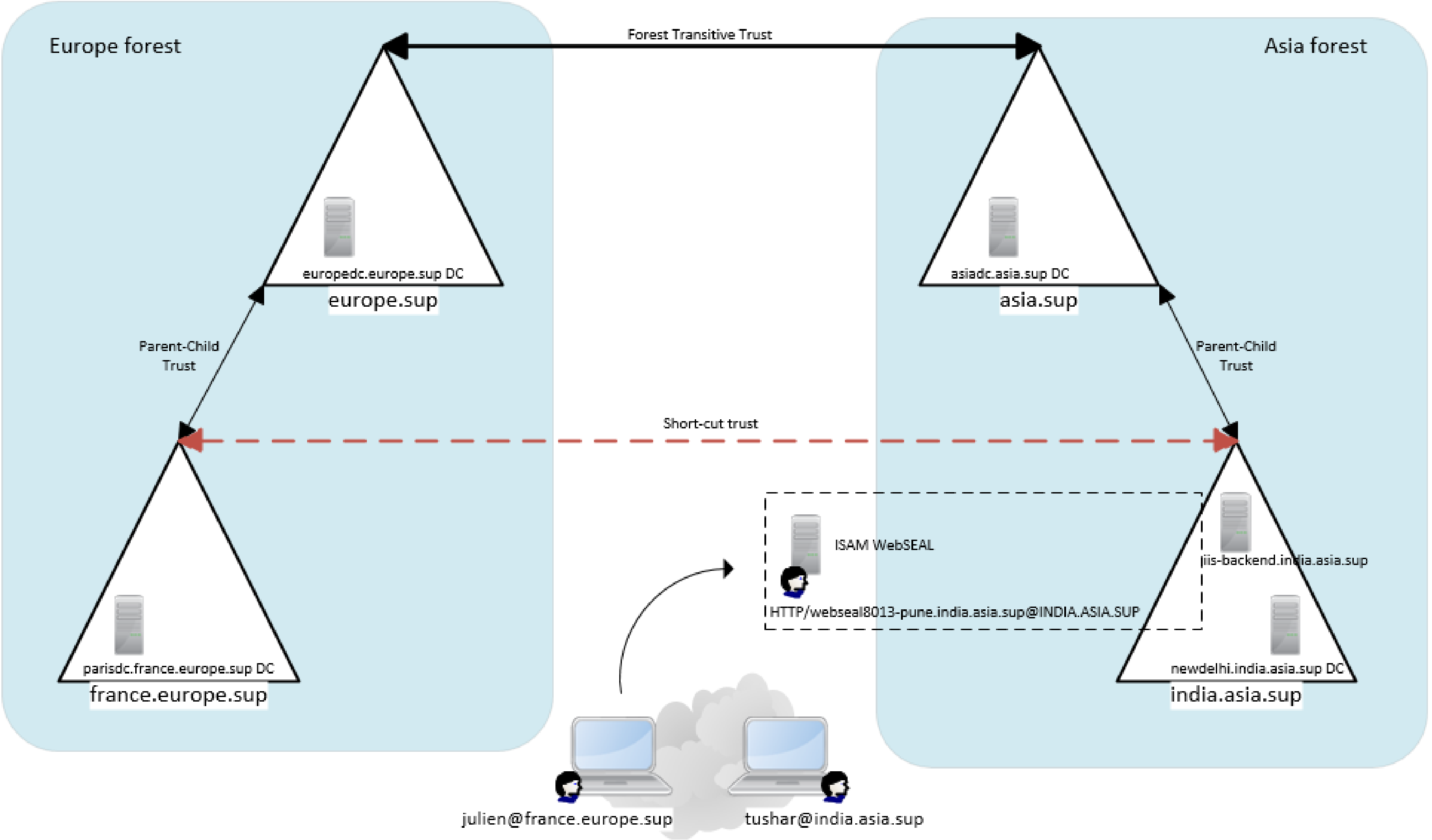
Delegation in Multiple Active Directory Domains

Multi-Domain Kerberos SSO support

- Functionality available starting in ISAM 8.0.1.0
- All domains must be configured in the kerberos Realm tab, and must have a kdc specified
- A transitive trust is required between the domains
- WebSEAL service account has to reside in the same domain as the back-end service account
- Users can reside in a domain that is different from the WebSEAL service account domain
- User identity needs to be customized to effectively achieve the constrained delegation from a user domain different from the WeBSEAL sevice account domain
  - Achieved via kerberos-user-identity parameter in the Web Reverse Proxy (WebSEAL) configuration file

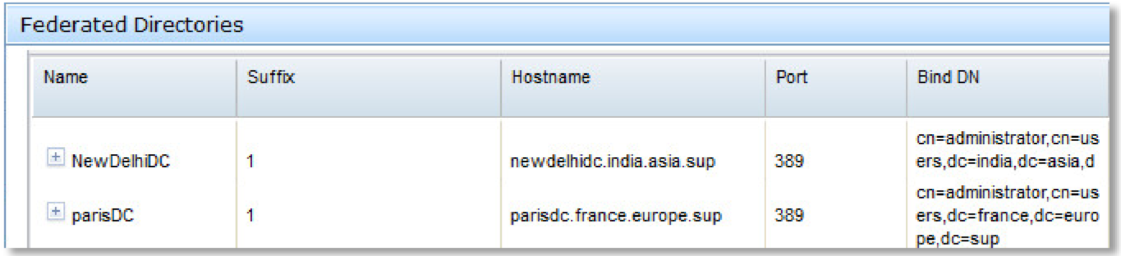
Delegation in Multiple Active Directory Domains

Architecture Domains and Trusts



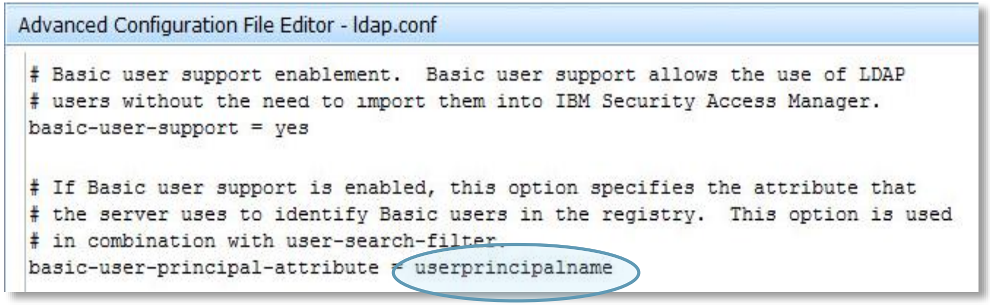
Delegation in Multiple Active Directory Domains

Leveraging Federated Directories and Basic User Support



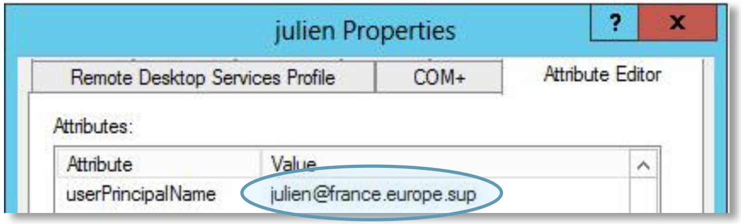
Federated Directories

Name	Suffix	Hostname	Port	Bind DN
⊞ NewDelhiDC	1	newdelhidc.india.asia.sup	389	cn=administrator,cn=users,dc=india,dc=asia,d
⊞ parisDC	1	parisdc.france.europe.sup	389	cn=administrator,cn=users,dc=france,dc=europe,dc=sup



Advanced Configuration File Editor - ldap.conf

```
# Basic user support enablement.  Basic user support allows the use of LDAP
# users without the need to import them into IBM Security Access Manager.
basic-user-support = yes

# If Basic user support is enabled, this option specifies the attribute that
# the server uses to identify Basic users in the registry.  This option is used
# in combination with user-search-filter.
basic-user-principal-attribute = userprincipalname
```



julien Properties

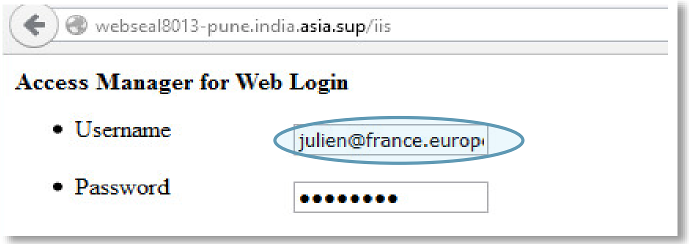
Attributes:

Attribute	Value
userPrincipalName	julien@france.europe.sup

Delegation in Multiple Active Directory Domains

Kerberos User Identity Rule

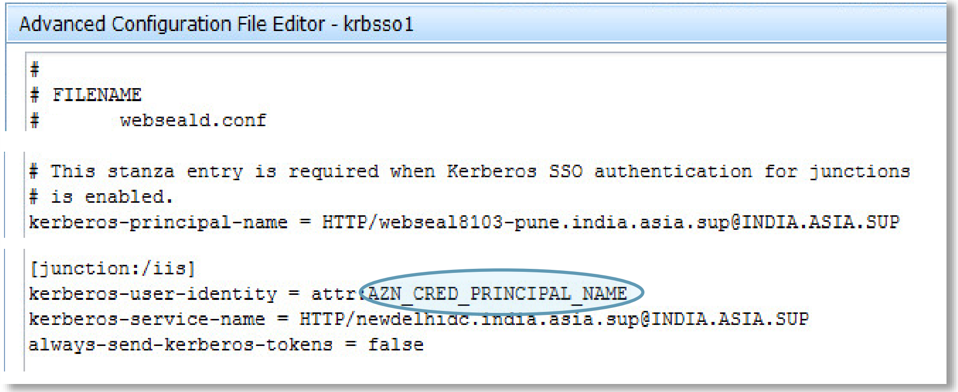
- Replacing the UPN with information from the credential



webseal8013-pune.india.asia.sup/iis

Access Manager for Web Login

- Username julien@france.europ
- Password ●●●●●●●●●



Advanced Configuration File Editor - krbsso1

```
#
# FILENAME
#       webseald.conf

# This stanza entry is required when Kerberos SSO authentication for junctions
# is enabled.
kerberos-principal-name = HTTP/webseal8103-pune.india.asia.sup@INDIA.ASIA.SUP

[junction:/iis]
kerberos-user-identity = attr:AZN_CRED_PRINCIPAL_NAME
kerberos-service-name = HTTP/newdelhidc.india.asia.sup@INDIA.ASIA.SUP
always-send-kerberos-tokens = false
```

Delegation in Multiple Active Directory Domains

Kerberos User Identity Rule

Possible formats

- kerberos-user-identity = julien@FRANCE.EUROPE.SUP
- kerberos-user-identity = julien
- kerberos-user-identity = tushar
- kerberos-user-identity = @FRANCE.EUROPE.SUP

- kerberos-user-identity = attr:username@attr:dom
- kerberos-user-identity = attr:username
- kerberos-user-identity = @attr:dom
- kerberos-user-identity = attr:upn

- kerberos-user-identity = attr:username@IBM.COM
- kerberos-user-identity = bob@attr:dom

