## Lumen<sup>®</sup> SD-WAN

## Versa SD-WAN AD Integration



## **General Disclaimer**

Although Lumen has attempted to provide accurate information in this guide, Lumen does not warrant or guarantee the accuracy of the information provided herein. Lumen may change the programs or products mentioned at any time without prior notice. Mention of non-Lumen products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

ALL INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS," WITH ALL FAULTS, AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED OR STATUTORY. LUMEN AND ITS SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES RELATED TO THIS GUIDE AND THE INFORMATION CONTAINED HEREIN, WHETHER EXPRESSED OR IMPLIED OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

LUMEN AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES, COSTS OF REPLACEMENT GOODS OR SERVICES, LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF THE GUIDE OR ANY LUMEN PRODUCT OR SERVICE, OR DAMAGES RESULTING FROM USE OF OR RELIANCE ON THE INFORMATION PROVIDED IN THIS GUIDE, EVEN IF LUMEN OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and other information used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Many of the Lumen products and services identified in this guide are provided with, and subject to, written software licenses and limited warranties. Those licenses and warranties provide the purchasers of those products with certain rights. Nothing in this guide shall be deemed to expand, alter, or modify any warranty or license or any other agreement provided by Lumen with any Lumen product, or to create any new or additional warranties or licenses.

## **Overview**

This document provides an overview of the steps a customer will need to perform in support of User and Group Authentication (Active Directory integration) into the Lumen SD-WAN customer's network. To activate and integrate User and Group Authentication (AD Directory), the customer will be required to assist with some steps in the deployment process. This document will give an overview of the Lumen Operations team's role and a detailed list of the customer steps necessary to integrate with the customer's AD environment.

### Summary

Customers need to be able to authenticate a user from an Active Directory server and authorize that authenticated identity to a Next Generation Firewall (NGFW) rule. This is also known as an Identity Based Policy (IBP). This is to allow or deny traffic or access to, any web destinations based on that user identity. Those destination sites, or group of sites (or categories), can be referred to as objects. The User Identity must be applied to a NGFW policy to make the decision to allow or deny access to the destination object. The user is defined as an individual, or as a member of a group.

- The Lumen SD-WAN (with Versa Networks) platform requires a web browser to attain the users identity to then build a table for acting upon a defined traffic flow.
- Requested Service Template deployment methodology is a method to allow the general template to be deployed first, to bring the device online with company defined standard configuration. The Service Template can then be used to deploy AD integration configuration.

### **Design Overview**

The Lumen SD-WAN platform supports two authentication methodologies in the currently deployed software version; LDAP, and Kerberos. Customers must support one of these two methods to identify the user and the IP address of the device they are using. LDAP is a **manual** method for identity verification with a web browser and Kerberos is considered the **silent** method.

The SD-WAN platform supports a manual (Captive Portal) authentication method using LDAP. This means that when traffic hits the policy that's destined for a website AND your identity is unknown, the browser session is redirected to a web page prompting for the manual entry of the user's credentials in the form of a fully qualified username (joe@mycompany.com) and a password. Those credentials are then passed, via the SD-WAN software, to an Active Directory server for authentication and group membership checks.

The SD-WAN platform also supports a silent (Kerberos) method. This is again using the web browser to identify the user via a Kerberos process in the background. This is referred to as silent, because the customer is not directly entering user credentials. Upon a web request, the SD-WAN software redirects a web request passing an unknown user request with a 401 or 407 "WWW-Authenticate/Proxy-Authenticate" header with value "negotiate". This will cause the browser to interact via Kerberos protocol and a configured keytab file, to validate the user's credentials and relay that info to the SD-WAN device for processing against the policy.

Notes:

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.

- The most important point is that all SD-WAN platform identity options require an interaction with the AD server using a web browser (HTTP/HTTPS), to provide that specific identity, to then be applied in the active NGFW policy. If the customer is trying to enforce a non-web-based protocol, it will be denied by default, until a web-based identification has occurred to establish the platforms User-to-IP mapping, which is loaded into the SD-WAN user database. You CAN allow non-HTTP/HTTPS protocols to be allowed out without user identity being known.
- There is an inactivity timer (which is configurable), and once reached (timer expires), the SD-WAN will remove the User-to-IP mapping from the database. Once removed, any new traffic will start the identification method again before allowing traffic to pass. This timer is recommended to be set to the minimum (which is 1 minute). This is to force re-authentication more often, to avoid a user change allowing the new user to inherit the previous users privilege level. Customer can work with Lumen TDE on the timer value that best fits their business need.
- Also note that if a user change occurs on a local PC or device (or possibly the IP is assigned to a different user/PC/device), there is a possible race condition where the IP being used is stilled registered in the SD-WAN User-to-IP mapping database, and the new user's traffic will assume the user privilege level of the prior user. This relationship (User-to-IP) will be maintained in the SD-WAN, based on the inactivity timeout not having occurred before the second user starts sending traffic through the SD-WAN device (which then resets the timer).
- NOTE: The Silent method using Kerberos is the Lumen recommended method based on the ease of user interaction, being no direct interaction.
- The certificate requirement is based on the platform. The recommendation is to use a single, PKI root signed certificate and password protected private key.

## **Summary of Responsibilities**

### **Customer Steps Summary**

- 1. Customer will provide Lumen TDE team representative the necessary information listed below for the customer's AD environment.
- 2. Customer will need access to the Lumen SD-WAN portal and be required to upload 3 file types: Keytab file, Key File, and Certificate. Detailed steps are provided below.
- 3. Customer will need to decide to use the **Lumen preferred method using Kerberos** or the alternative LDAP option for authentication.
- 4. See Appendix for Key Generation References.

# AD information Lumen TDE (Technical Design Engineer) will require from the customer

**NOTE:** This setup is necessary to get users/groups from the AD server so SDWAN policies can be configured using the users/groups functionality.

