CenturyLink® **SD-WAN**

AD Integration—September 2019

CenturyLink®

General Disclaimer

Although CenturyLink has attempted to provide accurate information in this guide, CenturyLink does not warrant or guarantee the accuracy of the information provided herein. CenturyLink may change the programs or products mentioned at any time without prior notice. Mention of non-CenturyLink 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. CENTURYLINK 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.

CENTURYLINK 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 CENTURYLINK PRODUCT OR SERVICE, OR DAMAGES RESULTING FROM USE OF OR RELIANCE ON THE INFORMATION PROVIDED IN THIS GUIDE, EVEN IF CENTURYLINK 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 CenturyLink 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 CenturyLink with any CenturyLink product, or to create any new or additional warranties or licenses.

Contents

Overview

Introduction

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 CenturyLink SD-WAN customer's network. To activate and integrate User and Group Authentication (A Directory), the customer will be required to assist with some steps in the deployment process. This document will give an overview of the CenturyLink 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 in order 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 CenturyLink SD-WAN (Powered by Versa) 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 CenturyLink 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 users credentials in the form of a fully qualified user name (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

- 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 in order 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.
- 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 users 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 sends traffic through the Versa (which then resets the timer).
- The Silent method using Kerberos is the CenturyLink 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

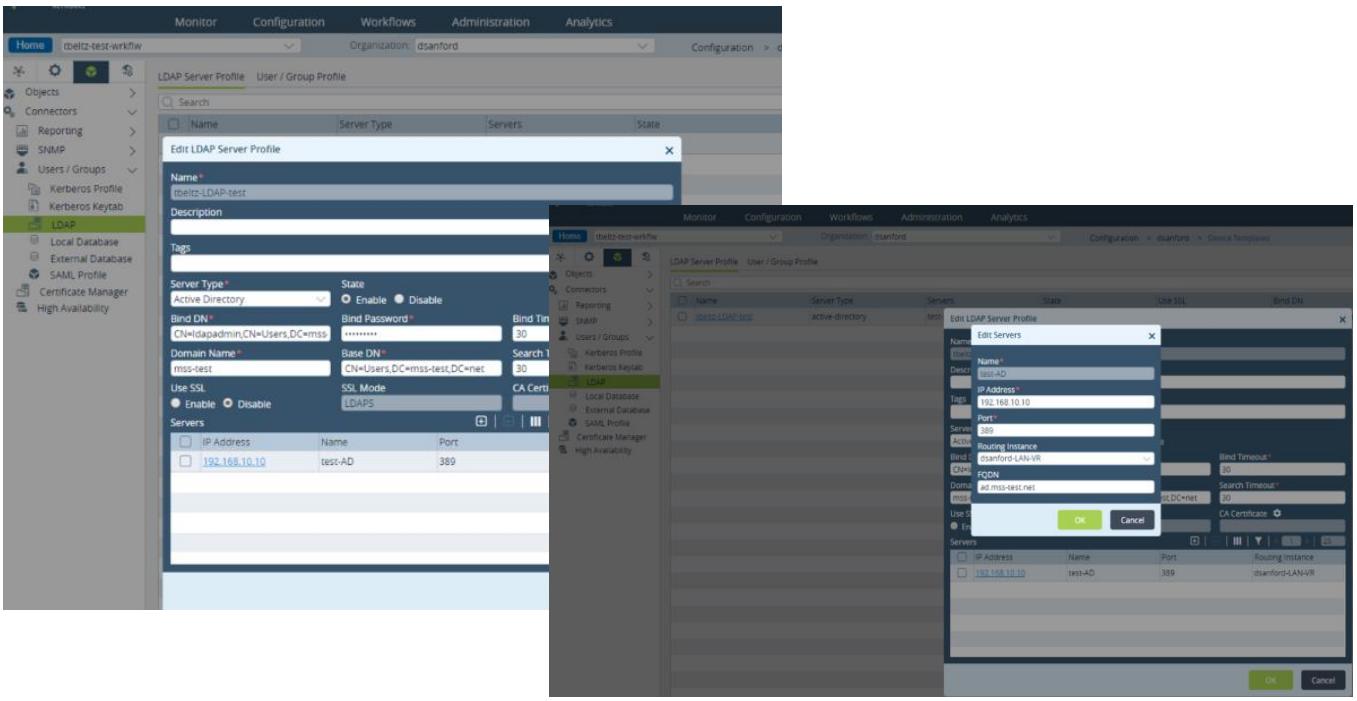
Customer Steps Summary

1. Customer will provide CenturyLink TDE team representative the necessary information listed below for the customer's AD environment.
2. Customer will need access to the CenturyLink 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 CenturyLink preferred method using Kerberos or the alternative LDAP option for authentication.
4. See Appendix for Key Generation References.