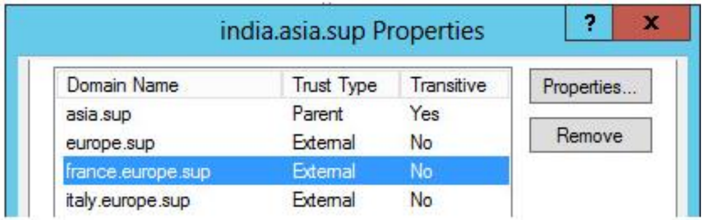
- kerberos-user-identity = @attr:dn

Delegation in Multiple Active Directory Domains

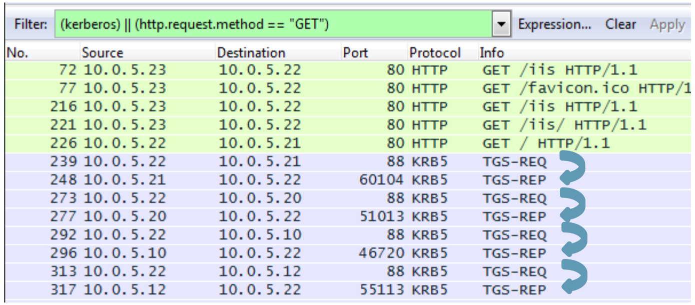
Shortcut Trusts

No shortcut trust in place

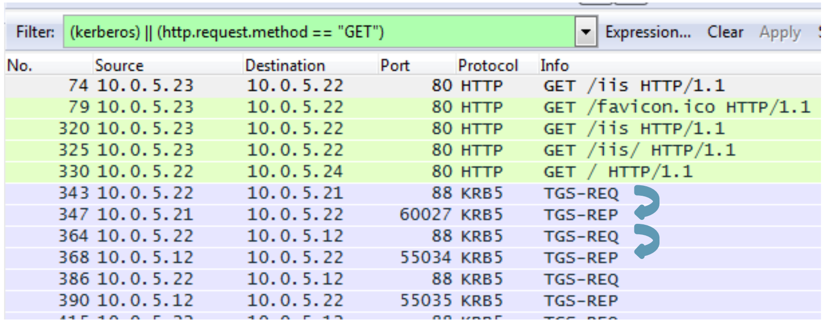
- WebSEAL will be instructed a path to follow to the point where it reaches the correct KDC
- From *india.asia.sup* DC to *asia.sup* root DC to *europe.sup* root DC to *france.europe.sup* DC
- With shortcut trust in place : Single hop to *france.europe.sup* domain



Domain Name	Trust Type	Transitive
asia.sup	Parent	Yes
europe.sup	External	No
france.europe.sup	External	No
italy.europe.sup	External	No



```
Filter: (kerberos) || (http.request.method == "GET")
No.   Source      Destination  Port   Protocol  Info
 72 10.0.5.23   10.0.5.22       80 HTTP     GET /iis HTTP/1.1
 77 10.0.5.23   10.0.5.22       80 HTTP     GET /favicon.ico HTTP/1
216 10.0.5.23   10.0.5.22       80 HTTP     GET /iis HTTP/1.1
221 10.0.5.23   10.0.5.22       80 HTTP     GET /iis/ HTTP/1.1
226 10.0.5.22   10.0.5.21       80 HTTP     GET / HTTP/1.1
239 10.0.5.22   10.0.5.21       88 KRB5     TGS-REQ
248 10.0.5.21   10.0.5.22    60104 KRB5     TGS-REP
273 10.0.5.22   10.0.5.20       88 KRB5     TGS-REQ
277 10.0.5.20   10.0.5.22    51013 KRB5     TGS-REP
292 10.0.5.22   10.0.5.10       88 KRB5     TGS-REQ
296 10.0.5.10   10.0.5.22    46720 KRB5     TGS-REP
313 10.0.5.22   10.0.5.12       88 KRB5     TGS-REQ
317 10.0.5.12   10.0.5.22    55113 KRB5     TGS-REP
```



```
Filter: (kerberos) || (http.request.method == "GET")
No.   Source      Destination  Port   Protocol  Info
 74 10.0.5.23   10.0.5.22       80 HTTP     GET /iis HTTP/1.1
 79 10.0.5.23   10.0.5.22       80 HTTP     GET /favicon.ico HTTP/1.1
320 10.0.5.23   10.0.5.22       80 HTTP     GET /iis HTTP/1.1
325 10.0.5.23   10.0.5.22       80 HTTP     GET /iis/ HTTP/1.1
330 10.0.5.22   10.0.5.24       80 HTTP     GET / HTTP/1.1
343 10.0.5.22   10.0.5.21       88 KRB5     TGS-REQ
347 10.0.5.21   10.0.5.22    60027 KRB5     TGS-REP
364 10.0.5.22   10.0.5.12       88 KRB5     TGS-REQ
368 10.0.5.12   10.0.5.22    55034 KRB5     TGS-REP
386 10.0.5.22   10.0.5.12       88 KRB5     TGS-REQ
390 10.0.5.12   10.0.5.22    55035 KRB5     TGS-REP
```

IBM Security

Intelligence. Integration. Expertise.

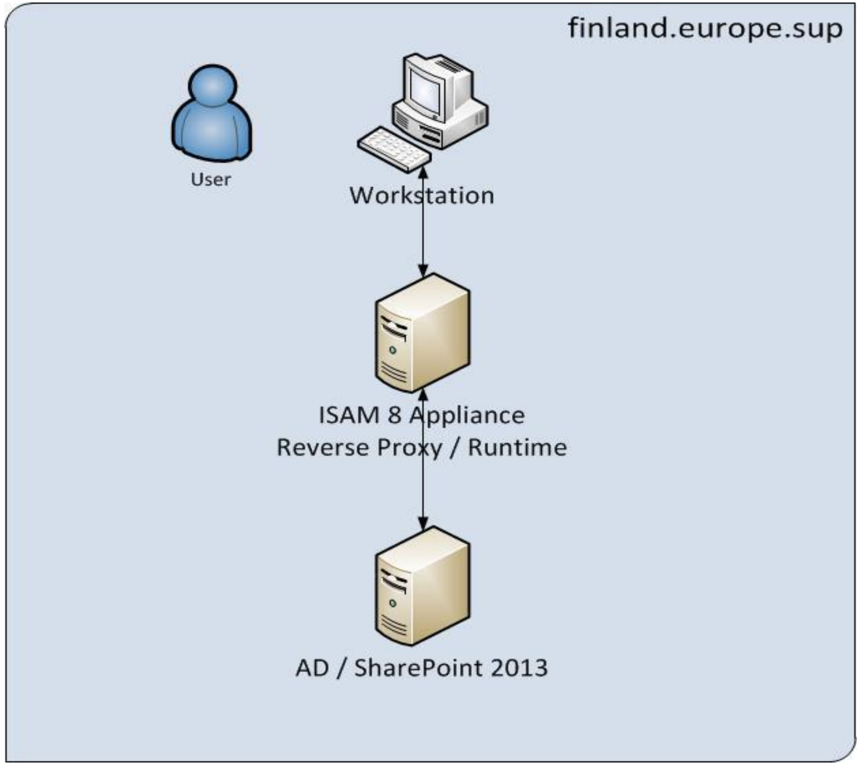
Integration with Microsoft SharePoint

Integration with Microsoft SharePoint

- Physical architecture view
- Logical architecture view
- Create the service account for the SharePoint
- Create the WebSEAL impersonation account
- Configure the SharePoint Web Application
- Verify SharePoint Kerberos Authentication
- Configure WebSEAL and junction on the ISAM appliance
- Access SharePoint through the WebSEAL junction

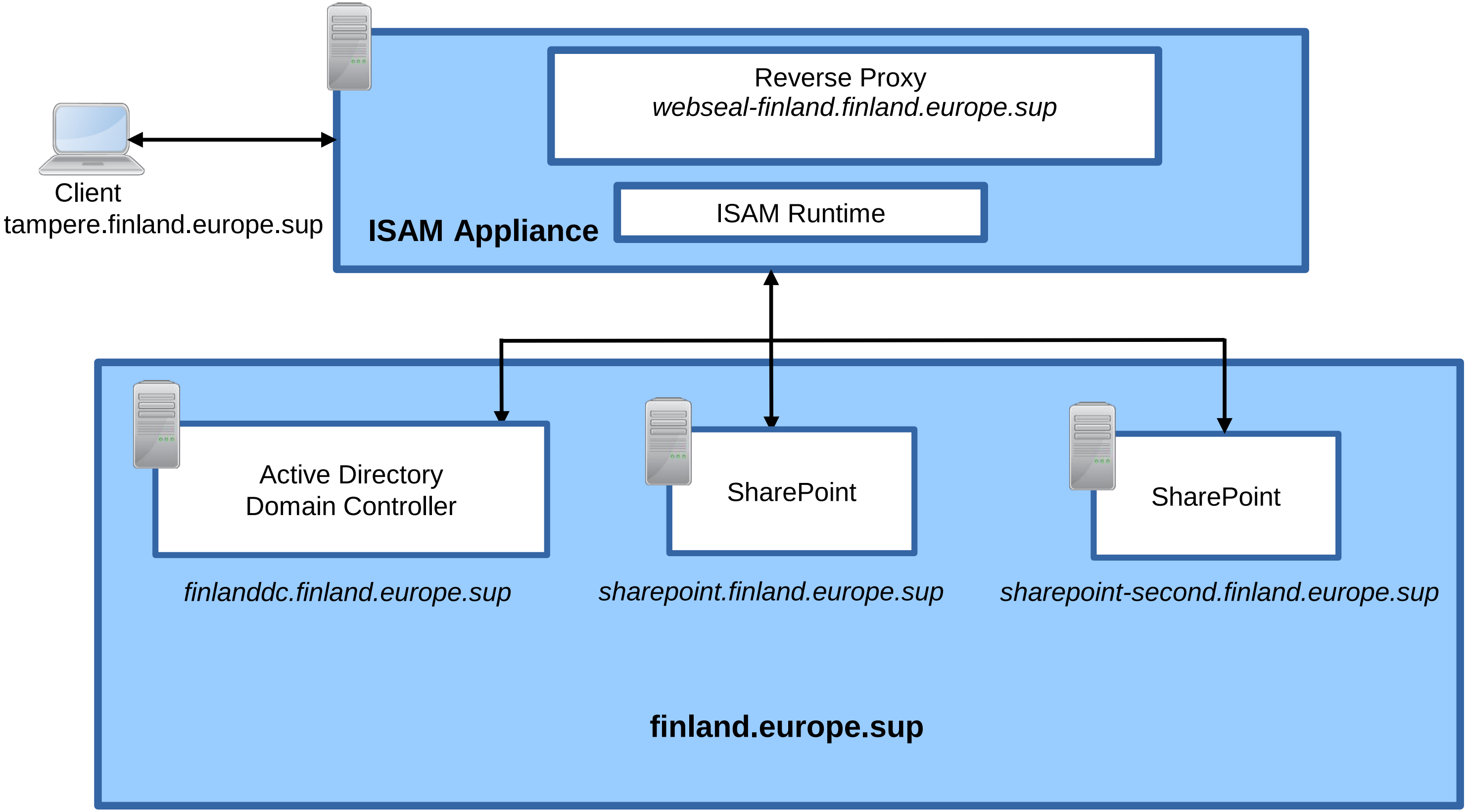
Integration with Microsoft SharePoint

Physical architecture view



Integration with Microsoft SharePoint

Logical architecture view



Reverse Proxy
webseal-finland.finland.europe.sup

ISAM Runtime

ISAM Appliance

Client
tampere.finland.europe.sup

Active Directory
Domain Controller

finlanddc.finland.europe.sup

SharePoint

sharepoint.finland.europe.sup

SharePoint

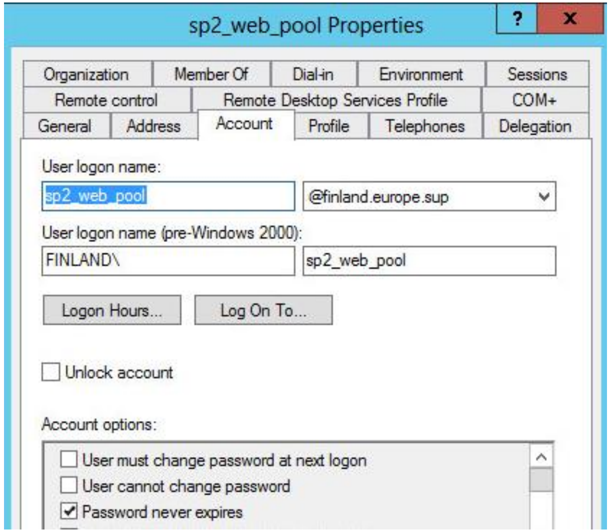
sharepoint-second.finland.europe.sup

finland.europe.sup

Integration with Microsoft SharePoint

Create the service account for the SharePoint

- Create an user account for the SharePoint Web Pool



sp2_web_pool Properties

User logon name: sp2_web_pool @finland.europe.sup

User logon name (pre-Windows 2000): FINLAND\ sp2_web_pool

☐ Unlock account

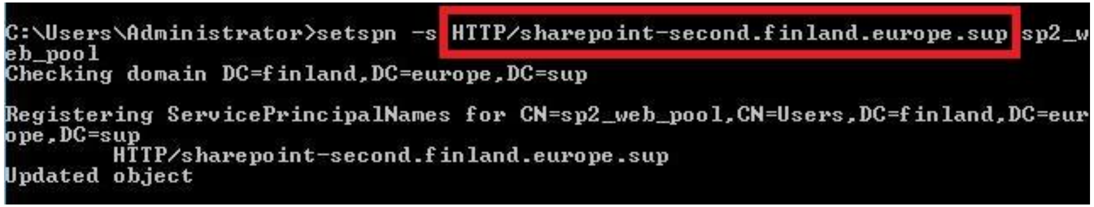
Account options:

☐ User must change password at next logon

☐ User cannot change password

☑ Password never expires

- Set SPN that match the FQDN of the SharePoint Web Site



```
C:\Users\Administrator>setspn -s HTTP/sharepoint-second.finland.europe.sup sp2_w
eb_pool
Checking domain DC=finland,DC=europe,DC=sup

Registering ServicePrincipalNames for CN=sp2_web_pool,CN=Users,DC=finland,DC=eur
ope,DC=sup
        HTTP/sharepoint-second.finland.europe.sup
Updated object
```

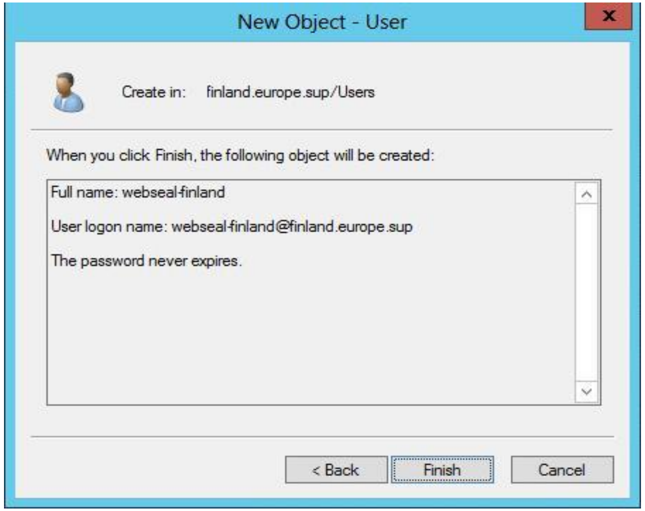
Integration with Microsoft SharePoint

Create the WebSEAL impersonation account

- Create an user account for the WebSEAL on the Active Directory

- Generate the keytab file
  Example:
  ktpass -out c:\tmp\webseal.keytab -princ HTTP/webseal-finland@FINLAND.EUROPE.SUP -mapuser webseal-finland -mapOp set -pass <passwd> -pType KRB5_NT_PRINCIPAL

- Modify the user account to delegate to the SharePoint service



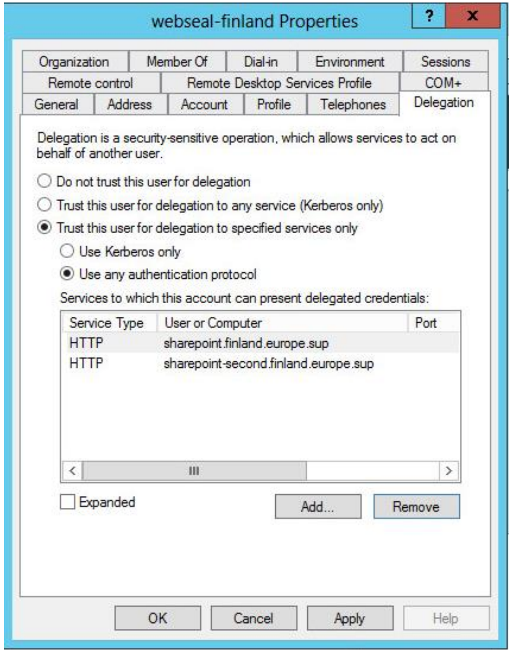
Create in: finland.europe.sup/Users

When you click Finish, the following object will be created:

Full name: webseal-finland

User logon name: webseal-finland@finland.europe.sup

The password never expires.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation
○ Trust this user for delegation to any service (Kerberos only)
● Trust this user for delegation to specified services only
  ○ Use Kerberos only
  ● Use any authentication protocol

Services to which this account can present delegated credentials:

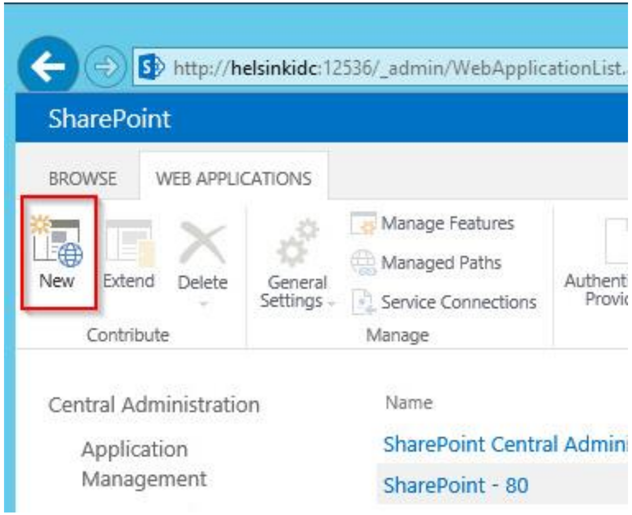
Service Type	User or Computer	Port
HTTP	sharepoint.finland.europe.sup	
HTTP	sharepoint-second.finland.europe.sup	

☐ Expanded

Integration with Microsoft SharePoint

Configure the SharePoint Web Application

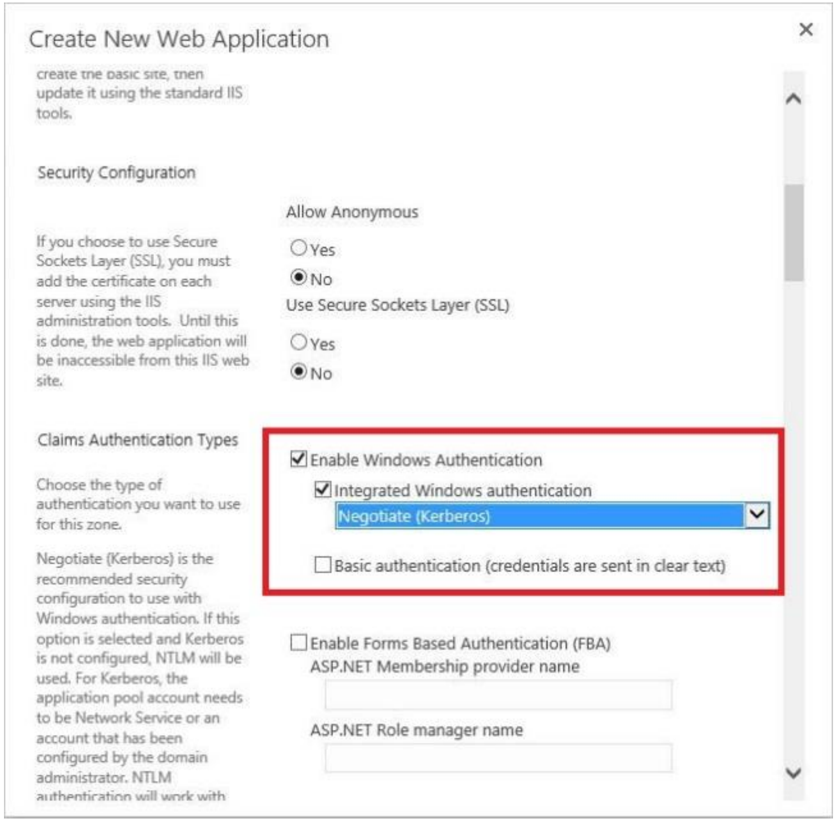
- From the SharePoint Central Administration page start a new Web Site



Integration with Microsoft SharePoint

Configure the SharePoint Web Application

- For the Integrated Windows authentication select Negotiate (Kerberos)



Create New Web Application

create the basic site, then update it using the standard IIS tools.

Security Configuration

If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS web site.

Allow Anonymous

○ Yes
● No

Use Secure Sockets Layer (SSL)

○ Yes
● No

Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with

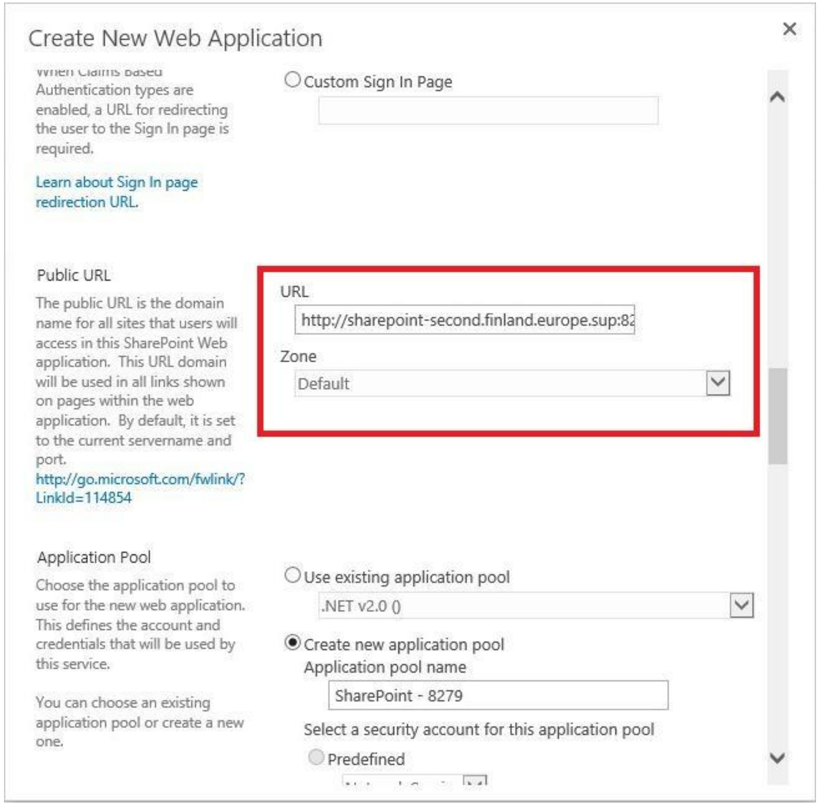
☑ Enable Windows Authentication
☑ Integrated Windows authentication
Negotiate (Kerberos)
☐ Basic authentication (credentials are sent in clear text)

☐ Enable Forms Based Authentication (FBA)
ASP.NET Membership provider name
ASP.NET Role manager name

Integration with Microsoft SharePoint

Configure the SharePoint Web Application

- The host name in the URL setting must match the SPN defined with the ”setspn -S <SPN> <accountname>” command



Create New Web Application

When Claims based Authentication types are enabled, a URL for redirecting the user to the Sign In page is required.

Learn about Sign In page redirection URL.

○ Custom Sign In Page

Public URL

The public URL is the domain name for all sites that users will access in this SharePoint Web application. This URL domain will be used in all links shown on pages within the web application. By default, it is set to the current servername and port. http://go.microsoft.com/fwlink/?LinkId=114854

URL: http://sharepoint-second.finland.europe.sup:8

Zone: Default

Application Pool

Choose the application pool to use for the new web application. This defines the account and credentials that will be used by this service.

You can choose an existing application pool or create a new one.