- Bind DN = Full distinguished name of admin user and location in directory tree
- Bind PW = LDAP admin password used for bind
- Domain Name = customer domain name
- Base DN = Location of users in directory tree
- LDAP/AD Server IP Address
- FQDN (Optional)

Example Screen Shots for reference:

Beneratedit       Implemente dierri Grand mette         Implemente die Grand die Grand mette         Implemente die Grand di		Monitor C								
Control Configuration	tbeltz-test-wrkflw		×1						> dsanford > 1	
Overlag       Image: Second Seco	0 0 8									
Greensen Services for and a service for a service to service the service of the	Objects >									
Normal Participant       Marine	Connectors 🗸									
AltA       Image: Alta Alta Alta Alta Alta Alta Alta Alta	A Reporting				(est-	Edit I DAR Somer	Brofile		0.96 354	Ding Di
Areaus Napus      Areaus	SNMP					Edit Serve	rionie	_	×	
Versen Skyler      Versen S	The Kerberos Profile					Name				
Used backson         Back backson	Kerberos Keytab					Descr Name*				
Use all assest       Image all assest         Start biologie       Image all assest						IP Address	5*			
MAINTERSTER Market	External Database					Tags 192.168.1	10.10			
	SAML Profile					Port*				
	Certificate Manager					Active Routing In	stance			
Image: Server Stoce         Shalk of the Stoce	<ul> <li>High Availability</li> </ul>					Bind C dsanford	-LAN-VR			Bind Timeout*
Address Router     Address     Addres						ENE FODN				30
Contracts     Configuration     Workflows     Administration     Analytics     Configuration     Workflows     Administration     Analytics     Configuration     Workflows     Administration     Analytics     Configuration     Workflows     Administration     Analytics     Configuration     Configuratin     Configuration     Configuration     Configuration     Conf						mss-t	est.net		st,DC=net	30
Image: Sever Type:       State         Image: Sever Type						Use S		Control		CA Certificate
Sever Subsection     Seve						En		Lante		
Monitor       Configuration       Workflows       Administration       Analytics         Monitor       Configuration       Workflows       Administration       Analytics         Construct       Configuration       Vorkflows       Administration       Analytics         Construct       Configuration       Configuration       Configuration       Configuration         State       Configuration       Configuration       Configuration       Configuration       Configuration         Users (Frougs)       State       Configuration       Configura						Servers				
Monitor Configuration Workflows Administration Analytics Monitor Configuration Workflows Administration Analytics Configuration © Organization: granization: Granter  Monitor Configuration User / Group Profile Conectors Reporting Kenteros Royals Users / Group Edit LDAP-Server Profile User / Group Profile Edit LDAP-Server Profile User / Group Profile Edit LDAP-Server Pro						102 168 1/	110 rast	40	390	dramford A
Monitor       Configuration       Workflows       Administration       Analytics         Image: Struct restruction       Organization: Granterd       Configuration:								~	203	03811010-0-0-0
Monitor       Configuration       Workflows       Administration       Analytics         Image: Description       Organization       Gantord       Configuration       Configurat										
Monitor         Configuration         Workflows         Administration         Analytics           Image: Configuration										
Monitor       Configuration       Workflows       Administration       Analytics         Image: Configuration       Organization:       Generation:       Configuration:       Image: Configuration:       Ima										
Monitor       Configuration       Workflows       Administration       Analytics         Image: Destablished Standard       Configuration       Orgenization:       Standard       Configuration       Configuration         Object: Destablished Standard       Configuration										
Monitor       Configuration       Workflows       Administration       Analytics         Image: Configuration       Organization:       Granitation:       Configuration:       Image: Configuratin:       Ima										
Monitor       Configuration       Workflows       Administration       Analytics         Monitor       Centiguration       © real-seteworther       © real-seteworther       © real-seteworther       © real-seteworther       © real-seteworther       © configuration > e         Concords       State       © seteworther       © seteworther       © configuration > e         Concords       State       © seteworther       © seteworther       © seteworther       © configuration > e         State       © seteworther       Seteworther       © seteworther       © seteworther       © configuration > e         Users / foroups       © seteworther       Seteworther       Seteworther       © seteworther       © seteworther         © local Database       Exercision Seteworther       © seteworthe							_	_	_	
Monitor       Configuration       Workflows       Administration       Analytics         Intervestwarthr       Organization       Organization       Configuration          Organization       Description       Configuration        Configuration          Organization       Configuration       Configuration        Configuration           Organization       Configuration       Configuration        Configuration           Organization       Configuration       Configuration       Configuration            Configuration       Configuration       Configuration       Same             State       Configuration       Configuration       Same       Same             State       Configuration       Configurat									_	OK
Interference       Organization: disarterd       Configuration: e         Objects       Output       Output       Configuration: disarterd       Configuration: e         Objects       Output       Save       Former       Save       Configuration: e										OK
