

Cloud Secure – PingOne Integration

Configuration Guide

Document Revisions4.0Published DateJuly 2020

Pulse Secure, LLC 2700 Zanker Road, Suite 200 San Jose CA 95134

https://www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Cloud Secure – PingOne Integration Configuration Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

INTRODUCTION	
About This guide	
Pre-requisites	
PULSE CONNECT SECURE CONFIGURATION	
PINGONE CONFIGURATION	
STEPS TO CONFIGURE7	
ZENDESK CONFIGURATION	7
Steps to Configure1	7
END-USER FLOW ON MOBILE DEVICES	9
END-USER FLOW ON DESKTOPS	C
TROUBLESHOOTING	1

List of Figures

FIGURE 1 ARCHITECTURE DIAGRAM	5
FIGURE 2 NEW METADATA PROVIDER	6
FIGURE 4 SETUP IDENTITY REPOSITORY	7
FIGURE 5 SELECT IDENTITY REPOSITORY	8
FIGURE 6 CONFIGURE IDP CONNECTION	8
FIGURE 7 IMPORT IDP METADATA	9
FIGURE 8 IMPORT IDP METADATA	9
FIGURE 9 ADD APPLICATION	10
FIGURE 10 SEARCH APPLICATION CATALOG	
FIGURE 11 SETUP ZENDESK	11
FIGURE 12 SSO INSTRUCTIONS	12
FIGURE 13 CONFIGURE SSO	13
FIGURE 14 ATTRIBUTE MAPPING	14
FIGURE 15 CUSTOMIZE PINGONE APP	14
FIGURE 16 REVIEW SETUP	15
FIGURE 17 DOWNLOAD SIGNING CERTIFICATE	16
FIGURE 18 ENABLE SSO FOR ADMIN	17
FIGURE 19 ENABLE SSO FOR END-USERS	18

Introduction

About This guide

Cloud Secure Solution provides Secure Single Sign-On for Cloud services using PingOne as Identity Management Provider. In this federated solution, PingOne acts as both Identity Provider (for Cloud services) and Service Provider (for Pulse Connect Secure). PingOne allows Pulse Connect Secure to be configured as Third Party SAML Identity Provider to enable Secure Single Sign-On to Cloud applications.

This document provides configuration of PingOne SP on Pulse Connect Secure, configuration of Zendesk Service Provider and PingOne. This document does not cover basic configurations on Pulse Connect Secure (PCS) and Pulse Workspace Mobile Device Management (PWS) Server which are required to be enabled before configuring PingOne and cloud service specific configurations outlined in this document. Basic configurations of PCS and PWS are covered as part of Cloud Secure Admin Guide.

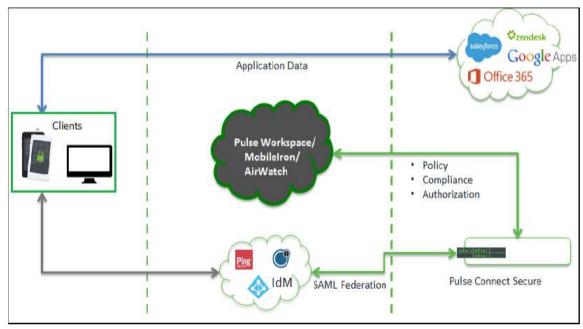
MobileIron and AirWatch Third-party MDM servers can also be used in this solution to manage devices and to evaluate compliance posture of the mobile devices.

Pre-requisites

Prerequisites for this solution include:

- Identity Provider: Pulse Connect Secure with minimum version of 8.2R3
- MDM Server: Pulse Workspace Server/ MobileIron/ AirWatch
- Identity Management Provider: PingOne
- Clients: iOS Device/ Android Device/ Windows/ MAC OS X Desktops

Figure 1 Architecture Diagram



Pulse Connect Secure Configuration

Cloud Secure can be configured with the new UX, which allows you to quickly and easily configure the Cloud Secure functionality without navigating into multiple pages. The new UX enhances the administrator experience through pre-populating some of the relevant settings and reusing the existing configurations.

For basic configurations details, refer to the following sections:

• Configuring Pulse Connect Secure - Basic Configurations (Mandatory)

• Configuring Pulse Workspace

Follow the below steps to configure PingOne as third-party IDP on PCS:

1. Navigate to System > Cloud Secure > Cloud Secure Configuration.

If you have completed the basic configurations and activated Cloud Secure. Click **Open** to go back to the Basic Configuration page.