○ Use existing application pool

.NET v2.0 ()

● Create new application pool

Application pool name: SharePoint - 8279

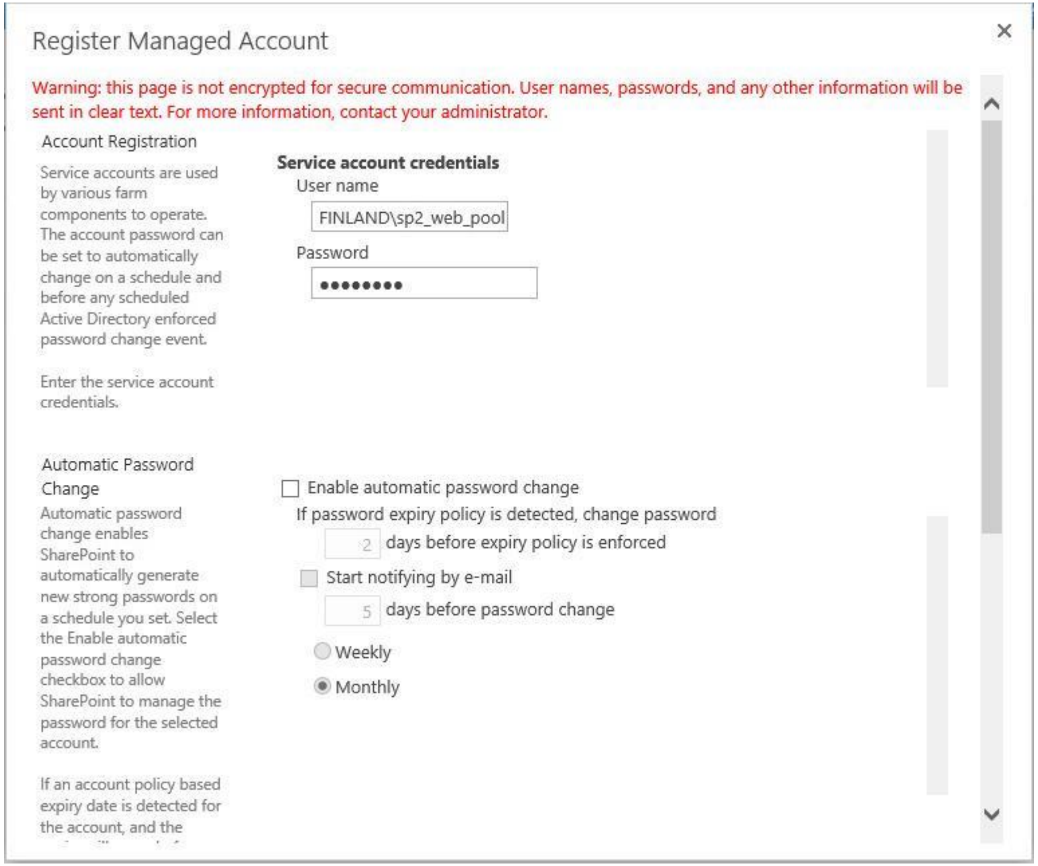
Select a security account for this application pool

○ Predefined

Integration with Microsoft SharePoint

Configure the SharePoint Web Application

- Register the account created earlier as SharePoint service account
- By clicking the ”Register New Managed Account” a pop-up will show up



Register Managed Account

Warning: this page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

Account Registration

Service accounts are used by various farm components to operate. The account password can be set to automatically change on a schedule and before any scheduled Active Directory enforced password change event.

Enter the service account credentials.

Service account credentials

User name: FINLAND\sp2_web_pool

Password: ●●●●●●●●●

Automatic Password Change

Automatic password change enables SharePoint to automatically generate new strong passwords on a schedule you set. Select the Enable automatic password change checkbox to allow SharePoint to manage the password for the selected account.

If an account policy based expiry date is detected for the account, and the

☐ Enable automatic password change

If password expiry policy is detected, change password

2 days before expiry policy is enforced

☐ Start notifying by e-mail

5 days before password change

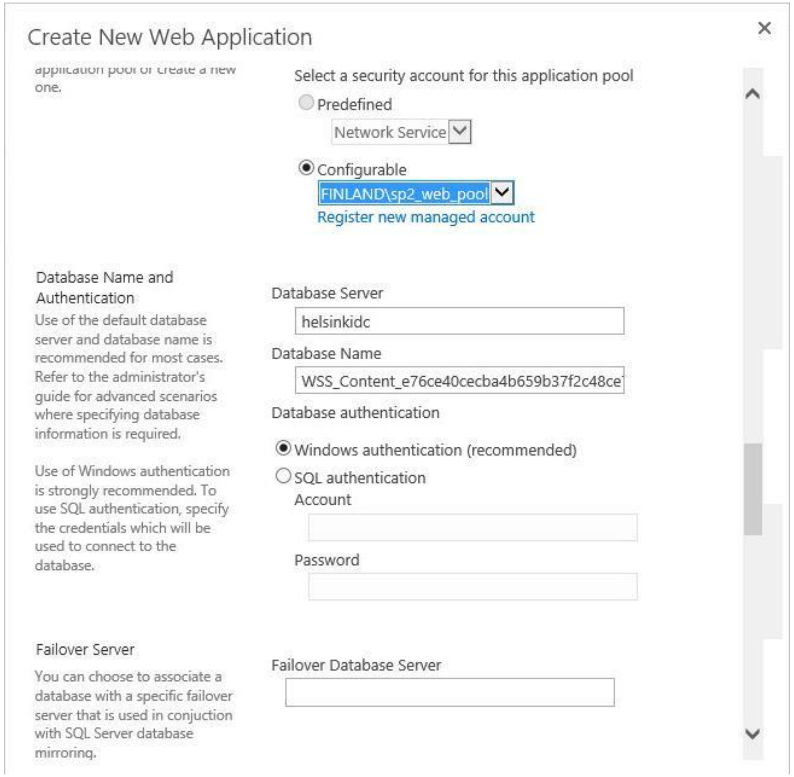
○ Weekly

● Monthly

Integration with Microsoft SharePoint

Configure the SharePoint Web Application

- Finalize the creation of the New Web Application



Create New Web Application

application pool or create a new one.

Select a security account for this application pool

○ Predefined

Network Service

● Configurable

FINLAND\sp2_web_pool

Register new managed account

Database Name and Authentication

Use of the default database server and database name is recommended for most cases. Refer to the administrator's guide for advanced scenarios where specifying database information is required.

Use of Windows authentication is strongly recommended. To use SQL authentication, specify the credentials which will be used to connect to the database.

Database Server: helsinkidc

Database Name: WSS_Content_e76ce40cecba4b659b37f2c48ce

Database authentication

● Windows authentication (recommended)

○ SQL authentication

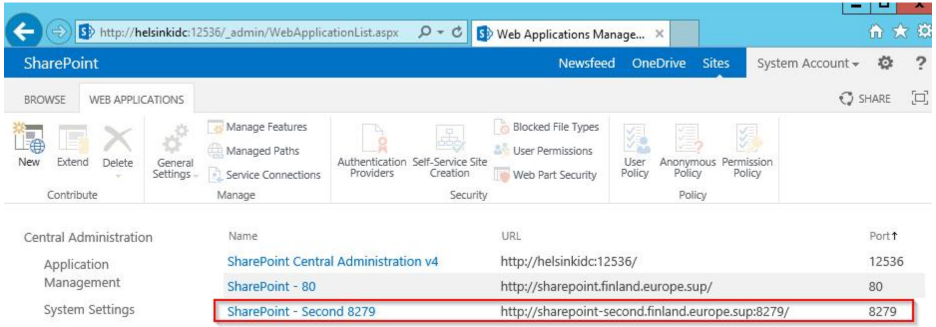
Account:

Password:

Failover Server

You can choose to associate a database with a specific failover server that is used in conjuction with SQL Server database mirroring.

Failover Database Server:



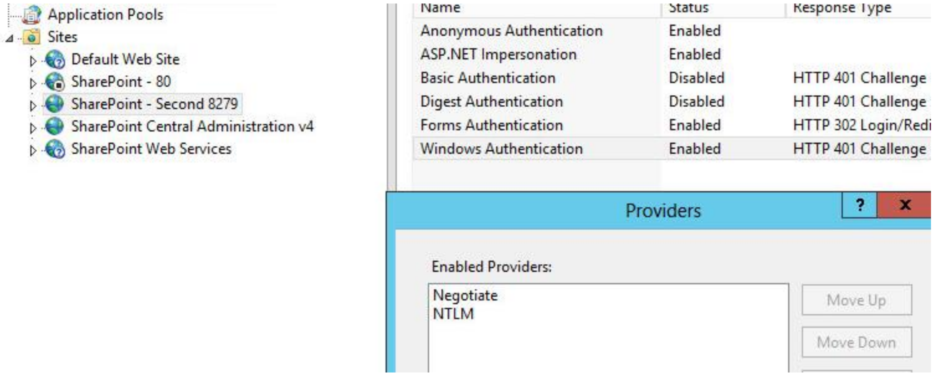
http://helsinkidc:12536/_admin/WebApplicationList.aspx

Name	URL	Port ↑
SharePoint Central Administration v4	http://helsinkidc:12536/	12536
SharePoint - 80	http://sharepoint.finland.europe.sup/	80
SharePoint - Second 8279	http://sharepoint-second.finland.europe.sup:8279/	8279

Integration with Microsoft SharePoint

Configure the SharePoint Web Application

- Sharepoint wizard configure IIS automatically

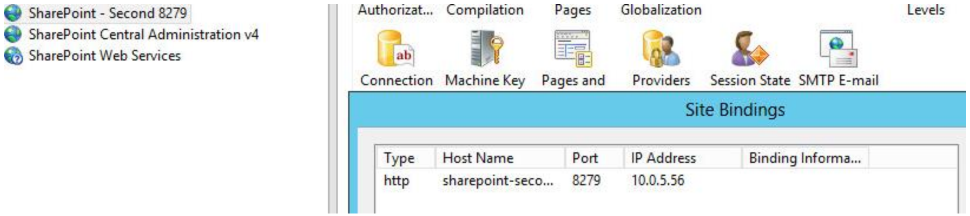


Application Pools
Sites
Default Web Site
SharePoint - 80
SharePoint - Second 8279
SharePoint Central Administration v4
SharePoint Web Services

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Enabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Enabled	HTTP 302 Login/Redi
Windows Authentication	Enabled	HTTP 401 Challenge

Enabled Providers:
Negotiate
NTLM

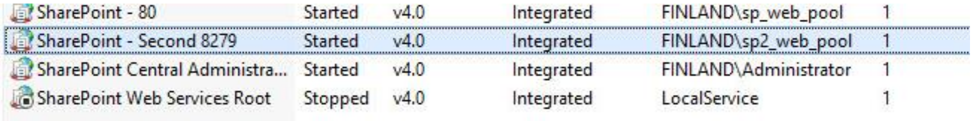
- Dedicated Web Site with specific authentication mechansim enabled (do not modify)



SharePoint - Second 8279
SharePoint Central Administration v4
SharePoint Web Services

Type	Host Name	Port	IP Address	Binding Informa...
http	sharepoint-seco...	8279	10.0.5.56	