CAP Server Profile User / Group Profile      Contextors      Reporting      Kenters Keyze      Contextors      State      Contextors      State      Contextors      State      Contextors      Contextor	an travel	Monitor	Configur	ration Wo	'kflows	Administratio	on Analyt	ics		DK
Operation     Connectors       Reporting     Sarath       Reporting     Sarath       Sarath     Sarath       Mame     Server Type       Edit LDAP Server Profile     X       Marei     Server Type       Kerbers Norline     X       Kerbers Nathanse     Server Type       Centificate Manager     Tagi       Centificate Manager     Sarate       Might Availability     Sarate       Intervent States     Sarate       Centificate Manager     Sarate       Centificate Manager     Sarate       Civel/Dapademin(N=Uperp.DC-mss)     Sarate       Mode     College DN       Servers     Sarate Timeout*       Display     Civel/Dapademin(N=Uperp.DC-mss)       Servers     Sarate Timeout*       Display     Sarate Timeout*       Display     Sarate Timeout*       Display     Sarate Timeout*       Display     Sarate Timeout*       Servers     Sarate Timeout*       Servers     Sarate Timeout*       Sa	formo toeltz-test-wrkf	Monitor	Configur	ration Wor	'kflows zalion: dsanfo	Administratic	on Analyt	ics ~	Configurat	ok tion > c
Contextors Reporting Source So	Tormo tbeltz-test-wrkf	Monitor	Configur	ration Wor	kflows zation: dsanfo	Administratic	on Analyt	ics V	Configurat	OX tion > c
Reporting     Image: Same Space Sp	forma toetz-test-wrkf	Monitor W	Configui V	ration Wor Organi roup Profile	rkflows zation: dsanfo	Administratio	on Analyt	ics V	Configurat	ok tion > c
SMR     Constants       Exception Stratule     Constants       Exception Stratule     Constants       Exception Stratule     Constants       Contracte Manager     Reprint Orable       Bind DN     Contracte Manager       Bind Stratule     Sauk Protectory       Contracte Manager     Bind Stratule       Bind Stratule     Sauk Protectory       Contracte Manager     Bind Stratule       Bind Stratule     Sauk Protectory       Cheldsaddmin, Cheldset, DCemes     Bind Timeout*       Sauk Protectory     Cheldsaddmin, Cheldset, DCemes       Bind Stratule     Sauk Protectory       Image: Sauk Protectory     Cheldsaddmin, Cheldset, DCemes       Sauk Protectory     Sauk Protectory       Sauk Protectory     Sauk Protectory       Image: Sauk Protectory     Sauk Protectory       Sauk Protectory     Sauk Protectory       Sauk Protectory     Sauk Protectory       Sauk Protectory     Sauk Protectory       Image: Sauk Protectory     Sauk Protectory <td< td=""><td>formo toelt2-test-wrkf</td><td>Monitor w LDAP Server Pro</td><td>Configui V</td><td>ration Wor Organi roup Profile</td><td>'kflows zation: dsanfo</td><td>Administratic</td><td>on Analyt</td><td>ics V</td><td>Configurat</td><td>tion &gt; c</td></td<>	formo toelt2-test-wrkf	Monitor w LDAP Server Pro	Configui V	ration Wor Organi roup Profile	'kflows zation: dsanfo	Administratic	on Analyt	ics V	Configurat	tion > c
Versif Groups       Name*         Interess Findle       Description         Isoan Statuse       Esternal Database         Central Brackers       Save         Central Rankinger       Tigs         Tigs       Save         Central Brackers       Save         Bind Finecut*       Bind Finecut*         Cleidagadmit/N=Users/DEvers       Save         Cleidagadmit/N=Users/DEvers       Save         Servers       Save         Isoale       Disable         Isoale       Disable         Isoale       Disable         Isoale       Disable         Isoale       Disable         Servers       Cleidagadmit/N=Users/DEvers         Isoale       Disable         Isoale	forma toeirz-rest-wrkf Coljects Connectors Connectors	Monitor w LDAP Server Pro	Configui Ville User / Gr	ration Wor Organi roup Profile Server Ty	'kflows zation: dsanfo	Administratio rd Servers	on Analyt	lcs V State	Configurat	ox tion > c
Keberos Rorda     Keberos Rorda     Keberos Keyda     Cod Database     Cod Database     Server Type     S	formo toeirz-test-wrkf Objects Connectors Reporting SNMP	Monitor w LDAP Server Pro Q. Search Name Edir LDAP Se	Configui Mie User/Gr rver Profile	ration Woo Organi roup Profile Server Ty	rkflows zation: dsanfo	Administratio	on Analyt	ics State	Configurat	CK
Continue Manager      Central Database     Cen	forme theirs rest wind Copiess Connectors Reporting Stative Users / Groups	Monitor W LDAP Server Pro Search Name Name	Configur Sofile User / Gr	ration Wor Organi roup Profile Server Ty	rkflows zation: dsanfo	Administratio	on Analyt	ics V State	Configurat	CK
Load Dankare Load Dankare Save Type: Save Type: Save Type: Save Directory High Availability     Save Directory Bind Timeout: Domain Name: Bind Simeout: Domain Name: Bind Simeout: Domain Name: Bind Simeout: Save Actificate Save Actificate Save Directory Di	tome meitz-test-wind Coljets Reporting Skult Users / Groups Users / Groups Gij Kethers Profile	Monitor W LDAP Server Pro Search Name Edir LDAP Tome- tbeltz-LDAP	Configur	ration Wo Organi roup Profile Server Ty	rkflows zation: dsanfo pe	Administratio	on Analyt	ics V State State	Configurat	tion > c
Tag:     Tag:       Status     Status       Certricate Name     Status       High Availability     Directory       Directory     Directory       Directory <t< td=""><td>tomo toeltz-test-wind Coljects C Conectors C Reporting C StMAP User / Groups Kerberos Reytab</td><td>Monitor w LDAP Server Pro Search Name Edir LDAP Se Name Name</td><td>Configu ville User / Gr rver Profile test</td><td>ration Wor Organi coup Profile Server Ty</td><td>kflows zation: dsanfor pe</td><td>Administratic rd Servers</td><td>on Analyt</td><td>ics State</td><td>Configurat</td><td>ion &gt; d</td></t<>	tomo toeltz-test-wind Coljects C Conectors C Reporting C StMAP User / Groups Kerberos Reytab	Monitor w LDAP Server Pro Search Name Edir LDAP Se Name Name	Configu ville User / Gr rver Profile test	ration Wor Organi coup Profile Server Ty	kflows zation: dsanfor pe	Administratic rd Servers	on Analyt	ics State	Configurat	ion > d