AD Information CenturyLink Technical Design Engineer (TDE) Will Require from the Customer

- 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

Example screenshots for reference:

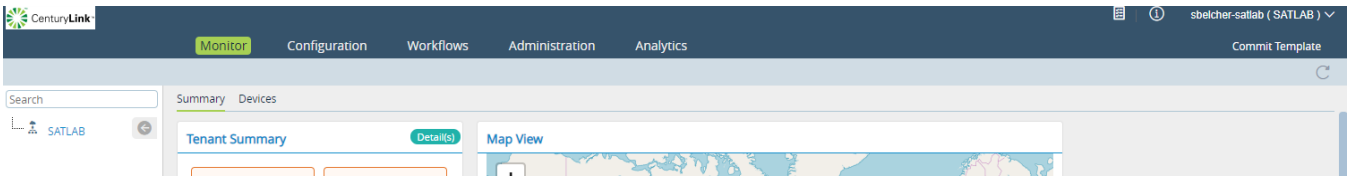


Upload of Private Key and Certificates (Customer Responsibility)

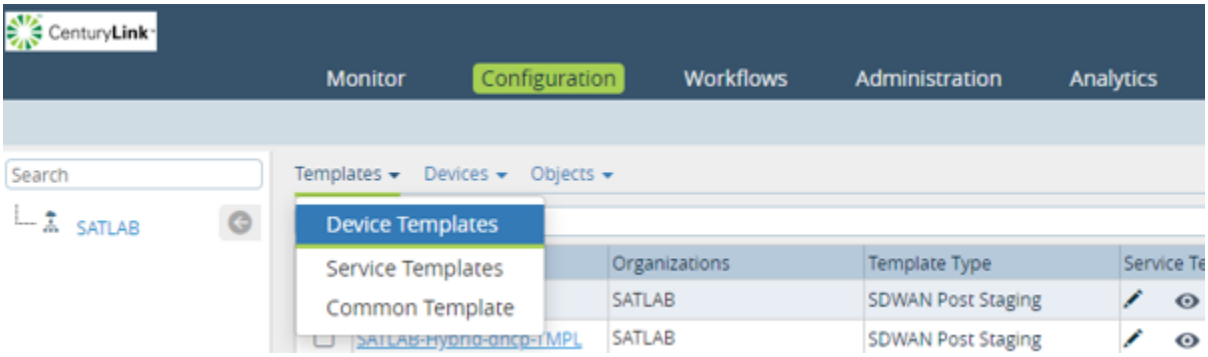
Customer will need to upload these 3 files into the CenturyLink SD-WAN Portal. These can be uploaded in the following sequence and all can be uploaded at the same timeframe. There is no need to wait on another step from CenturyLink engineering. Customer should notify their CenturyLink TDE (engineer) 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 CenturyLink 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 five menus as shown below. Note: The other context called the Appliance Context will only have three menus across the top.



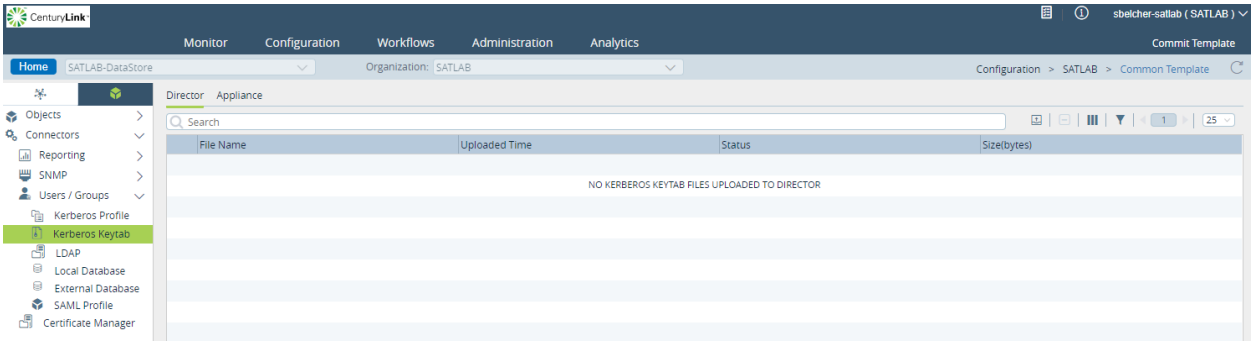
Navigate to Configuration > Templates > Common Template