- Dedicated Application Pool using user service account created

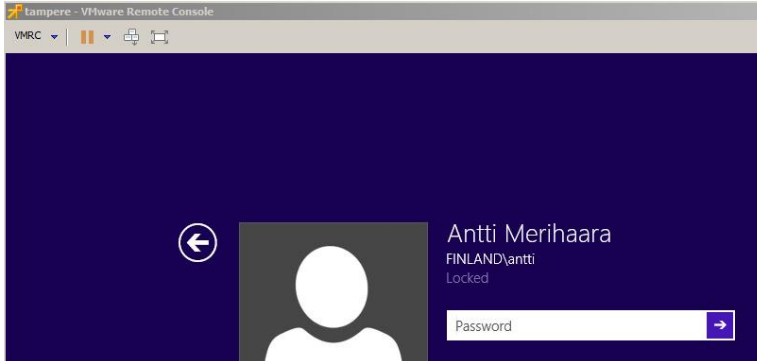


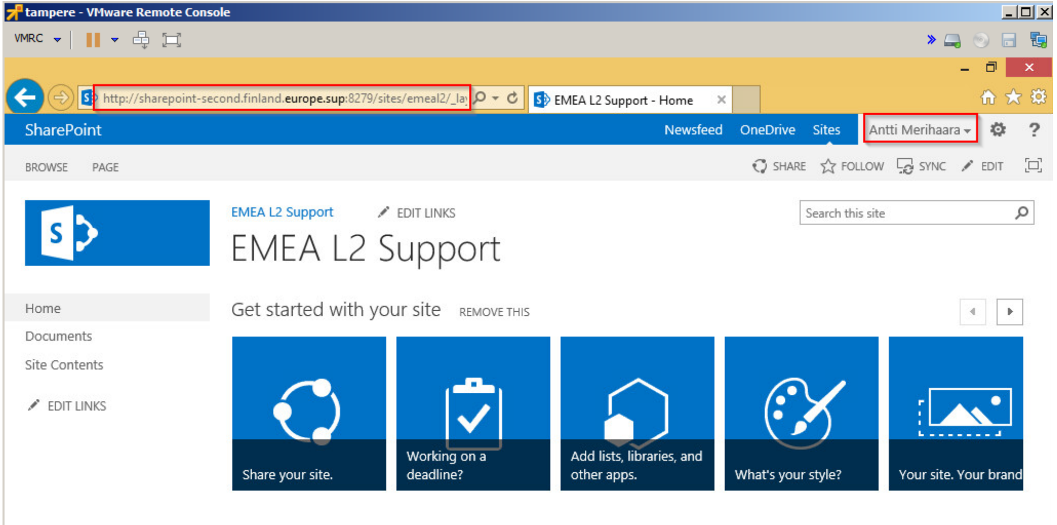
SharePoint - 80	Started	v4.0	Integrated	FINLAND\sp_web_pool	1
SharePoint - Second 8279	Started	v4.0	Integrated	FINLAND\sp2_web_pool	1
SharePoint Central Administra...	Started	v4.0	Integrated	FINLAND\Administrator	1
SharePoint Web Services Root	Stopped	v4.0	Integrated	LocalService	1

Integration with Microsoft SharePoint

Verify SharePoint Kerberos Authentication

- Verify Kerberos authentication
- Login with domain accout on workstation
- Connect to the Sharepoint web site with a kerberos enabled browser




http://sharepoint-second.finland.europe.sup:8279/sites/emeal2/_la

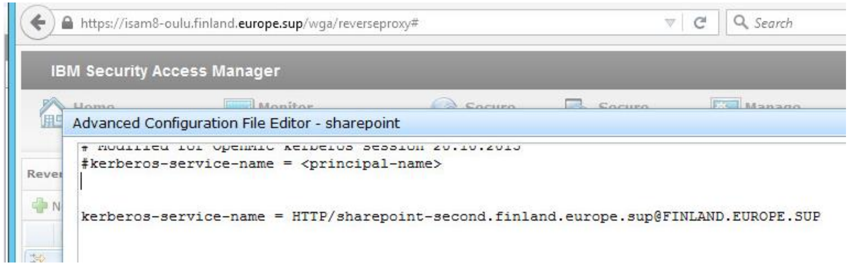
Integration with Microsoft SharePoint

Configure WebSeal and the junction on the Appliance

- Edit webseal conf file

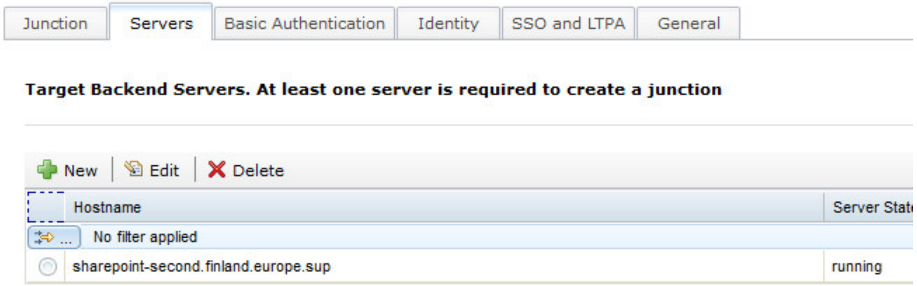
- Enable kerberos junction sso

    - Define keytab
    - Define kerberos service name
    - Define kerberos service principal


https://isam8-oulu.finland.europe.sup/wga/reverseproxy#
Search
IBM Security Access Manager
Advanced Configuration File Editor - sharepoint

```
#kerberos-service-name = <principal-name>


kerberos-service-name = HTTP/sharepoint-second.finland.europe.sup@FINLAND.EUROPE.SUP
```

- Create a junction */sharep-second* to SharePoint IIS web site



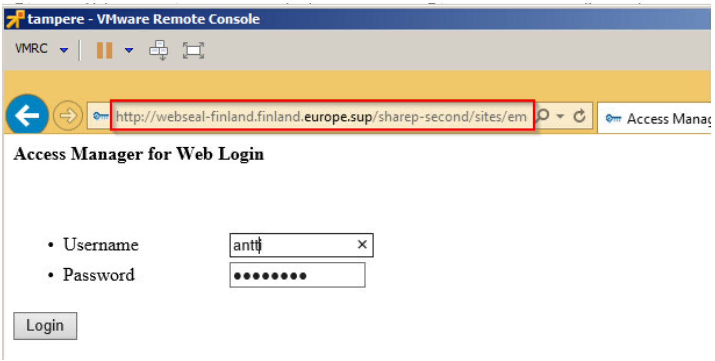
Target Backend Servers. At least one server is required to create a junction

	Hostname	Server Stat
	No filter applied	
○	sharepoint-second.finland.europe.sup	running

Integration with Microsoft SharePoint

Access SharePoint through the WebSeal Junction

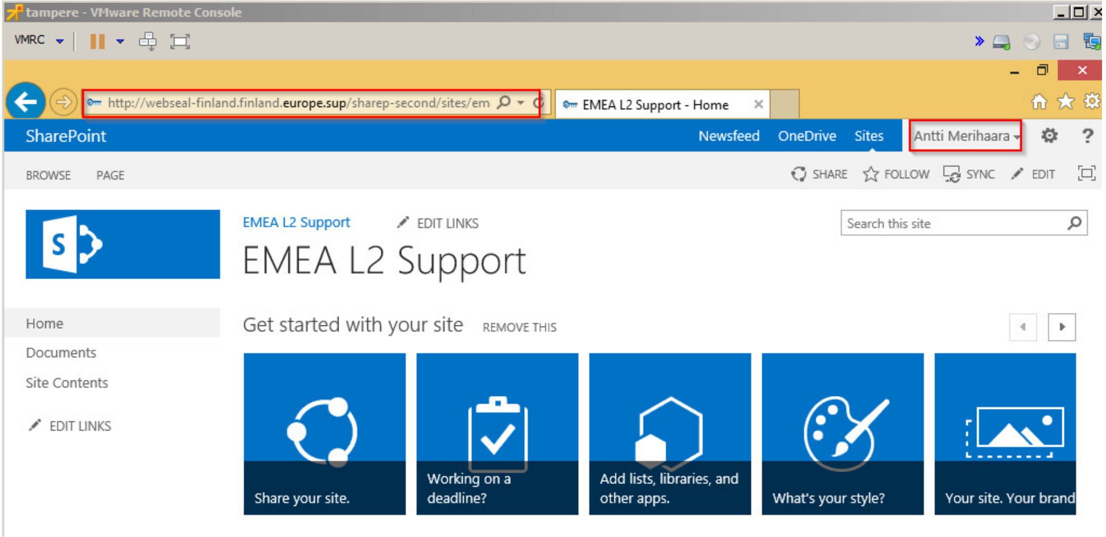
- Verify Kerberos junction
- Login on WebSeal using the configured auth mechanism
- Connect to the Sharepoint web site through the WebSeal junction



http://webseal-finland.finland.europe.sup/sharep-second/sites/em

Access Manager for Web Login

- Username antti
- Password ••••••••



http://webseal-finland.finland.europe.sup/sharep-second/sites/em

EMEA L2 Support

EMEA L2 Support

Get started with your site

Share your site.

Working on a deadline?

Add lists, libraries, and other apps.

What's your style?

Your site. Your brand

Questions ?

Questions for the panel?

Now is your opportunity to ask questions of our panelists.

To ask a question now:

Press *1 to ask a question over the phone

or

Type your question into the SmartCloud Meetings chat

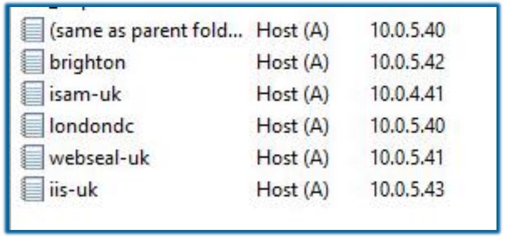
To ask a question after this presentation:

You are encouraged to participate in our Forum topics <link to IBM Security topic A in product X's Forum>.

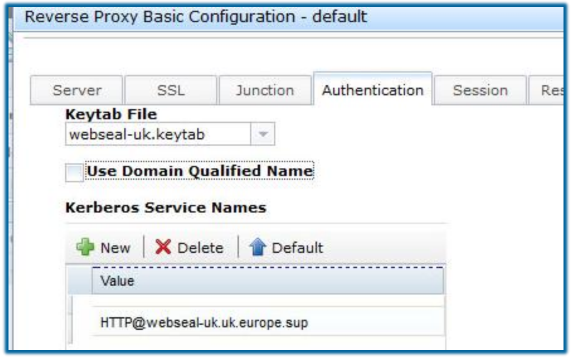
Extra Slides

Kerberos pass through

Enable Desktop SSO (see first open mic)



(same as parent fold...	Host (A)	10.0.5.40
brighton	Host (A)	10.0.5.42
isam-uk	Host (A)	10.0.4.41
londondc	Host (A)	10.0.5.40
webseal-uk	Host (A)	10.0.5.41
iis-uk	Host (A)	10.0.5.43



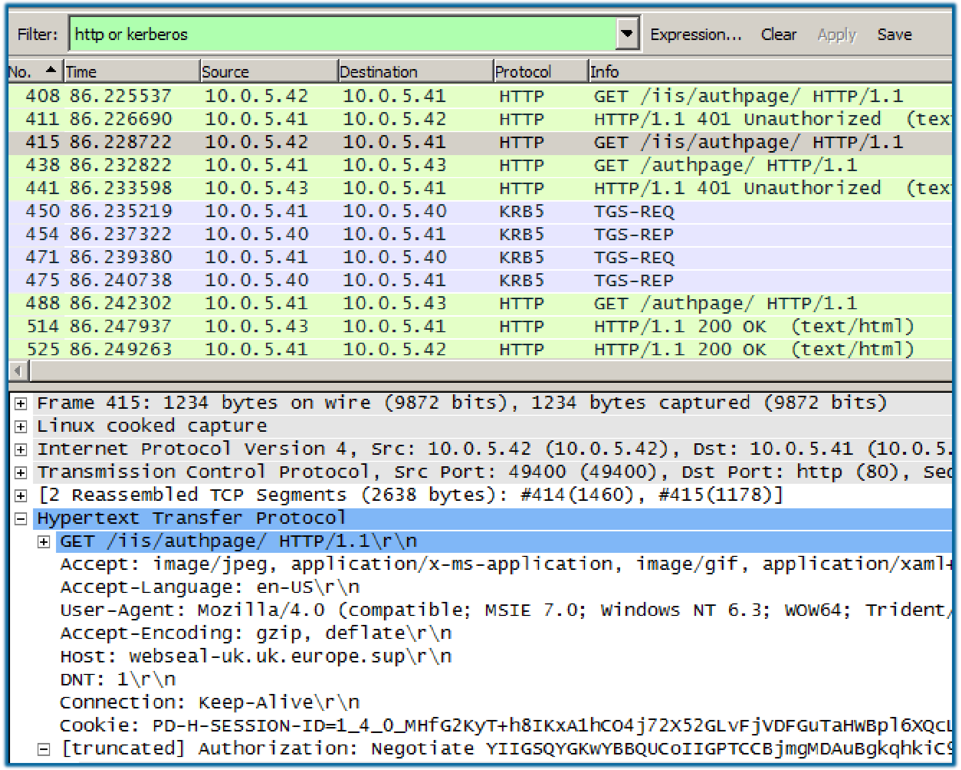
Reverse Proxy Basic Configuration - default