SANL Profile     Cernfricase Manger High Availability     High Availability     Server Type     Save     Save     Save     Save     Save     Save     Save     Save     Bind Password*     Bind Password*     Bind Password*     Bind Password*     Soverh Timeoux*     Challers DC+mss-testDC+met     Soverh Timeoux*     Challers DC+mss-testDC+met     Soverh Timeoux*     Challers DC+mss-testDC+met     Soverh Timeoux*     Challers DC+mss-testDC+met     Soverh Timeoux*     Soverh Timeou	Conectors Conectors Copers Reporting SMAP Users / Groups Users / Groups Kerberos Profile Report of Come States - C	Monistor w DAP Server Pro Search Name Edir LDAP Se Name Barcharts Description	Configur Sine User / Gr rver Profile	ration Wor Organi roup Profile Server Ty	kflows zation: dsanfo	Administratic rd	on Analyt	ICS State	Configurat	ton > c
Centricase Manager     Austion Statution     Statution       High Availability     O Table © Datable     Bind Timeout*       Bind Timeout     O Table © Table © Statution     Bind Timeout*       Domain Name:     Bind Timeout*     Bind Timeout*       Domain Name:     O N=UsersDC+mss     Bind Timeout*       Domain Name:     O N=UsersDC+mss-setsDC+mss     Bind Timeout*       Domain Name:     O N=UsersDC+mss-setsDC+mss     Bind Timeout*       Domain Name:     O N=UsersDC+mss-setsDC+mss     Bind Timeout*       Use SL     O N=UsersDC+mss-setsDC+mss     Bind Timeout*       Use SL     O N=UsersDC+mss-setsD	Conecors     Conecors     Conecors     Conecors     Reporting     Switz     Kerberss Rytab     Col Database     External Database	Monitor w LDAP Server Pro Search Name Edit LDAPS Description Tags	Configur ville user / Gr rver Profile	ration Wo Organi roup Profile Server Ty	kflows zadon: dsanfo	Administratic rd Servers	on Analyz	JCS State	Configurat	tion > e
High Availability     Bind DN*:     Bind Password*     Bind Timeout*       Cheldapadmin_CN+Uper_DC+mis     Soverh Timeout*     Soverh Timeout*       Domain Name     Bind Password*     Bind Timeout*       Cheldapadmin_CN+Uper_DC+mis     Soverh Timeout*     Soverh Timeout*       Exact N     Soverh Timeout*     Soverh Timeout*       Servers     Domain Anne*     Cheldapadmin_CN+Uper_DC+mis     Sover       Ip Address     Name     Port     Sover       Ip Address     Name     Port     Sover       Ip 2,158.10.10     test-AD     389     disanford-LAN-VR	Connectors Connectors SAMAP Users / Groups Users / Groups Users / Groups Connectors SAMAP Local Database Eccal Database SAMAProfile	Monitor UDAP Server Pro Control Search Control Search Control Search Marmen Detro: CDAP Detro: CDAP D	Configur Onlie User / Gr rver Profile	ration Wor Organi Server Ty	kflows colon: dsanfor pe	Administratic rd Servers	on Analyt	State	Configurat	
CkHidapadmin,CNHUsers,DC+mss     30       Demain Name     Base DNH       Search Timeout*     0       mss-seast     CN-Users,DC+mss       Uhe SSL     SSL Mode       C Cardificate     C       Enable     Disable       Envers     Image: Comparison of the standard of the	Conectors Conectors Conectors Statup Statup Uters / Groups Uters / Groups	Monitor w LDAP Server Pro Server Pro Server Type Kanne 1 Tags Server Type Server Type	Configur Configur User / Gr rver Profile	ration Wor Organi Server Ty Server Ty	kflows zašion: dsanto pe	Administratic d	on Analyt	Jos V State	Configurat	
Demain Name     Bate DN     Search Timeout*       mastet     Chelbash DC+mastettDC+met     Solution       Use SSL     SSL, Mode     CA Centificate       © Enable     Diable     Diable       Servers     © Image     Image       IP Address     Name     Port       IS2_168.10.19     test-AD     389	Connectors Connectors Reporting Shafe Users / croups Users / croups Kerberos Krytab Escena Database Control Database Certificate Manager Certificate Manager Hign Availability	Monitor W LDAP Server Pro Kanne Katric LDAP Gescription Tags Server Type* Active Direct Bind Bind Bind	Configur Ville User / Gr rver Profile test	ration Woo Organi Coup Profile Server Ty State Bind Res Bind Res	k/flows cation: dsanfor pe e • Disable sword •	Administratic d Serveri	on Analyc	ICS State	Configurat	
Inss-test CN-Upers.DC-mss-test.DC-met 0 Ute SSL SSL Mode CA Certificate 0 Enable 0 Duable EARS Servers 0 III V Control CA Certificate 0 III Address Name Port Routing Instance III 192.158.10.19 test-AD 389 dtanford-LAN-VR		Monitor w LDAP Server Pro Name Edit LDAP Generation Registry Regis	Configu User / Gr rver Profile test	ration Work Organi Coup Profile Server Ty State O Enable Send Pas Comas	kflows zation: dsanfo pe e • Disable sword*	Administratic rd Servers	on Analyt : : ind Timeout*	ics State >	Configurat	
Use SSL Mode CA Certificate C Servers O Mathematical Cardinal Cardina Cardinal Cardinal Cardina Cardinal Cardi	Conectors Conectors Shamp Shamp Users / Groups Users / Groups Users / Groups Users / Groups Users / Groups Users / Database Coal Database Shamp Coal Database Shamp Coal Database Shamp Coal Database Shamp High Availability	Monitor w LDAP Server Pro Server Pro Server Type Hentrs-LDAP Server Ings Server Type Server Type Bind DNB Cov-Idapate Domain Narr	Configur onne User / Gr rver Profile test	ration Woorgan Organi oug Profile Server Ty Enable Email Band Para Email Band Para	e Disable sword *	Administratic rd Servers	on Analyt : : : : : : : : : : : : : : : : : : :	ics State	Configurat	
Servers	Conectors Conectors Conectors Sharp Sharp Users / croups Users / croups Users / croups Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Sharp Conectors Conectors Sharp Conectors Conectors Sharp Conectors Conectors Conectors Sharp Conectors Cone	Monitor w LDAP Server Pro C. Search Name Edit LDAP Se Name Edit LD	Configur User / Gr rver Profile test test tory	ration Woo Organi Cup Profile Server Ty Server Ty End Bas Band Bas Cents Base DM Base DM Creuting	kflows cason: dsanfo pe e • Disable sword •	Administratic rd Servers DC-net	on Analyn	State	Configurat	