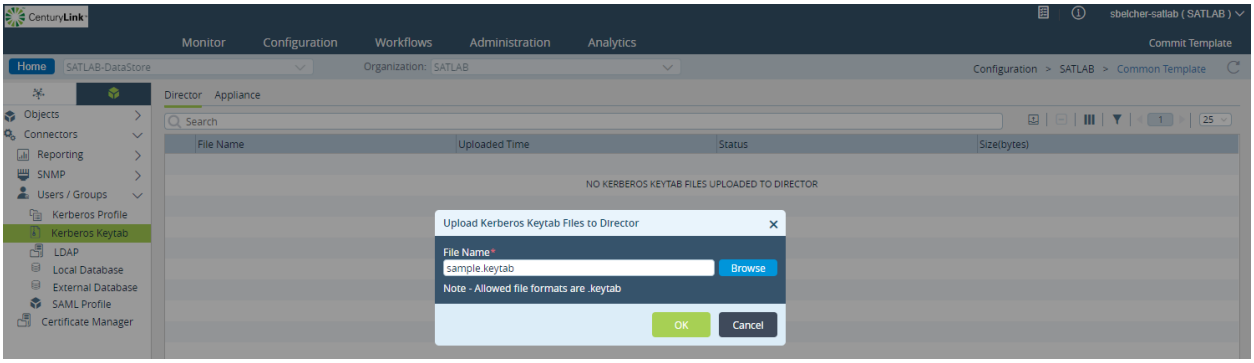
After selecting the Common Template, navigate to the icon in the upper left corner. It will be labeled “Objects and Connectors.”

1. Keytab File upload:

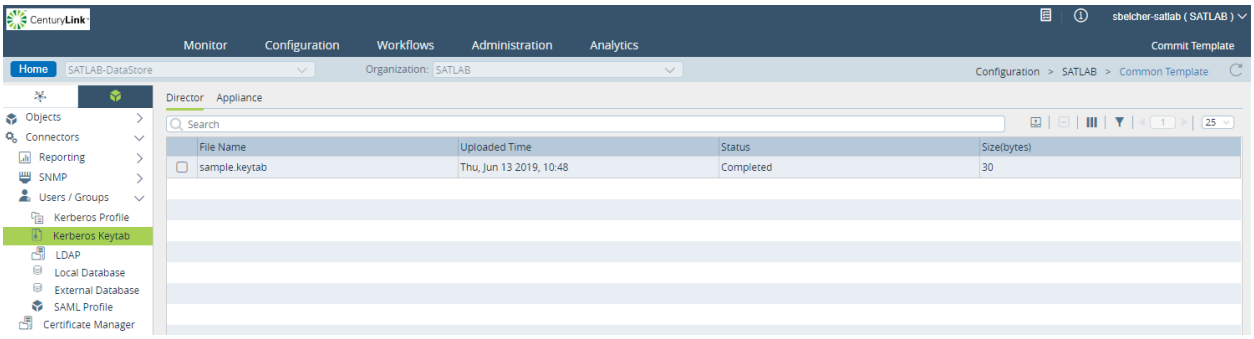
   Navigate to Connectors > Users/Groups > Kerberos Keytab.



Select the upload icon  on the upper right and browse for your ".keytab" file and click OK.