Keytab File: webseal-uk.keytab

☐ **Use Domain Qualified Name**

Kerberos Service Names

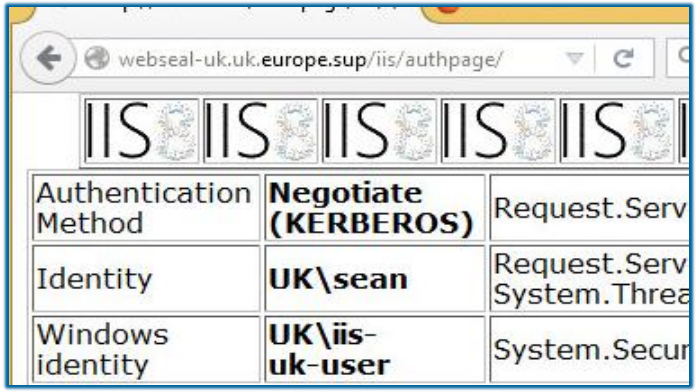
Value
HTTP@webseal-uk.uk.europe.sup



Filter: http or kerberos

```
No.  Time       Source     Destination Protocol Info
408 86.225537  10.0.5.42  10.0.5.41   HTTP     GET /iis/authpage/ HTTP/1.1
411 86.226690  10.0.5.41  10.0.5.42   HTTP     HTTP/1.1 401 Unauthorized  (tex
415 86.228722  10.0.5.42  10.0.5.41   HTTP     GET /iis/authpage/ HTTP/1.1
438 86.232822  10.0.5.41  10.0.5.43   HTTP     GET /authpage/ HTTP/1.1
441 86.233598  10.0.5.43  10.0.5.41   HTTP     HTTP/1.1 401 Unauthorized  (tex
450 86.235219  10.0.5.41  10.0.5.40   KRB5     TGS-REQ
454 86.237322  10.0.5.40  10.0.5.41   KRB5     TGS-REP
471 86.239380  10.0.5.41  10.0.5.40   KRB5     TGS-REQ
475 86.240738  10.0.5.40  10.0.5.41   KRB5     TGS-REP
488 86.242302  10.0.5.41  10.0.5.43   HTTP     GET /authpage/ HTTP/1.1
514 86.247937  10.0.5.43  10.0.5.41   HTTP     HTTP/1.1 200 OK  (text/html)
525 86.249263  10.0.5.41  10.0.5.42   HTTP     HTTP/1.1 200 OK  (text/html)
```

```
⊞ Frame 415: 1234 bytes on wire (9872 bits), 1234 bytes captured (9872 bits)
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: 10.0.5.42 (10.0.5.42), Dst: 10.0.5.41 (10.0.5.
⊞ Transmission Control Protocol, Src Port: 49400 (49400), Dst Port: http (80), Sec
⊞ [2 Reassembled TCP Segments (2638 bytes): #414(1460), #415(1178)]
⊟ Hypertext Transfer Protocol
  ⊞ GET /iis/authpage/ HTTP/1.1\r\n
    Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.3; WOW64; Trident/
    Accept-Encoding: gzip, deflate\r\n
    Host: webseal-uk.uk.europe.sup\r\n
    DNT: 1\r\n
    Connection: Keep-Alive\r\n
    Cookie: PD-H-SESSION-ID=1_4_0_MHfG2KyT+h8IKxA1hCO4j72X52GLvFjVDFGuTaHWBpl6XQc
  ⊟ [truncated] Authorization: Negotiate YIIGSQYGKwYBBQUCoIIGPTCCBjmgMDAuBgkqhkic
```

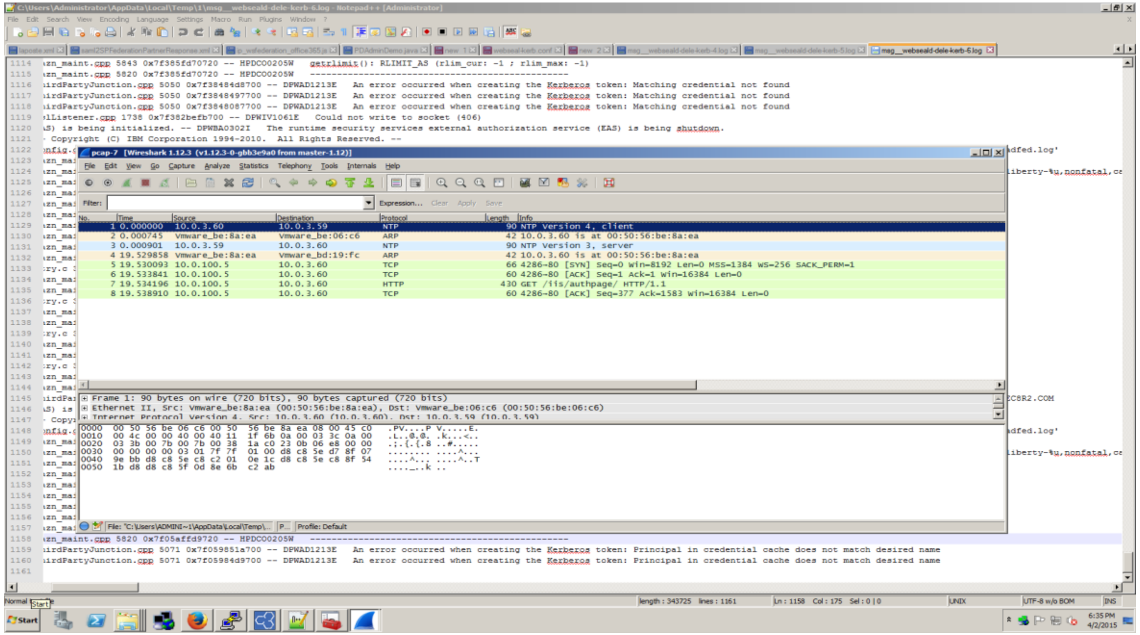


webseal-uk.uk.europe.sup/iis/authpage/

Authentication Method	Negotiate (KERBEROS)	Request.Serv
Identity	UK\sean	Request.Serv System.Threa
Windows identity	UK\iis-uk-user	System.Secur

Troubleshooting

Principal in credential cache does not match desired name



```
azn_maint.cpp 5843 0x7f385fd70720 -- HPDCO0205W   getrlimit(): RLIMIT_AS (rlim_cur: -1 ; rlim_max: -1)
azn_maint.cpp 5820 0x7f385fd70720 -- HPDCO0205W   ----------------------------------------------
irdPartyJunction.cpp 5050 0x7f38484d8700 -- DPWAD1213E   An error occurred when creating the Kerberos token: Matching credential not found
irdPartyJunction.cpp 5050 0x7f3848497700 -- DPWAD1213E   An error occurred when creating the Kerberos token: Matching credential not found
irdPartyJunction.cpp 5050 0x7f3848087700 -- DPWAD1213E   An error occurred when creating the Kerberos token: Matching credential not found
lListener.cpp 1738 0x7f382befb700 -- DPWIV1061E   Could not write to socket (406)
AS) is being initialized. -- DPWBA0302I   The runtime security services external authorization service (EAS) is being shutdown.
- Copyright (C) IBM Corporation 1994-2010.  All Rights Reserved. --
```

```
No.  Time        Source             Destination        Protocol  Length  Info
  1  0.000000    10.0.3.60          10.0.3.59          NTP           90  NTP Version 4, client
  2  0.000745    Vmware_be:8a:ea    Vmware_be:06:c6    ARP           42  10.0.3.60 is at 00:50:56:be:8a:ea
  3  0.000901    10.0.3.59          10.0.3.60          NTP           90  NTP Version 3, server
  4  19.529858   Vmware_be:8a:ea    Vmware_bd:19:fc    ARP           42  10.0.3.60 is at 00:50:56:be:8a:ea
  5  19.530093   10.0.100.5         10.0.3.60          TCP           66  4286→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1384 WS=256 SACK_PERM=1
  6  19.533841   10.0.100.5         10.0.3.60          TCP           60  4286→80 [ACK] Seq=1 Ack=1 Win=16384 Len=0
  7  19.534196   10.0.100.5         10.0.3.60          HTTP         430  GET /iis/authpage/ HTTP/1.1
  8  19.538910   10.0.100.5         10.0.3.60          TCP           60  4286→80 [ACK] Seq=377 Ack=1583 Win=16384 Len=0
```

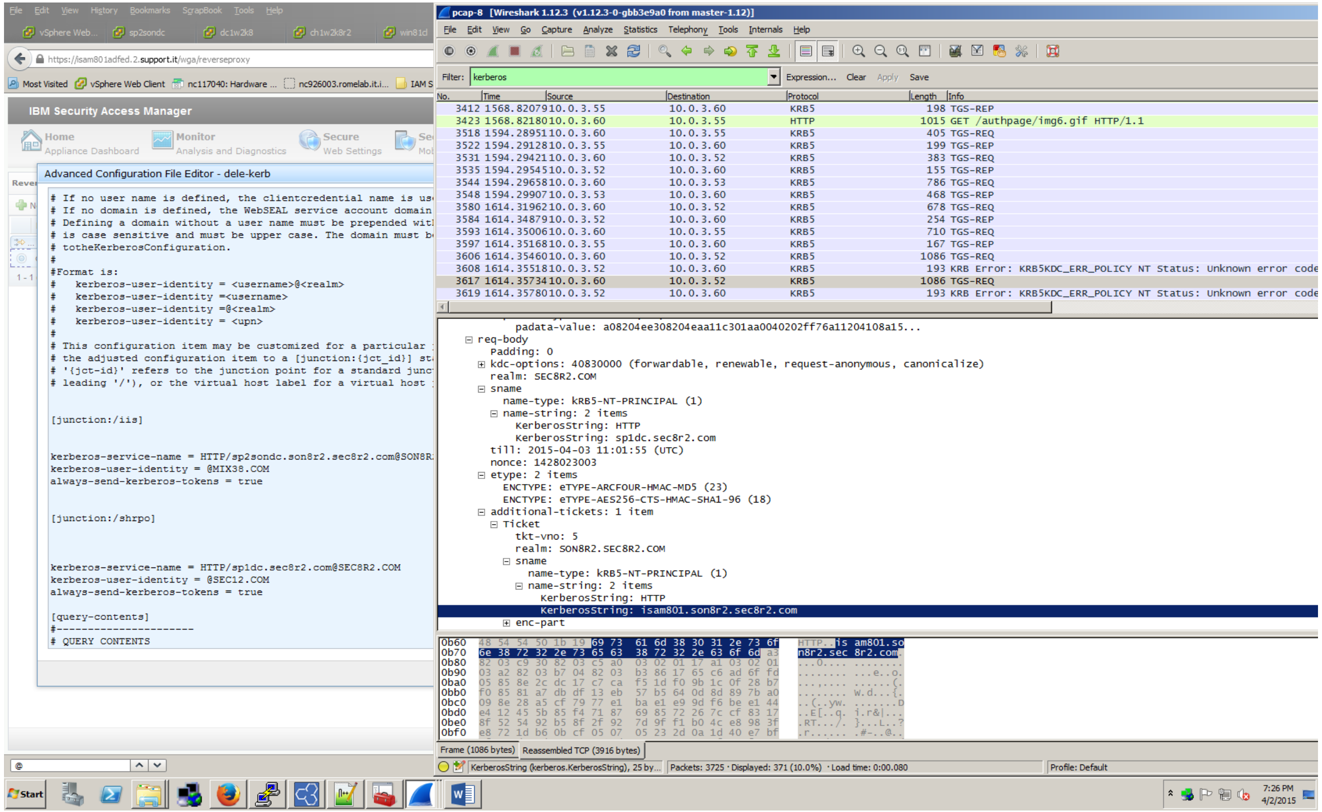
```
Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Vmware_be:8a:ea (00:50:56:be:8a:ea), Dst: Vmware_be:06:c6 (00:50:56:be:06:c6)
Internet Protocol Version 4, Src: 10.0.3.60 (10.0.3.60), Dst: 10.0.3.59 (10.0.3.59)

0000  00 50 56 be 06 c6 00 50  56 be 8a ea 08 00 45 c0   .PV....P V.....E.
0010  00 4c 00 00 40 00 40 11  1f 6b 0a 00 03 3c 0a 00   .L..@.@. .k...<..
0020  03 3b 00 7b 00 7b 00 38  1a c0 23 0b 06 e8 00 00   .;.{.{.8 ..#.....
0030  00 00 00 00 03 01 7f 7f  01 00 d8 c8 5e d7 8f 07   ........ ....^...
0040  9e bb d8 c8 5e c8 c2 01  0e 1c d8 c8 5e c8 8f 54   ....^... ....^..T
0050  1b d8 d8 c8 5f 0d 8e 6b  c2 ab                     ...._..k ..
```

```
azn_maint.cpp 5820 0x7f05affd9720 -- HPDCO0205W   ----------------------------------------------
irdPartyJunction.cpp 5071 0x7f059851a700 -- DPWAD1213E   An error occurred when creating the Kerberos token: Principal in credential cache does not match desired name
irdPartyJunction.cpp 5071 0x7f05984d9700 -- DPWAD1213E   An error occurred when creating the Kerberos token: Principal in credential cache does not match desired name
```