IP Address Name Port Routing Instance     192_168.10.19 test-AD 389 dtanford-LAN-VR	Anne coelsxesserer Copers Copers Reporting SNAP Users / Coopers SNAP Users / Coopers Coopers SNAP Users / Coopers Coopers SNAP Coopers SNAP Coopers SNAP Coopers SNAP Coopers SNAP Coopers SNAP Coopers SNAP Coopers SNAP Coopers SNAP Coopers SNAP Coopers SNAP Coopers SNAP Coopers SNAP Coopers SNAP SNAP SNAP SNAP Coopers SNAP	Monitor w LDAP Server Pro Search Name Edit LDAPS Record Pro Record	Configure	ration Work Organi coup Profile Server Ty Cents Band Pata Band Pata Cents Cents Server State Cents Server State Cents Server State Cents Server State Cents Server State Cents Server State Server State State Server State Server State State Server State	kflows cation: dsanfor pe e • Disable sword •	Administratik rd Servers DC=net 6	on Analyt ind Timeout* 10 Search Timeout* 10 A Certificate <b>©</b>	State	Configurat	
192_168_10_10     test-AD     389     dsamford-LAN-VR		Monitor w LDAP Server Pro Server Pro Server Type Kenter ChAP Server Type Kenter ChAP Server Type Kenter Cher Chap Server Type Kenter Cher Cher Cher Cher Cher Chap Server Type Kenter Cher Cher Cher Cher Cher Cher Cher Ch	Configur vitie User/Gr rver Profile test tory hin_CN=Users.D e: Disable	ration Woorgan Organ oug Profile Server Ty Ease DN Caress Base DN Caress State Base DN Caress State Base DN	e  Disable sword sale a	Administratic co Servers	on Analyt ind Timeout* 10 earch Timeout* 10 6 (Certificate O (Certificate O (Certificate O)	ics State	Configurat	
	Conectors Conectors Sharp Sharp Sharp Users / croups Users / croups Users / croups Users / croups Users / croups Users / croups Elevens Reptao Elevens Reptao Elevens Autoritation Elevens Autoritation	Monitor w LDAP Server Pro Server Pro Server Pro Name Fort LDAP Se Name Fort LDAP Se Name Fort LDAP Se Server Type Server Type Server Type Got DN CN-Isapac Bind DN CN-Isapac B	Configur	ration Work Organi Server Ty Server Ty Enable Band Pas Cerves Band Pas Cerves Server Ty Cerves Band Pas Cerves Server Ty Cerves Server Serv	kflows zakion: disanto pe e Disable sword •	Administratic ra Servers DC=ret C	on Analyr ind Timeout* 10 A Certificate A Certificate C	scare	Configurat	
	Conectors Conectors Reporting SNAP Users / Cooptor Kerberos Profile Kerberos Profile Exema Database Statu, Profile Card Database SANL, Profile Card Database SANL, Profile	Monitor W LDAP Server Pro Rame Edit LDAP Edit LDAP Edit LDAP Description Tags Server Type Active Diret Bin Darian Nam rmss-tess Use SSL Servers Servers Pro	Configure	ration Work Organi Coup Profile Server Ty Cents Emild Pas Server Ty Cents Band Pas Server Ty Cents Band Pas Server Ty Cents Server Ty Server Ty Se	kflows catoon: dsanfor pe e Disable sword • • r, DC-mss-test e	Administratik rd Servers DC=net C DC=net C	on Analyt ind Timeout* 0 Search Timeout* 10 A Certificate Q Routing D	State State	Configurat	
		Monitor w LDAP Server Pro Search Edit LDAP Se Name Edit LDAP Server Type Server Type Bind DN4 Domain Nam mis-Seat Use SL Use SL Server Type Bind DN4 Domain Nam Tags Server Type Bind DN4 Domain Nam Server Type Bind DN4 Domain Nam	Configure vittle User / Gr rver Profile test test test bory Disable gress 66.10.10	Altion Wool Organi Coup Profile Server Ty Central Base DN Safe Central Base DN Safe Lister Safe Safe Safe Safe Safe Safe Safe Safe	e Disable sword * e PP 200-mst-test	Administratic o Servers DC=net C 2 7	on Analyt ind Timeout.* 10 exch Timeout.* 10 Excerticate Rouing I dsanford	ICS State State		
	Conectors Conectors Conectors ShMP Users / Conectors ShMP Users / Conectors Users / Conectors Users / Conectors Users / Conectors Users / Conectors Conectors Users / Conectors Conectors Conectors ShMP Conectors Users / Conectors Conecto	Monitor w LDAP Server Pro Server Pro Server Type Celescoption Tags Server Type Active Direct Bind DN Celescoption Tags Server Type Active Direct Bind DN Celescoption Tags Server Type Celescoption Tags Server Type Celescoption Tags Server Type Tags Description T	Configur virile User / Gr river Profile tess	ration Woo Organi coup Profile Server Ty Enable Cerras Bind Pati Cerras Bind Pati Cerras Bind Pati Cerras Bind Pati Cerras Bind Pati Cerras Bind Pati Cerras Bind Pati Cerras	e  pe	Administratic ra Servers DCenet C 9	on Analyr ind Timeout* 10 exch Timeout* 10 C Certificate 10 Roung Iu disanford	Ics State State		
	Conectors Conectors Reporting Number of Conectors Reporting Number of Conectors Number of Conectors Number of Conectors Number of Conectors Conectors Number of Conectors Conectors Conectors Number of Conectors Coneco	Monitor W LDAP Server Pro Name Name Edit LDAP Server Type Tags Description Tags Server Type: Active Direc Bind	Configure User / Gr rver Profile tesz toory nin_CN=Users_D isony Disable aress 58.10.10	ration Work oup Profile Server Ty Server Ty Server Ty Example Server Ty Example Serv	k/lows cation: dsanfor pe e Disable sword : - r, DC-mis-test e	Administratic d Servers DCenet C 9	on Analyt and Timeout* 10 Search Timeout* 10 A Certificate Q Houting II Routing II	ICS SEARE SEARE SEARE SEARCE LAN-VR	Configurat	
	Conectors Conectors Reporting SMMP Users / Groups Users / Groups Users / Groups Martines Profile Conectors Profile Conectors SMI Profile Conectors Econectors Conectors SMI Profile Conectors SMI Profile	Monitor W LDAP Server Pro Server Pro Server Pro Server Type Ent LDAP Server Type Server Type Active Direct Bind DN4 Construct Type Server Type End DN4 Construct Domain Nam mis-seat End DN4 Construct Server Type End Server	Configure vitile User / Gr river Profile test test test bory Disable gress 56.10.10	Action Woo Organi Coup Profile Server Ty O Enable Base DN Exame Issi-AD	e Disable sword * P P P P P B B B B B B B B B B B B B B	Administratic d Servera DC=net C 9	on Analyt ind Temeout* 10 exch Temeout* 10 exch Temeout* 10 exch Temeout* 10 exch Temeout*	State		

