Generate the Service Principal Name (SPN) and Keytab File

To set up the SPN and generate the keytab file, perform the following steps:

- 1. Log on to the active directory that uses the Kerberos Key Distribution Center (KDC).
- 2. For the user account in active directory, set the account to as "Password never expires" and "This account supports

test 1 Properties	? ×	
Member Of Dial-in Environment S Remote Desktop Services Profile Personal General Address Account Profile Telephone	essions Remote control Virtual Desktop COM+ s Delegation Organization	
User logon name: HTTP/qa31.idcad.com User logon name (pre- <u>W</u> indows 2000): IDCAD\ test	m 💌	
Logon Hours Log On <u>T</u> o	Account options:	
Unlock account Account options:	 Use Kerberos DES encryption types f This account supports Kerberos AES This account supports Kerberos AES Do not require Kerberos preauthentic 	for this account 128 bit encryption. 256 bit encryption. ation
 User cannot change password Password never expires Store password using reversible encryption Account is disabled 		Scroll down to view the "This account supports Kerberos AES 256 bit
 Account expires 	2013	encryption" option.
	Apple Links	
	Дрру нер	

3. Open the Windows Command prompt and run the following command to generate a keytab for the user account.

ktpass	-princ	HTTP/	[FQDN_LOWE	RCASE]@	[DOMA]	IN_1	JPPERCASE]	-mapus	ser	[USERNA	AME]	G
[DOMAIN	NAME] -	-pass	[PASSWORD]	-ptype	KRB5	NT	PRINCIPAL	-kvno	0 .	-crypto	AES2	256-
SHA1 -ou	ut [OUT]	PUT-FI	LENAME].ke	ytab								

Note: Execute this command in the Active Directory server

Here FQDN is the RiskVision Web Server Hostname

4. After the keytab file is generated, open the Windows Command Prompt, and run the following command to verify whether the SPN is registered for the hostname that a user will need for logging into RiskVision.



Administrator: Command Prompt C:\Users\Administrator>setspn -1 test Registered ServicePrincipalNames for CN=test 1,CN=Users,DC=idcad,DC=com: C:\Users\Administrator>ktpass /out http-ro.keytab /mapuser test@idcad.com /pass welcome@123 -ptype KRB5_NT_PRINCIPAL -kvno 0 /crypto AES256-SHA1 /princ HTTP/qa3 1.idcad.com@IDCAD.COM Targeting domain controller: dev163.idcad.com Using legacy password setting method Successfully mapped HTTP/qa31.idcad.com to test. Key created. Output keytab to http-ro.keytab: Keytab version: 0x502 keysize 80 HTTP/qa31.idcad.com@IDCAD.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x12 (AES256-SHA1) keylength 32 (0x40fe9350731009b1d714281be8f441cd3d08ab37f079 6a3064733cfec4321cdd) C:\Users\Administrator>setspn -1 test Registered ServicePrincipalNames for CN=test 1,CN=Users,DC=idcad,DC=com: HTTP/qa31.idcad.com C:\Users\Administrator>_

5. Copy the keytab file to a directory in the RiskVision Application Server to enable the Kerberos Authentication.