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



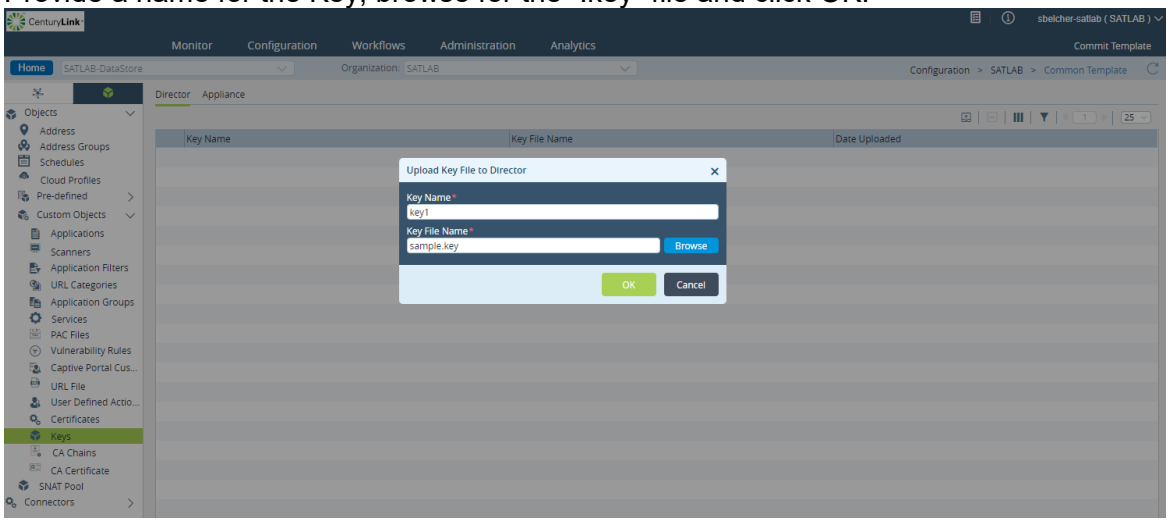
2. Key file upload:

   This process will be similar to the above with the exception of the starting point.

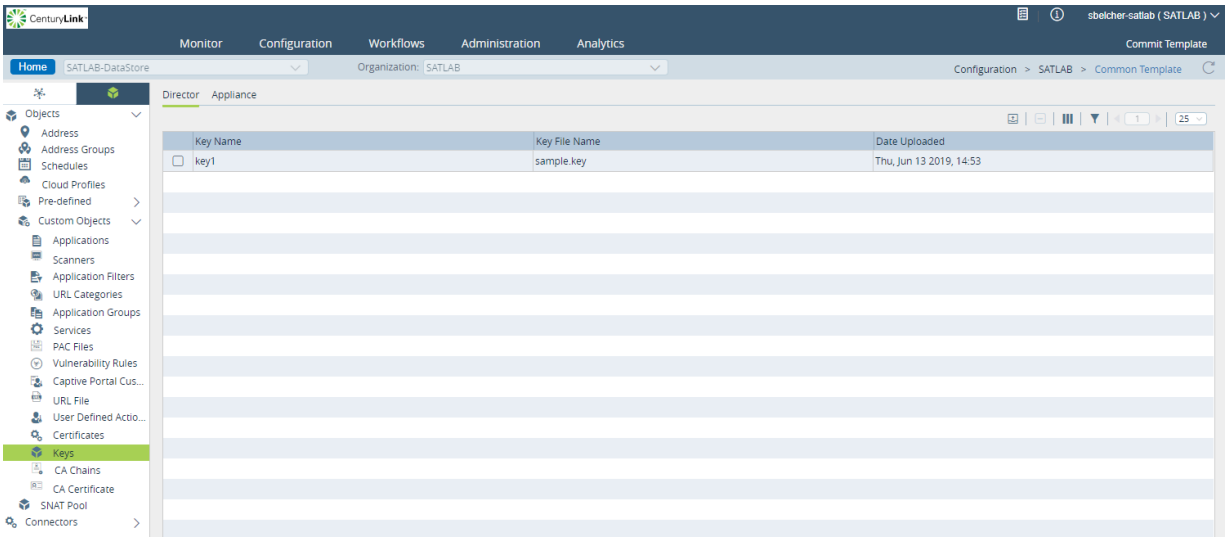
   Navigate to Objects > Custom Objects > Keys

Do the following:

1. Click the upload icon  on the upper right of the screen.
2. Provide a name for the Key, browse for the ".key" file and click OK.