TCP-IP trace confirm that there is even no attempt to get a ticket, the problem could be the usage of a wrong kerberos-principal-name for that junction

Troubleshooting

KDC policy rejects request



File Edit View History Bookmarks ScrapBook Tools Help
vSphere Web… sp2sondc dc1w2k8 ch1w2k8r2 win81d
https://isam801adfed.2.support.it/wga/reverseproxy
Most Visited vSphere Web Client nc117040: Hardware … nc926003.romelab.it.i… IAM S
IBM Security Access Manager
Home Appliance Dashboard
Monitor Analysis and Diagnostics
Secure Web Settings
Advanced Configuration File Editor - dele-kerb
pcap-8 [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression… Clear Apply Save
Frame (1086 bytes) Reassembled TCP (3916 bytes)
Profile: Default
Start
7:26 PM
4/2/2015

```
# If no user name is defined, the clientcredential name is us
# If no domain is defined, the WebSEAL service account domain
# Defining a domain without a user name must be prepended wit
# is case sensitive and must be upper case. The domain must b
# totheKerberosConfiguration.
#
#Format is:
#   kerberos-user-identity = <username>@<realm>
#   kerberos-user-identity =<username>
#   kerberos-user-identity =@<realm>
#   kerberos-user-identity = <upn>
#
# This configuration item may be customized for a particular
# the adjusted configuration item to a [junction:{jct_id}] st
# '{jct-id}' refers to the junction point for a standard junc
# leading '/'), or the virtual host label for a virtual host


[junction:/iis]


kerberos-service-name = HTTP/sp2sondc.son8r2.sec8r2.com@SON8R
kerberos-user-identity = @MIX38.COM
always-send-kerberos-tokens = true


[junction:/shrpo]



kerberos-service-name = HTTP/sp1dc.sec8r2.com@SEC8R2.COM
kerberos-user-identity = @SEC12.COM
always-send-kerberos-tokens = true

[query-contents]
#----------------------
# QUERY CONTENTS
```

Filter: kerberos

```
No.  Time           Source      Destination Protocol Length Info
3412 1568.8207910.0.3.55   10.0.3.60   KRB5      198 TGS-REP
3423 1568.8218010.0.3.60   10.0.3.55   HTTP     1015 GET /authpage/img6.gif HTTP/1.1
3518 1594.2895110.0.3.60   10.0.3.55   KRB5      405 TGS-REQ
3522 1594.2912810.0.3.55   10.0.3.60   KRB5      199 TGS-REP
3531 1594.2942110.0.3.60   10.0.3.52   KRB5      383 TGS-REQ
3535 1594.2954510.0.3.52   10.0.3.60   KRB5      155 TGS-REP
3544 1594.2965810.0.3.60   10.0.3.53   KRB5      786 TGS-REQ
3548 1594.2990710.0.3.53   10.0.3.60   KRB5      468 TGS-REP
3580 1614.3196210.0.3.60   10.0.3.52   KRB5      678 TGS-REQ
3584 1614.3487910.0.3.52   10.0.3.60   KRB5      254 TGS-REP
3593 1614.3500610.0.3.60   10.0.3.55   KRB5      710 TGS-REQ
3597 1614.3516810.0.3.55   10.0.3.60   KRB5      167 TGS-REP
3606 1614.3546010.0.3.60   10.0.3.52   KRB5     1086 TGS-REQ
3608 1614.3551810.0.3.52   10.0.3.60   KRB5      193 KRB Error: KRB5KDC_ERR_POLICY NT Status: Unknown error code
3617 1614.3573410.0.3.60   10.0.3.52   KRB5     1086 TGS-REQ
3619 1614.3578010.0.3.52   10.0.3.60   KRB5      193 KRB Error: KRB5KDC_ERR_POLICY NT Status: Unknown error code
```

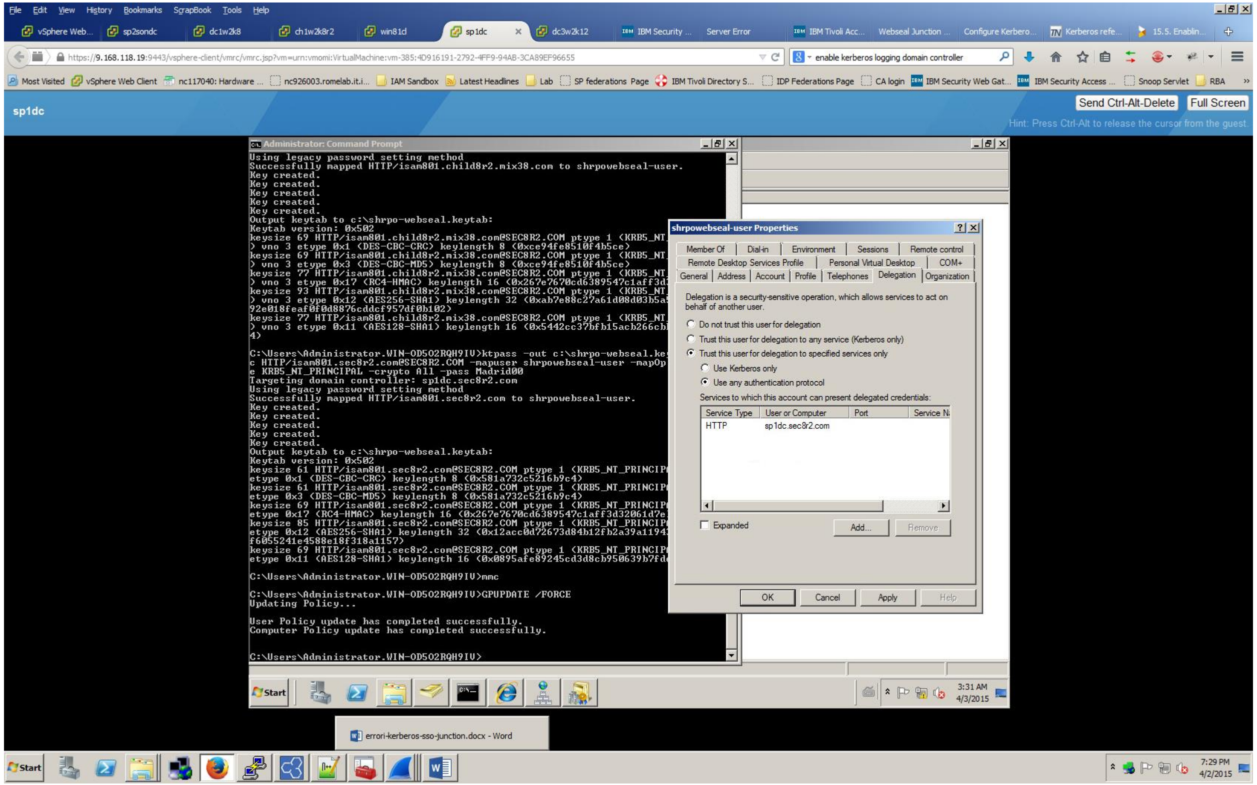
```
        padata-value: a08204ee308204eaa11c301aa0040202ff76a11204108a15...
  ⊟ req-body
      Padding: 0
    ⊞ kdc-options: 40830000 (forwardable, renewable, request-anonymous, canonicalize)
      realm: SEC8R2.COM
    ⊟ sname
        name-type: kRB5-NT-PRINCIPAL (1)
      ⊟ name-string: 2 items
          KerberosString: HTTP
          KerberosString: sp1dc.sec8r2.com
      till: 2015-04-03 11:01:55 (UTC)
      nonce: 1428023003
    ⊟ etype: 2 items
        ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
        ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
    ⊟ additional-tickets: 1 item
      ⊟ Ticket
          tkt-vno: 5
          realm: SON8R2.SEC8R2.COM
        ⊟ sname
            name-type: kRB5-NT-PRINCIPAL (1)
          ⊟ name-string: 2 items
              KerberosString: HTTP
              KerberosString: isam801.son8r2.sec8r2.com
        ⊞ enc-part
```

```
0b60  48 54 54 50 1b 19 69 73  61 6d 38 30 31 2e 73 6f   HTTP..is am801.so
0b70  6e 38 72 32 2e 73 65 63  38 72 32 2e 63 6f 6d a3   n8r2.sec 8r2.com.
0b80  82 03 c9 30 82 03 c5 a0  03 02 01 17 a1 03 02 01   ...0.... ........
0b90  03 a2 82 03 b7 04 82 03  b3 86 17 65 c6 ad 6f fd   ........ ...e..o.
0ba0  05 85 8e 2c dc 17 c7 ca  f5 1d f0 9b 1c 0f 28 b7   ...,.... ......(.
0bb0  f0 85 81 a7 db df 13 eb  57 b5 64 0d 8d 89 7b a0   ........ W.d...{.
0bc0  09 8e 28 a5 cf 79 77 e1  ba e1 e9 9d f6 be e1 44   ..(..yw. .......D
0bd0  e4 12 45 5b 85 f4 71 87  69 85 72 26 7c cf 83 17   ..E[..q. i.r&|...
0be0  8f 52 54 92 b5 8f 2f 92  7d 9f f1 b0 4c e8 98 3f   .RT.../. }...L..?
0bf0  e8 72 1d b6 0b cf 05 07  05 23 2d 0a 1d 40 e7 bf   .r...... .#-..@..
```

KerberosString (kerberos.KerberosString), 25 by… | Packets: 3725 · Displayed: 371 (10.0%) · Load time: 0:00.080

