

WALLIX - OKTA

LDAP AND RADIUS AUTHENTICATION

INTEGRATION GUIDE

November 2020

VERSION**1.0**

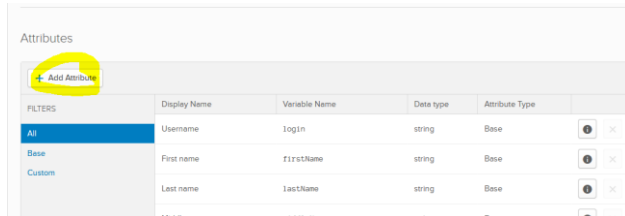
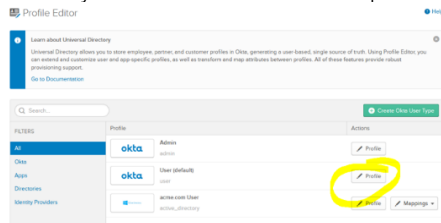
WALLIX Contacts:

Chief Strategy Officer	Name: Didier Cohen Tel: +33 6 26 51 12 02 E-mail: dcohen@wallix.com
Pre-Sales Engineer North America	Name: Grant Burst Tel: +1 978 880 2040 E-mail: gburst@wallix.com

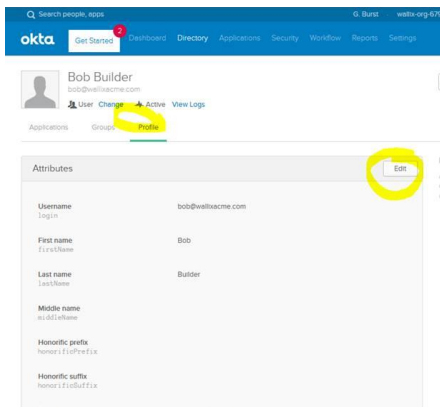
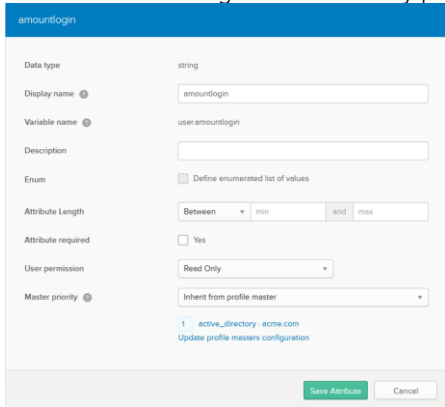
Date: 23/11/2020

Integration of OKTA LDAP with the WALLIX Bastion

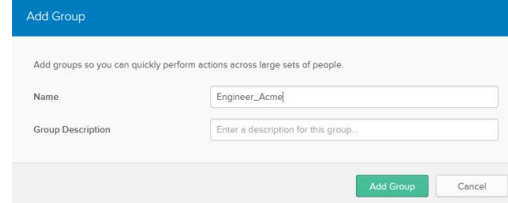
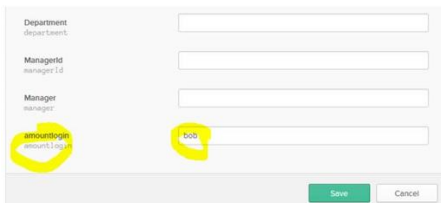
When integrating the Okta LDAP with the bastion you must use DNS with the full FQDN i.e. wallixacme.ldap.okta.com
PORT Either StartTLS 389 or SSL 939 will work and a certificate is not needed
Base DN Ensure you add dc=okta i.e dc=wallixacme,dc=okta,dc=com
Login Attribute this needs changing and it is best to start with the Profile configuration via Octa Directory /Profile Editor / user default profile Add Attribute



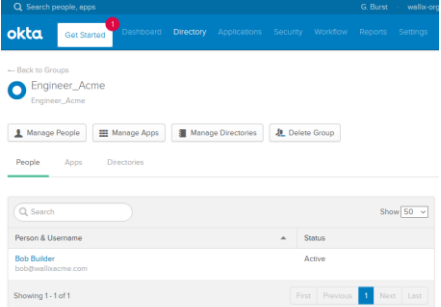
In this case "amountlogin" Go to Directory/people Click on a user that will authenticate and Edit



Scroll to the bottom and add the login name to the attribute in this case "Bob" Create a group for the user