- 2. Click Third-party IdP Settings:
 - a. Click Add New and select the Third-party IdP as PingOne.
 - b. Select the Subject Name Format = Email Address.
 - c. Enter the Subject Name.
 - d. Click Browse and upload the metadata file (Step 7 of PingOne Configuration).
 - e. Set the signature algorithm to Sha-1 or Sha-256.
 - f. Select the desired roles.
 - g. Click OK.

Figure 2 New Metadata Provider

	(0	
		and a second sec	
	A		
	Figure		
	Collegent		
No. Shenny			() Add free 1 minutes
Subject Name Format - 😧 -	Eval Admen	÷	
Sabject Name 9	-continues-g-consis-		
Metadada Filo	Duran fa		
Signatory Algorithm 😡	4 Stu-1 0 Sta-2%		
4 Select Al Holes (they Role)	a war belange it falses saweight then		
where we say it is the many of any to a	a ne porth a door too rai		
educarit Settings			
olonash Sellinga Craata Boolenash		marials Subject News Inneal and Subject Name Sy specify Summeric	

Note:

• Click Show IdP to view the details of the configured Third-Party IdP servers.

PingOne Configuration

In this solution, PingOne serves as Identity Management Provider. PingOne acts as Identity Provider for Cloud services and as Service Provider for Pulse Connect Secure. For Cloud Secure solution, PingOne has to be configured with:

- PingOne Account
- Add PCS as SAML IdP
- Configure Cloud Applications

Steps to Configure

Follow the below steps to configure PingOne::

- 1. Sign up for PingOne admin account at https://admin.pingone.com/web-portal/login and create your domain.
- 2. Log in to PingOne domain account as admin at https://desktop.pingone.com/<Domain>.
- 3. Navigate to Setup > Identity Repository. Click Change Identity Repository.

Figure 3 Setup Identity Repository

ing One'	DAS-BOHD	APPLICATIONS	USES SETUP	ADDOLHT			fign.
Identity Repository Dock	Authentication Policy	PingID De	ectory Certricat	es			
Settings							
() Thurse currently evaluation of the second	utting promium features of th	w ProgOne Dire	sclury. For informatic	er un beemwig opfians, pie	are contact your account.		
				12			
PingOne Directory				Cha	inge Identity Repositury	王	
DRECTORY STATISTICS	I						
USERS: 4							
GROUPS 2							
SSO SETTINGS							
REGISTRATION							
BASSWORD POLICY							
ATTOBUTES API CREDENTIALS							

4. Select CUSTOM SAML as Identity Repository. Click Next.

Figure 4 Select Identity Repository

ECT AN IDENTITY REPOSITOR irely connect users and groups for singl	Y : PingOne Directory e sign-on through your PingOne account.		
P1	Integrate with AD in minutes	Pf Integrate multiple user	Integrate with Azure AD in
offers centralized administration and self-service user registration.	using our lightweight agent with automatic failover, load balancing and no firewall changes.	directories, provide offline MFA or enable advanced on- premises and hybrid use cases.	minutes and connect via OpenID Connect flows.
PINGONE DIRECTORY	ACTIVE DIRECTORY	PINGFEDERATE	MICROSOFT AZURE AD
	G	Ā	R
Integrate with Microsoft's federation server and connect via SAML metadata exchange.	Integrate with an existing GSuite domain and connect via OpenID Connect flows.	Integrate with your existing OpenID Connect provider. Fully customizable.	Integrate with your existing SAML provider. Fully customizable.
MICROSOFT AD FS	GOOGLE	CUSTOM OIDC	CUSTOM SAML

5. Select Enable Account Specific Entity ID. Click Next.

Figure 5 Configure IDP Connection

- 80	ngOne Universal Certificate Primary (Expires 20/05) 🖂
P	ngone onversal ceruncate Printary (expires 20/05)
N#	BLE ACCOUNT SPECIFIC ENTITY ID 🔞
t	ittp://pingone.com/lb35c15d-0a79-4/8d-86ca-b81
sig	IN AUTHINREQUEST FROM PINGONE
EIG	NING ALGORITHM
	ISA_SHA256
	nfigure the IdP connection to PingOne at your IdP. Either upload the metadata to your IdP (recommended), inually enter the SAML parameter values at your IdP.
	Download the PingOne metadata and upload it to your IdP
C	Download PingOne Metadata
	Enter the PingOne connection information manually at your IdP.