### Generate Kerberos Keytab (Customer Responsibility)

Create a Versa account in Active Directory for access to Kerberos.

Versa User1 Properties				?	$\times$			
Organization Me	mber Of	Dial-in	Environment	Sess	sions			
Remote control	Remote	Desktop Se	rvices Profile	CO	M+			
General Address	Account	Profile	Telephones	Delegation				
User logon name:								
versauser		@mssla	b.net		$\sim$			
User logon name (pre-	Windows 20	)00):						
MSSLAB\		versaus	er					
Logon Hours Unlock account Account options:	Log On	To at next logor	1		^			
User cannot cha	nge passwo expires using reversi	ord ible encryptio	n		~			
Account expires Never C End of: Wednesday, November 18, 2020								
OF	(	Cancel	Apply	He	lp			

It is recommended to generate a Kerberos Keytab file using a random Kerberos Password. See command examples below.

1

ktpass -princ HTTP/{DOMAIN\_USER.DOMAIN@DOMAIN} -mapuser {DOMAIN\_USER} +rndPass -mapOp set +DumpSalt crypto AES256-SHA1 -ptype KRB5\_NT\_PRINCIPAL -out {KEYTAB\_FILENAME}

#### Example using Crypto All (Most Compatible)

1

ktpass -princ HTTP/{DOMAIN\_USER.DOMAIN@DOMAIN} -mapuser {DOMAIN\_USER} -mapOp set -pass
{DOMAIN\_PASSWORD} -crypto all -ptype KRB5\_NT\_PRINCIPAL -out {KEYTAB\_FILENAME}

#### Additional Options:

1

ktpass -princ HTTP/{DOMAIN\_USER.DOMAIN@DOMAIN}-mapuser {DOMAIN\_USER} -crypto all -ptype
KRB5\_NT\_PRINCIPAL -pass {DOMAIN\_PASSWORD} -out {KEYTAB\_FILENAME}

#### Additional Example:

1

ktpass -princ HTTP/{DOMAIN\_USER.DOMAIN@DOMAIN} -mapuser {DOMAIN\_USER} -mapOp set -pass
{DOMAIN\_PASSWORD} -crypto all -ptype KRB5\_NT\_PRINCIPAL -out {KEYTAB\_FILENAME}

**NOTE:** the -pass option allows for a known password, which is considered risky, as the account can be used by others manually. Should consider using +rndPass which will reset the user account password to a random string, thus assuring it is ONLY used by Kerberos

**NOTE:** For detailed steps related to Keytab file generation on a Microsoft Windows system, please refer to these resources:

#### Vendor Documentation:

https://social.technet.microsoft.com/wiki/contents/articles/36470.kerberos-keytabs-explained.aspx https://blogs.technet.microsoft.com/pie/2018/01/03/all-you-need-to-know-about-keytab-files/ https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ktpass

### **DNS Configuration**

Create a Versa DNS entry in Active Directory to point the Virtual URL to a global DNS entry. In this example it is using the LAN interface of the Versa FlexVNF connected to the Domain Controller.

Bit of the Director (December 2017)       Bit of the Director (December 2017)       File       Action       View       Help       Image: Sector (December 2017)			-
<ul> <li>DNS</li> <li>AD-LABSERVER</li> <li>Forward Lookup Zones</li> <li>rmsdlab.net</li> <li>rmsslab.net</li> <li>Reverse Lookup Zones</li> <li>Trust Points</li> <li>Conditional Forwarders</li> </ul>	<ul> <li>Name         <ul> <li>sites</li> </ul> </li> <li>Versauser Properties</li> <li>Host (A) Security</li> <li>Host (uses parent dom         <ul> <li>versauser</li> </ul> </li> <li>Fully qualified domain reversauser</li> <li>Fully qualified domain reversauser.msslab.net</li> <li>IP address:         <ul> <li>10.10.20.1</li> <li>Update associated</li> </ul> </li> </ul>	Type ain if left blank): name (FQDN):	Data
		OK Cano	el Apply

### Upload of Private Key and Certificates (Customer Responsibility)

Customer will need to upload these 3 files into the Lumen SD-WAN Portal. These can be uploaded in the following sequence and all can be uploaded at the same timeframe. There is no need to wait on another step from Lumen engineering. Customer should notify their Lumen TDE (engineer) once ALL THREE of these files have been uploaded to the director.

**NOTE:** If the customer does not have proper access and credentials to the Lumen SD-WAN portal, please reach out to your TDE engineer to have an account created for the user that will be performing the actions below.

After logging into the SD-WAN portal, please make sure you are in the Director context. The easiest way to see this is based on the menus across the top. The Director context will show 5 menus as shown below. NOTE: The other context called the Appliance Context will only have 4 menus across the top.

LUMEN'							<b>1</b> 0		1	belchers $\checkmark$
	Monitor	Configuration	Workflows	Administration	Analytics					
						Configuration	ו > S/	ATLAB	> Dev	rices C
Search	Templates 👻 🛛	Devices 👻 Objects 👻								

#### Navigate to Configuration > Templates > Common Template

LUMEN						
	Monitor Cor	figuration	Norkflows	Administration	Analytics	
Search	Templates + Devices +	Objects +				
CenturyLink	Device Templates Service Templates					
- Å CAVS-IFT-BIIT-01 ↓ Å CTLLABS	Common Template	Mgmt, Address	Туре	Time Created	Service Start Ti	Software Vers
- A EMEA-TEST-ORG	DCX4-Controller-0	100.70.42.168	Controller	Tue, Dec 08 20	Tue, Dec 08 20.	20.2.2-GA
After selecting the Cc	ommon Template ([	DataStore), na	vigate to th	e	icon in th	e upper left

corner. It will be labeled "Objects and Connectors".

#### 1. Keytab File upload:

Navigate to Connectors > Users/Groups > Kerberos Keytab.

LUMEN	Monitor Configuration	Workflows Administration	Analytics		🔎 🗐   🛈 belchers 🗸
Home SATLAB-DataStore	× ]	Organization: SATLAB	Show from Common Template		C
* 😚 😪	Director Appliance				
S Objects	Q Search				
Connectors	File Name	Uploaded Time	Status	Size(bytes)	
Lisers / Groups	ad.satlab_Kerberos.keytab	Thu, Feb 13 2020, 01:00	Completed	407	
Chi Kerberos Profile	satlab-kerberos.keytab	Sat, Sep 19 2020, 14:08	Completed	372	
Kerberos Keytab					
LDAP					
Local Database					
External Database					
SAML Profile					
Authentication Pro					
Certificate Manager					

Select the upload icon <a>Image: Select the upload icon</a> on the upper right and browse for your ".keytab" file and click OK.