And add the User



Head back to the Bastion Configuration/External Authentication
Add the new attribute to the Login Attribute

[Edit this authentication](#)

Authentication type: LDAP
 Authentication name: okta
 Server: wallixacme.ldap.okta.com
 Port: 636
 Timeout (s): 6.0
 Base DN: dc=wallixacme, dc=okta, dc=com
 Login attribute: **amountlogin**
 User name attribute: uid
 Bind method: simple
 Active Directory:
 Encryption: SSL
 User: uid=spiderman, dc=wallixacme, dc=okta, dc=com
 Description: --

Two-Factor Authentication (2FA)
 Use primary domain name:

Configuration/LDAP AD Domains
Chose LDAP and then the New Okta domain

Edit LDAP/AD domain: okta

Description:

Default domain:

LDAP/AD domain name: wallixacme.com

Directory:

Available Directories

LDAP

Selected Directories

okta

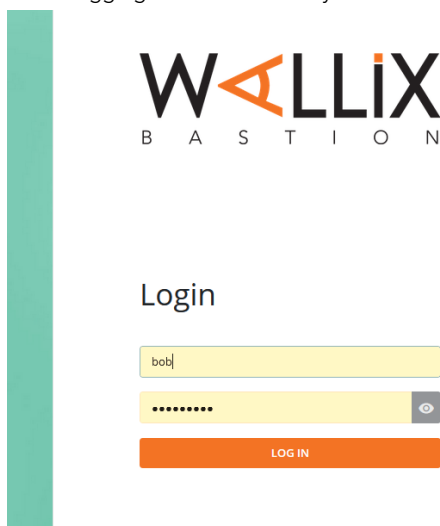
Select all Delete all

Map the Bastion Group to the New Groups as configured in Okta

LDAP authentication mapping

User group	Profile	LDAP group
<input checked="" type="checkbox"/> Engineers	user	Default group for users without group in this domain
Engineers	user	
Engineers	user	cn=engineer_Acme.ou=groups,dc=wallixacme,dc=okta,dc=com
Helpdesk	user	cn=test.ou=groups,dc=wallixacme,dc=okta,dc=com

When logging on to the bastion you will now just use the new attribute i.e. Bob



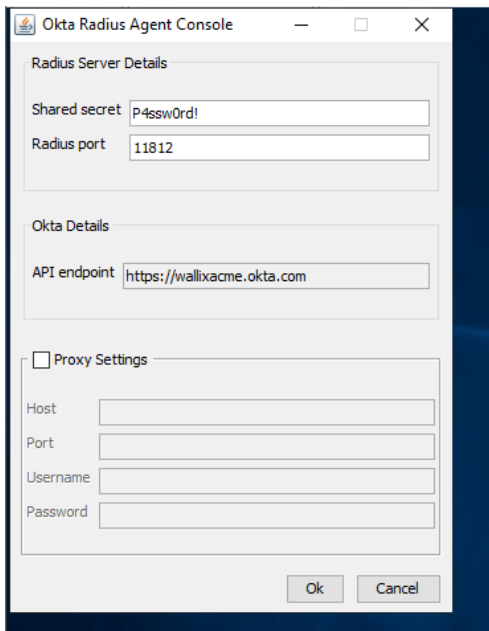
WALLIX
BASTION

Login

LOG IN

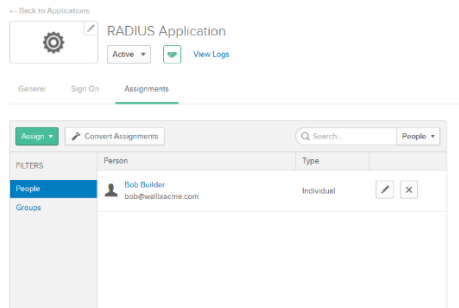
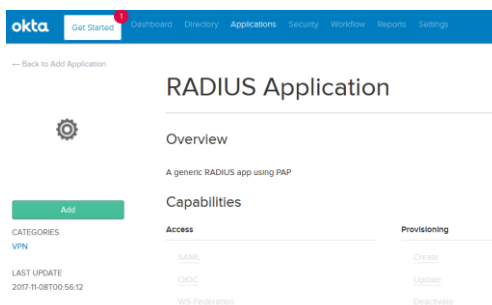
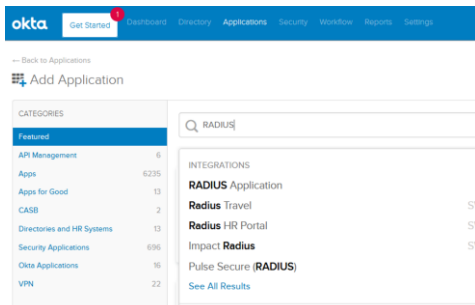
Adding Okta RADIUS authentication