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



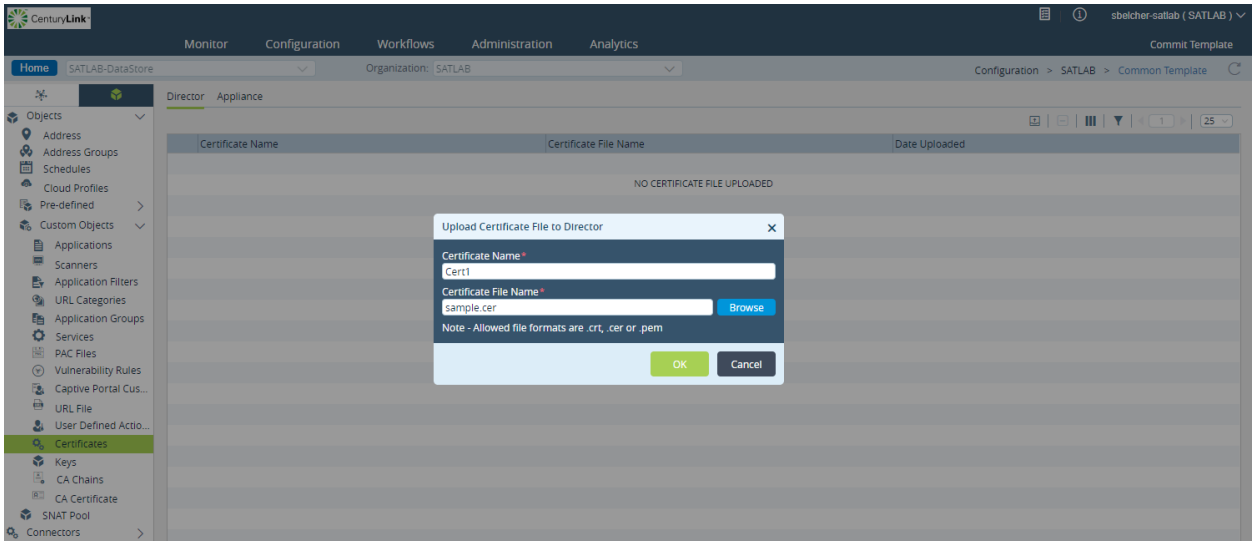
This step must be completed after uploading the ".key" file above.

Navigate to Objects > Custom Objects > Certificates

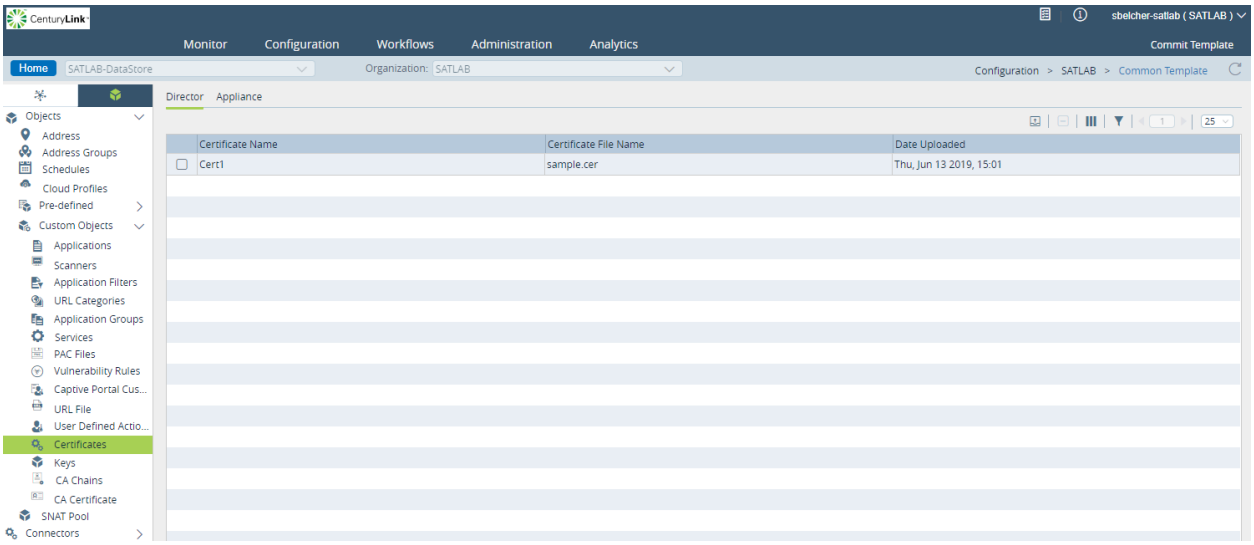
Do the following:

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

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



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



Kerberos Method Summary

General overview of steps to use Kerberos: Key generation is performed using OpenSSL

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 CenturyLink 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 no 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 user name and password option checked.

Security Best Practices

- 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 CenturyLink Recommendations

The following table defines the @VARIABLES@ used within the configuration templates defined within this page: software-version-change

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

Vendor Documentation: Keytab file information:

- 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

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