LUMEN	Monitor Configuration Workf	ows Administration Analytics		国 ① sbelcher-satlab(SATLAB)~ Commit Template
Home SATLAB-DataStore	↓ Organizati	n: SATLAB	Show from Common Template	Configuration $$ > SATLAB $$ > Common Template $$ $$ $$ $$ $$ $$ $$
Connectors	Director Appliance          Search         File Name         ad.satlab_Kerberos.keytab         satlab-kerberos.keytab	Upload Kerberos Keytab Files to Director File Name Sample keytab Note - Allowed file formats are keytab	K Browse OK Cancel	Sizelby(res) 407 372

This will save your ".keytab" file on the SD-WAN portal.

LUMEN'								[	]   (1)	sbelcher-satlab ( SATLAB ) 🗸
	N	Aonitor	Configuration	Workflows	Administration	Analytics				Commit Template
Home SATLAB-DataStore				Organization: SATI	AB	×	Show from Common Ter	mplate Configuration	> SATLAB	> Common Template C
* 😵	Direc	tor Applian	ce							
Solution Objects	Q	Search								▼   < 1 >   25 ∨
Q Connectors ∨		File Name		L	ploaded Time		Status	Size(bytes)		
Lin Reporting		ad.satlab_K	erberos.keytab	т	hu, Feb 13 2020, 01:00		Completed	407		
Kerberos Profile		satlab-kerb	eros.keytab	S	at, Sep 19 2020, 14:08		Completed	372		
Kerberos Keytab		sample.key	tab	V	/ed, Jan 20 2021, 18:08		Completed	30		
LDAP										
Local Database										
External Database										
SAML Profile										
Authentication Pro										

#### 2. Key file upload:

This process will be similar to the above with the exception of the starting point. You will need to navigate away from the Common Template and select an individual device. Hit "Home", go to Configuration > Devices > "Select a Device" > Objects and Connectors > Custom Objects > Keys

**NOTE:** At this point you have navigated away from the "Director Context" and into the "Appliance Context". To go back, you would hit the HOME button in the upper left.

Click the upload icon <a>Image</a> on the upper right of the screen.

Provide a name for the Key, browse for the ".key" file and click **OK**.

LUMEN'				🗐 🕕 sbelcher-satlab ( SATLAB	)~
	Monitor Analytics	Configuration Administration			
Home SATLAB-Chicago	∼ Org	anization: SATLAB		Build	C
条 🗘 😚 😵	Director Appliance				
🗘 Objects 🛛 🗸		Upload Key File to Director	×		
Address	In the second second				
😣 Address Groups	Rey Name	Key Name*		Date oploaded	
😣 Persistent Actions	[_] privkey.key	sampiekey		Thu, Feb 13 2020, 01:02	
Schedules		Key File Name*	Denue		
Cloud Profiles		sample.key	Browse		
Re-defined >					
🐔 Custom Objects 🛛 🗸			OK Cancel		
Applications					
Scanners					
🛃 Application Filters					
ORL Categories					
Application Groups					
Services					
PAC Files					
<ul> <li>Vulnerability Rules</li> </ul>					
Captive Portal Cus					
🗎 URL File					
Address Files					
🏭 User Defined Actio					
💁 Certificates					
😽 Keys					
CA Chains					
CA Certificate					

This will save your ".key" file on the SD-WAN portal.

LUMEN'				E	(i) sbelcher-satlab ( SATLAB ) $\checkmark$
2011214	Monitor Analyti	ics Configuration	Administration		
Home SATLAB-Chicago		<ul> <li>Organization: SATLAB</li> </ul>	~		Build C
* 🗘 😚 🗞	Director Appliance				
🕏 Objects 🗸 🗸					
Address	Key Name		Key File Name	Date Uploaded	
Address Groups	privkey.key		privkey.key	Thu, Feb 13 2020, 01:02	
Schedules					
Cloud Profiles					
Pre-defined >					
🐔 Custom Objects 🗸 🗸					
Applications					
<ul> <li>Scanners</li> <li>Application Filters</li> </ul>					
URL Categories					
Application Groups					
Services					
PAC Files					
Captive Portal Cus					
URL File					
Address Files					
🌡 User Defined Actio					
🗞 Certificates					
Keys					

#### 3. Certificate file upload:

This step must be completed after uploading the ".key" file above. On the same device as the ".key" file upload

Navigate to Objects > Custom Objects > Certificates

Click the upload icon at the upper right of the screen.

Provide a name for the Certificate, browse for the ".cer, .crt, or .pem" file and click OK.

LUMEN					🗐 🕕 sbelcher-satlab ( SATLAB )	~
	Monitor Analytics Config	uration Administration				
Home SATLAB-Chicago	→] Organizati	on: SATLAB 🗸 🗸			Build	6.2
* 🗘 🚫 %	Director Appliance					
🗘 Objects 🗸 🗸		Upload Certificate File to Director	×			
Address	Certificate Name	Certificate Name*		Date Uploaded		
Address Groups     Persistent Actions	certnew.cert	samplecer		Thu, Feb 13 2020, 01:04		
Schedules		Certificate File Name*	_			
Cloud Profiles		sample.cer	Browse			
Pre-defined >		Note - Allowed file formats are .crt, .cer or .pem				
Custom Objects V		ок	Cancel			
Graphers						
Application Filters						
WRL Categories						
Application Groups						
Services						
Vulnerability Rules						
Captive Portal Cus						
URL File						
Address Files						
User Defined Actio						
Kevs						
CA Chains						

This will save your certificate file on the SD-WAN portal.