If Okta Radius Authentication is required
Download the Agent from the Octa Admin site Settings/download
Install on windows server and follow the wizard
Ensure that the firewall ports are open UDP in this case 11812

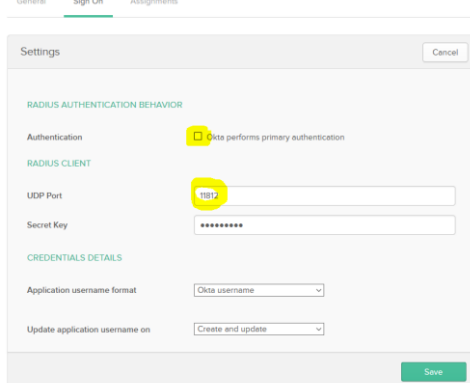


On the Okta admin site go to applications /Add Application
Search for RADIUS

Chose RADIUS Application



Settings/Sign On
Untick Okta performs primary authentication and add the new port.
Settings/Assignments add the users or groups



On the Bastion
 Configuration/External Authentications
 Add RADIUS
 For the server point to the server with the RADIUS Agent installed
 Change to the New Port
 And tick Use Primary Domain Name

Configuration options Time frames External authentications LDAP/AD domains Notifications Local password policy

Edit external authentication

Authentication type *: RADIUS
 Authentication name *: Okta_Radius
 Server *: win2k19.acme.com
 Port *: 11812
 Timeout (s) *: 5,0
 Secret *: ●●●●●●
 Description :

Two-Factor Authentication (2FA)
 Use primary domain name:
Force usage of full user name (e.g. user@domain) during second authentication login

Apply

Configuration /LDAP AD Domains
 Add the Radius Authentication to Secondary Authentication

Configuration options Time frames External authentications LDAP/AD domains Notifications Local password policy Connection messages X509 configuration API keys License Encryption Audit logs

Edit LDAP/AD domain data

Description :

Default domain
 LDAP/AD domain name *: win2k19.acme.com
 Directory :

Available Directories: LDAP
 Selected Directories: LDAP

Secondary authentication:

Available Secondary Authentications:
 Selected Secondary Authentications: Okta_Radius

Log on to the Bastion with the Okta LDAP user as before using the Okta LDAP Password



Login

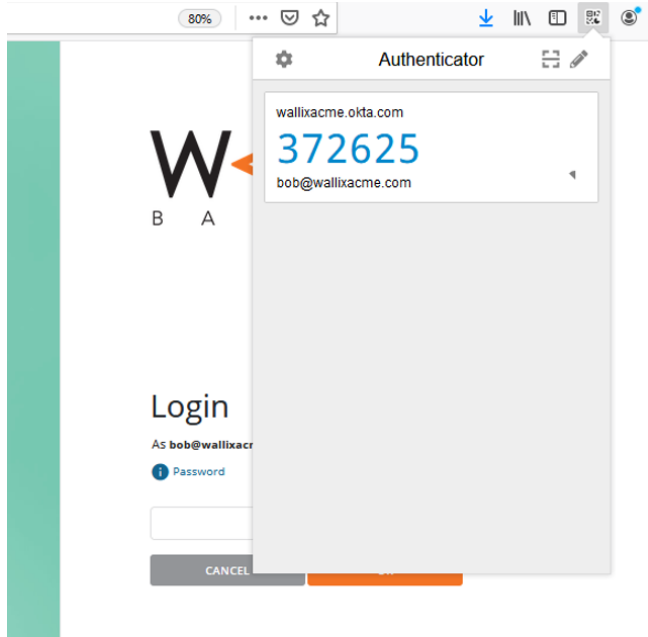
You will see that the login has been accepted and the username has been replaced with the full username and is asking for the 2nd factor



Login

As bob@wallixacme.com

I have used Google authenticator to generate the token



And Bob is now signed on to the Bastion using Multifactor Authentication
Username
LDAP Password
Generated Token