 Under the Configure your PingOne Connection section, select Import your IDP Connection Metadata, select PCS SAML Metadata file and click Save (To download PCS Metadata file, navigate to Authentication >Signing-in >Sign-in SAML >Metadata Provider and click on 'Download Metadata' on PCS admin console).

Figure 6 Import IDP Metadata

Connec	ct to an Identify Repository
0	DELECT AN IDENTITY REPOSITORY : 3rd Purty SAME, For
0	CONFIGURE YOUR DP CONNECTION WWW
-	CONFIGURE YOUR PINGONE CONNECTION Angle LeP current that information is the PingGrie SAM, parameters. Effort optical that metadole to your telP (inconstructed), in report must be connection date or your SP. Charge Re D same-relations of plant Research Leg. Leg. Messarly teles must bP Connection releasables (2)
	Gintel

7. Once the settings are saved, verify that all the PingOne Settings and SAML Settings are updated. Click on the edit icon and download **PingOne SAML Metadata**.

Figure 7 Import IDP Metadata

One:		1065 5	HHLCH!	one une	10 <u>SETU</u>	ACCOUNT	O	
identity texpository DOCK	Authentication	Policy 7	adio	Certificala	84			
Settings								
3rd Party SAML							Change Identity Repository	王
PHOOSE SETTINGS								
ENABLE ACCOUNT SPEC	and animate pa	No.						
SIGN AUTO MEED CENT O		Nip						
PERCONE ENTITY RL			ate curs?	hitte mail	Po estis de			
ASSERTION CONSUMER	SERVICE LOL:					ACL sare?		
RELAY TITATE		Super-Paris	parie-carty	ADExaes.	1			
ACS URL PARAMETER:		Training (a	34.00					
PROTOCOL.		SAML 20						
ACTIVE BIOHING CENTR		Type: PSW Express 20 Disenters	20/05/03	ž.				_
ENCRYPTION CERTIFICA	18.	Expires, 20 Dissertion		0				2
BAME SETTINGS								
DKTTY ID	https://soo.jude	secureacce	ss.reeVda	he notauto	arti-endpo	18.00		
\$50 ENDPORT:	інцис./грондани	a puberecu	Reaccess	NOTION IN	indiani	the op		
SKONING ALCORITHM.	R54_5H4756							
PRIMARY CERTIFICATE.	DN: ON-public Expense 2010/07		net, OU	Duman Co	drui Valend	pα		

Connec	t to an Identity Repository
2	CONFIGURE YOUR IDP CONNECTION CHOOSE SIGNING CERTIFICATE
e	ENABLE ACCOUNT SPECIFIC ENTITY ID
	http://pingone.com/tb35c15d-0a79-4f8d-86ca-b81;
	SIGN AUTHINREQUEST FROM PINGONE
	SIGNING ALGORITHM
	Configure the IdP connection to PingOne at your IdP. Either upload the metadata to your IdP (recommended), or manually enter the SAML parameter values at your IdP.
	Download the PingOne metadata and upload it to your idP.
	Enter the PingOne connection Information manuality at your IdP. (?)

- 8. To add Zendesk application in PingOne for SSO, follow below steps:
 - a. Navigate to **Applications > My Applications**.
 - b. Click on Add Application and select Search Application Catalog.

Figure 8 Add Application

My Applic	ations				
SAML CO	ж.				
Applications yo	u've added to your account are hit	ed from You can search	by application name, i	tescription or untituite	
· Active mpb	cations are enabled for single sign slays the application defails.				
Make sure to an authorizen the l	ssign each application to the appro-	priate groups on the Us e applications.	er Groun page. This e	rables the display of the i	opplications in the dock and
	Application Name	Type	Status	Enabled	
		100	-	100.0	Remove 🕨
					Remave
					Remove
					Remove
10					Person 🕨
Add Applicati	on -				Faute All 550

c. Type **Zendesk** in search list. Click on Zendesk application in the results.