LUMEN'					(1) sbelcher-sat	tlab ( SATLAB ) 🗸
	Monitor Analytic	cs Configuration	Administration			
Home SATLAB-Chicago	N	Organization: SATLAB	~			Build C
* 🗘 😚 %	Director Appliance					
💲 Objects 🛛 🗸				Ţ.	- III <b>Y</b>   < 1	▶ 25 ∨
Address	Certificate Name		Certificate File Name	Date Uploaded		
Address Groups Dersistent Actions	certnew.cert		certnew.cer	Thu, Feb 13 2020, 01:04		
Schedules						
Cloud Profiles						
🗞 Pre-defined >						
🗞 Custom Objects 🛛 🗸						
Applications						
Scanners						
Application Filters						
ORL Categories     Application Groups						
Services						
PAC Files						
<ul> <li>Vulnerability Rules</li> </ul>						
Captive Portal Cus						
URL File						
Address Files						
User Defined Actio						
Kevs						
CA Chains						

### Configure web browsers in clients

Windows authentication credentials are sent through the Web browsers, which must be configured to do such. For additional information, please refer to these online resources:

https://support.pingidentity.com/s/article/How-to-configure-supported-browsers-for-Kerberos-NTLM

https://active-directorywp.com/docs/Networking/Single Sign On/Configure browsers to use Kerberos.html

#### Internet Explorer and Google Chrome:

Open the Control panel.

Click on Network and Internet, Internet Options.

In the Security tab, Internet Zone, Custom level, and scroll down and select Automatic logon with current username and password.



#### Firefox:

Type *about:config* in the search bar, click in Accept the risk and continue.

Enter your domain name in the network.negotiate-auth.trusted-uris field.

Advanced Preferences	× +			
← → C' ŵ	Sirefox about:config	Sirefox about:config		
○ negotiate				
network.negotiate-auth.allow-non-fqdn		false		⇒
network.negotiate-auth.allow-proxies		true		⇒
network.negotiate-auth.delegation-uris				1
network.negotiate-auth.	gsslib			1
network.negotiate-auth.trusted-uris		testing-domain.internal		1 5
network.negotiate-auth.using-native-gsslib		true		⇒
negotiate		●Boolean ○Number ○String		+

### Kerberos Method Summary

General overview of steps to use Kerberos:

Customer Certificate Responsibility:

- 1. Generate private key with password (openssl genrsa -aes128 -passout pass:(complex password) -out privkey.pem 2048
- 2. Generate public CSR (certificate signing request) with that key (openssl req -out key-csr.csr key privkey3.pem -passin pass:(complex password) -new)
- 3. Copy and paste the CSR into your internal trust CA, to be signed. MUST be signed using a subordinate CA template.
- 4. Export as Base 64 encoded certificate.
- 5. Upload Private Key and signed Certificate into the Director Context, named a common name specified in the template.
- 6. Customer MUST also install this signed certificate into the local Key Store for all users, into the Intermediate Trusted CA tab.
- 7. Customer must also modify the end user browsers internal configuration to allow the authentication to occur.

### **SSL Certificate Considerations**

The design is to use a single certificate and key, PKI signed, loaded into the SD-WAN Portal, and then pulled manually into each appliance context (performed by Lumen engineer). This certificate is then referenced in both the captive portal section and the Decrypt Profile, and they must match. This certificate must also be loaded into the AD users key store/per PC. If this is not done, and HTTPS websites will not authenticate the user.

When the certificate is signed by the customers private CA root, it **MUST** be signed using the subordinate template, meaning it has the CA:true attribute. This certificate also **MUST** be loaded into the users key store, in the Intermediate root authority. The browser must also be configured to pass identity parameters. In IE this is in Internet Options > Security tab > Custom Level > User Authentication > Logon>Automatic logon with current username and password option checked.

### **Security Best Practice**

- Use a password when generating the Private Key (requires the .pem extension to be changed to .key in order to import).
- Only leave the private key on the SD-WAN Portal when needed to move into the appliance. Key file can be deleted after the appliances have been uploaded.

## Appendix - Key Certificate Generation Process – Lumen Recommendations

The following table defines the **@VARIABLES@** used within the configuration templates defined within this page:

Variable	Description	Example	Additional Comments
@DOMAIN_USER.DOMAIN@ DOMAIN@	Standard customer domain user at customer domain	customer1.company@com pany.com	Use AD/LDAP standard naming convention
@DOMAIN_USER@	Standard AD/LDAP domain username	customer1	Use AD/LDAP standard naming convention

### **OpenSSL Commands**

It is recommended to OpenSSL to generate a private SSL key and public Certificate Signing Request (CSR). See command examples below.

## **Private SSL Key Generation**

openssl genrsa -aes128 -passout pass:@CUSTOMER\_PASSWORD@ -out privkey3.pem 3072

### **Public CSR Generation**

\_\_\_\_\_

openssl req -out key-csr.csr -key privkey3.pem -passin pass:@CUSTOMER\_PASSWORD@ -new

## **Keytab File Generation**

• Random Kerberos Password (Recommended Method):

ktpass -princ HTTP/@DOMAIN\_USER.DOMAIN@DOMAIN@ -mapuser @DOMAIN\_USER@ +rndPass -mapOp set +DumpSalt -crypto AES256-SHA1 -ptype KRB5\_NT\_PRINCIPAL -out mss-test.keytab

• Crypto All (Most Compatible):

ktpass -princ HTTP/@DOMAIN\_USER.DOMAIN@DOMAIN@ -mapuser @DOMAIN\_USER@ -mapOp set -pass @DOMAIN\_USER\_PASSWORD@ -crypto all -ptype KRB5\_NT\_PRINCIPAL -out Sample.keytab • Additional Options:

ktpass -princ HTTP/@DOMAIN\_USER.DOMAIN@DOMAIN@ -mapuser @DOMAIN\_USER@ -crypto all -ptype KRB5\_NT\_PRINCIPAL -pass @DOMAIN\_USER\_PASSWORD@ -out mss-test3.keytab

• Additional Example:

ktpass -princ HTTP/@DOMAIN\_USER.DOMAIN@DOMAIN@ -mapuser @DOMAIN\_USER@ -mapOp set -pass @DOMAIN\_USER\_PASSWORD@ -crypto all -ptype KRB5\_NT\_PRINCIPAL -out mss-test\_Kerberos.keytab

• Note: the -pass option allows for a known password, which is considered risky, as the account can be used by others manually. Should consider using +rndPass which will reset the user account password to a random string, thus assuring it is ONLY used by Kerberos.