Troubleshooting

KDC policy rejects request (cont)


sp1dc
Send Ctrl-Alt-Delete
Full Screen
Administrator: Command Prompt
errori-kerberos-sso-junction.docx - Word

```
Using legacy password setting method
Successfully mapped HTTP/isam801.child8r2.mix38.com to shrpowebseal-user.
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to c:\shrpo-webseal.keytab:
Keytab version: 0x502
keysize 69 HTTP/isam801.child8r2.mix38.com@SEC8R2.COM ptype 1 (KRB5_NT
) vno 3 etype 0x1 (DES-CBC-CRC) keylength 8 (0xce94fe8510f4b5ce)
keysize 69 HTTP/isam801.child8r2.mix38.com@SEC8R2.COM ptype 1 (KRB5_NT
) vno 3 etype 0x3 (DES-CBC-MD5) keylength 8 (0xce94fe8510f4b5ce)
keysize 77 HTTP/isam801.child8r2.mix38.com@SEC8R2.COM ptype 1 (KRB5_NT
) vno 3 etype 0x17 (RC4-HMAC) keylength 16 (0x267e7670cd6389547c1aff3d
keysize 93 HTTP/isam801.child8r2.mix38.com@SEC8R2.COM ptype 1 (KRB5_NT
) vno 3 etype 0x12 (AES256-SHA1) keylength 32 (0xab7e88c27a61d08d03b5a
92e018feaf0f0d8876cddcf957df0b102)
keysize 77 HTTP/isam801.child8r2.mix38.com@SEC8R2.COM ptype 1 (KRB5_NT
) vno 3 etype 0x11 (AES128-SHA1) keylength 16 (0x5442cc37bfb15acb266cb
4)

C:\Users\Administrator.WIN-OD5O2RQH9IV>ktpass -out c:\shrpo-webseal.ke
c HTTP/isam801.sec8r2.com@SEC8R2.COM -mapuser shrpowebseal-user -mapOp
e KRB5_NT_PRINCIPAL -crypto All -pass Madrid00
Targeting domain controller: sp1dc.sec8r2.com
Using legacy password setting method
Successfully mapped HTTP/isam801.sec8r2.com to shrpowebseal-user.
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to c:\shrpo-webseal.keytab:
Keytab version: 0x502
keysize 61 HTTP/isam801.sec8r2.com@SEC8R2.COM ptype 1 (KRB5_NT_PRINCIP
etype 0x1 (DES-CBC-CRC) keylength 8 (0x581a732c5216b9c4)
keysize 61 HTTP/isam801.sec8r2.com@SEC8R2.COM ptype 1 (KRB5_NT_PRINCIP
etype 0x3 (DES-CBC-MD5) keylength 8 (0x581a732c5216b9c4)
keysize 69 HTTP/isam801.sec8r2.com@SEC8R2.COM ptype 1 (KRB5_NT_PRINCIP
etype 0x17 (RC4-HMAC) keylength 16 (0x267e7670cd6389547c1aff3d32061d7e
keysize 85 HTTP/isam801.sec8r2.com@SEC8R2.COM ptype 1 (KRB5_NT_PRINCIP
etype 0x12 (AES256-SHA1) keylength 32 (0x12acc0d72673d84b12fb2a39a1194
f6055241e4588e18f318a1157)
keysize 69 HTTP/isam801.sec8r2.com@SEC8R2.COM ptype 1 (KRB5_NT_PRINCIP
etype 0x11 (AES128-SHA1) keylength 16 (0x0895afe89245cd3d8cb950639b7fd

C:\Users\Administrator.WIN-OD5O2RQH9IV>mmc

C:\Users\Administrator.WIN-OD5O2RQH9IV>GPUPDATE /FORCE
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.


C:\Users\Administrator.WIN-OD5O2RQH9IV>
```

shrpowebseal-user Properties

Member Of | Dial-in | Environment | Sessions | Remote control | Remote Desktop Services Profile | Personal Virtual Desktop | COM+ | General | Address | Account | Profile | Telephones | **Delegation** | Organization

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation
○ Trust this user for delegation to any service (Kerberos only)
● Trust this user for delegation to specified services only
  ○ Use Kerberos only
  ● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
HTTP	sp1dc.sec8r2.com		

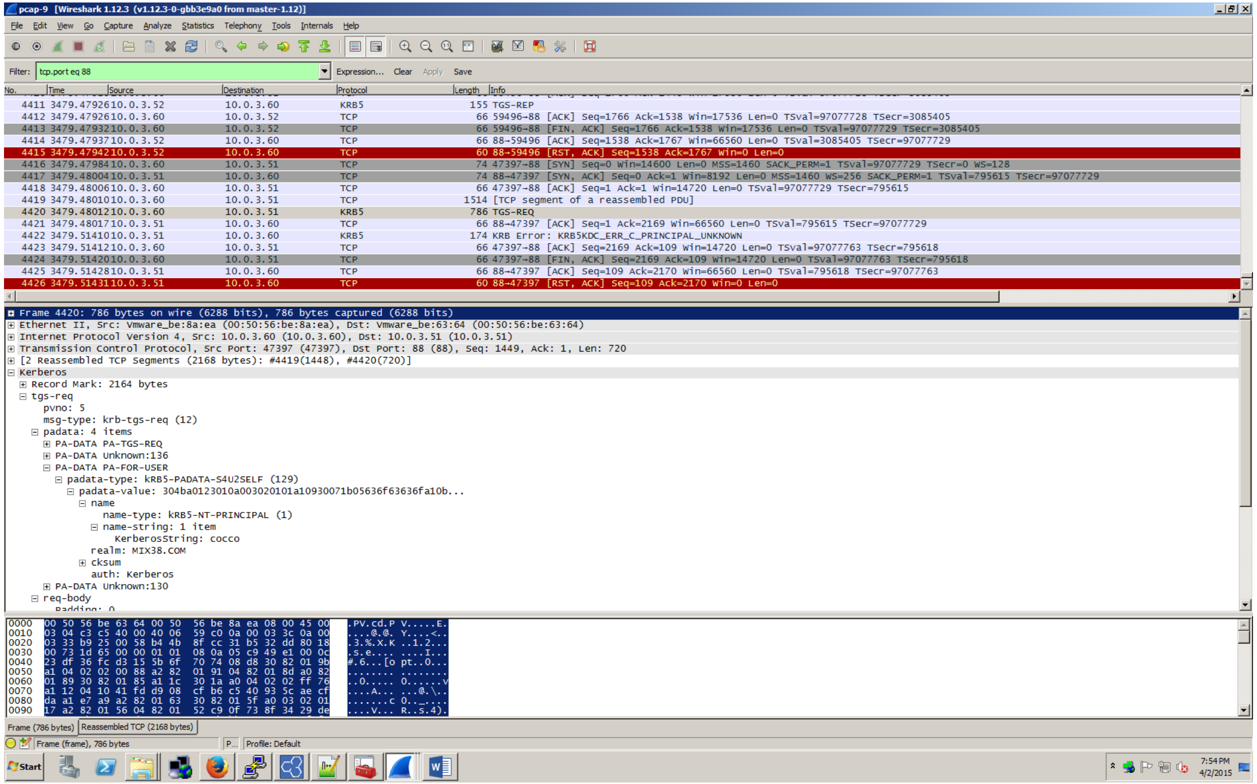
☐ Expanded

Add... | Remove | OK | Cancel | Apply | Help

The KDC that webseal uses is unable to find the SPN specified by webseal (in the tcp-ip trace isam801.son8r2.sec8r2.com) , this is a mismatch between what in webseal keytab (SPN of webSeal HTTP/Isam801.sec8r2.com) and what defined in the kerberos-service-name for the jucntion (this case in webseal conf file for /shrpo there is HTTP/ isam801.son8r2.sec8r2.com)

Troubleshooting

Client not found in Kerberos database



Filter: tcp.port eq 88

```
No.   Time      Source     Destination  Protocol  Length Info
 4411 3479.479210.0.3.52   10.0.3.60    KRB5       155 TGS-REP
 4412 3479.479210.0.3.60   10.0.3.52    TCP         66 59496→88 [ACK] Seq=1766 Ack=1538 Win=17536 Len=0 TSval=97077728 TSecr=3085405
 4413 3479.479310.0.3.60   10.0.3.52    TCP         66 59496→88 [FIN, ACK] Seq=1766 Ack=1538 Win=17536 Len=0 TSval=97077729 TSecr=3085405
 4414 3479.479310.0.3.52   10.0.3.60    TCP         66 88→59496 [ACK] Seq=1538 Ack=1767 Win=66560 Len=0 TSval=3085405 TSecr=97077729
 4415 3479.479410.0.3.52   10.0.3.60    TCP         60 88→59496 [RST, ACK] Seq=1538 Ack=1767 Win=0 Len=0
 4416 3479.479810.0.3.60   10.0.3.51    TCP         74 47397→88 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=97077729 TSecr=0 WS=128
 4417 3479.480010.0.3.51   10.0.3.60    TCP         74 88→47397 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=795615 TSecr=97077729
 4418 3479.480010.0.3.60   10.0.3.51    TCP         66 47397→88 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=97077729 TSecr=795615
 4419 3479.480110.0.3.60   10.0.3.51    TCP       1514 [TCP segment of a reassembled PDU]
 4420 3479.480110.0.3.60   10.0.3.51    KRB5       786 TGS-REQ
 4421 3479.480110.0.3.51   10.0.3.60    TCP         66 88→47397 [ACK] Seq=1 Ack=2169 Win=66560 Len=0 TSval=795615 TSecr=97077729
 4422 3479.514110.0.3.51   10.0.3.60    KRB5       174 KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
 4423 3479.514110.0.3.60   10.0.3.51    TCP         66 47397→88 [ACK] Seq=2169 Ack=109 Win=14720 Len=0 TSval=97077763 TSecr=795618
 4424 3479.514210.0.3.60   10.0.3.51    TCP         66 47397→88 [FIN, ACK] Seq=2169 Ack=109 Win=14720 Len=0 TSval=97077763 TSecr=795618
 4425 3479.514210.0.3.51   10.0.3.60    TCP         66 88→47397 [ACK] Seq=109 Ack=2170 Win=66560 Len=0 TSval=795618 TSecr=97077763
 4426 3479.514310.0.3.51   10.0.3.60    TCP         60 88→47397 [RST, ACK] Seq=109 Ack=2170 Win=0 Len=0
```

```
⊞ Frame 4420: 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits)
⊞ Ethernet II, Src: Vmware_be:8a:ea (00:50:56:be:8a:ea), Dst: Vmware_be:63:64 (00:50:56:be:63:64)
⊞ Internet Protocol Version 4, Src: 10.0.3.60 (10.0.3.60), Dst: 10.0.3.51 (10.0.3.51)
⊞ Transmission Control Protocol, Src Port: 47397 (47397), Dst Port: 88 (88), Seq: 1449, Ack: 1, Len: 720
⊞ [2 Reassembled TCP Segments (2168 bytes): #4419(1448), #4420(720)]
⊟ Kerberos
  ⊞ Record Mark: 2164 bytes
  ⊟ tgs-req
      pvno: 5
      msg-type: krb-tgs-req (12)
    ⊟ padata: 4 items
      ⊞ PA-DATA PA-TGS-REQ
      ⊞ PA-DATA Unknown:136
      ⊟ PA-DATA PA-FOR-USER
        ⊟ padata-type: kRB5-PADATA-S4U2SELF (129)
          ⊟ padata-value: 304ba0123010a003020101a10930071b05636f63636fa10b...
            ⊟ name
                name-type: kRB5-NT-PRINCIPAL (1)
              ⊟ name-string: 1 item
                  KerberosString: cocco
              realm: MIX38.COM
            ⊞ cksum
              auth: Kerberos
      ⊞ PA-DATA Unknown:130
    ⊟ req-body
        Padding: 0
```

```
0000  00 50 56 be 63 64 00 50  56 be 8a ea 08 00 45 00   .PV.cd.P V.....E.
0010  03 04 c3 c5 40 00 40 06  59 c0 0a 00 03 3c 0a 00   ....@.@. Y....<..
0020  03 33 b9 25 00 58 b4 4b  8f cc 31 b5 32 dd 80 18   .3.%.X.K ..1.2...
0030  00 73 1d 65 00 00 01 01  08 0a 05 c9 49 e1 00 0c   .s.e.... ....I...
0040  23 df 36 fc d3 15 5b 6f  70 74 08 d8 30 82 01 9b   #.6...[o pt..0...
0050  a1 04 02 02 00 88 a2 82  01 91 04 82 01 8d a0 82   ........ ........
0060  01 89 30 82 01 85 a1 1c  30 1a a0 04 02 02 ff 76   ..0..... 0......v
0070  a1 12 04 10 41 fd d9 08  cf b6 c5 40 93 5c ae cf   ....A... ...@.\..
0080  da a1 e7 a9 a2 82 01 63  30 82 01 5f a0 03 02 01   .......c 0.._....
0090  17 a2 82 01 56 04 82 01  52 c9 0f 73 8f 34 29 de   ....V... R..s.4).
```

Frame (786 bytes) | Reassembled TCP (2168 bytes)

Frame (frame), 786 bytes | P... | Profile: Default

The user that need to be impersonified (cocco) by WebSEAL is not found on the KDC this is a consequence of a wrong combination of logged-in user, the service to access (on the junction /iis) and rule used in kerberos-user-identity .

THANK YOU

www.ibm.com/security

IBM

IBM **Security**

Intelligence. Integration. Expertise.