Figure 9 Search Application Catalog

	A / /	Applications / Applic	ation Catalog
r it by name. Don't see the	application you're looking for? Fill out our Appli	cation Request Form	1.
Search			
me	↑ Type		
	SAML		•
	-	r it by name. Don't see the application you're looking for? Fill out our Appli Search me Type	ime Type

d. Click Setup.

Figure 10 Setup Zendesk

Zendesk		Search				
	Application Na	ame		* Туре		
2	Zendesk			SAML		Υ.
	Logo @	Zzen á	lesk			
	lcon @	2				
	Name @	Zendesk				
	Description @	Zendesk simplifies custom automatic a and streamlined sys content	actions, meaningful (organization,		
	Category @	CRM			Sctup	

e. Leave values to default and click Continue to Next Step.

Figure 11 SSO Instructions

Signing Certificate		PingOne Account	Origination Certificate ·	
		Download		
		For reference, pleas	se note the following configuration parameters:	
	SaaS ID	e9a1bcee-4f4c-4fe	2-a5b9-ec83d2a53491	
Initiate	Single Sign-On (SSO) URL o		.pingidentity.com/sso/sp/initsso?saasid=e9a1bcee-4f4c-4fe2-a5b8- iid=673b5ebc-e6ce-4326-a445-999cf3fdd8ab	
	Issuer	https://ngs.aqa.puls	esecureça.net/dana-na/auth/saml-endpoint.cgi	
Sig	gning Algorithm	RSA_SHA256	/*	
		S OL N AV 284		
		in order to set up 53	SO to Zendesk, please follow the instructions below.	
SETTING	GS > SECURITY >	Authentication		
	1-01-4-01-1			
	Label	Des	scription	
1	Label Configure SS parameters	0	scription ack Single Sign On	
1	Configure SS	O Che		
	Configure SS parameters Configure SS	0 Che 0 Mod 0 SAN	eck Single Sign On	idpid={Enter
2	Configure SS parameters Configure SS parameters Configure SS	O Che O Moo O SAN you O http	eck Single Sign On de: SAML ML SSO URL: https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?	
2	Configure SS parameters Configure SS parameters Configure SS parameters Configure SS	Che Che Mod SAN you Co http redi	eck Single Sign On de: SAML ML SSO URL: https://sso.connect.pingidentify.com/sso/idp/SSO saml2? ir IDP ID} is://sso.connect.pingidentity.com/sso/terminatesession?page=https://(er	
2 3 4	Configure SS parameters Configure SS parameters Configure SS parameters Configure SS parameters Configure SS	Che Che Mod C SAM you C SAM you C SAM you C SAM you C SAM YOU C SAM YOU C SA SA SA SA SA SA SA SA SA SA SA SA SA	eck Single Sign On de: SAML ML SSO URL: https://sso.connect.pingidentity.com/sso/idp/SSO samt2? ir IDP ID} is://sso.connect.pingidentity.com/sso/terminatesession?page=https://(er irect.users.to}	nter a URL to
2 3 4 5	Configure SS parameters Configure SS parameters Configure SS parameters Configure SS parameters Configure SS parameters Configure SS	Che Che Mod C SAM you C SAM you C SAM you C SAM you C SAM YOU C SAM YOU C SA SA SA SA SA SA SA SA SA SA SA SA SA	eck Single Sign On de: SAML ML SSO URL: https://sso.connect.pingidentity.com/sso/idp/SSO.samt2? ir IDP ID} os://sso.connect.pingidentity.com/sso/terminatesession?page=https://{er irect users to} ranges (optional): Leave blank for all IPs to use SSO. rtificate Fingerprint: Obtain the fingerprint of your PingOne signing certi	nter a URL to
2 3 4 5	Configure SS parameters Configure SS parameters Configure SS parameters Configure SS parameters Configure SS parameters Configure SS	Che Che Mod C SAM you C SAM you C SAM you C SAM you C SAM YOU C SAM YOU C SA SA SA SA SA SA SA SA SA SA SA SA SA	eck Single Sign On de: SAML ML SSO URL: https://sso.connect.pingidentity.com/sso/idp/SSO.samt2? ir IDP ID} os://sso.connect.pingidentity.com/sso/terminatesession?page=https://{er irect users to} ranges (optional): Leave blank for all IPs to use SSO. rtificate Fingerprint: Obtain the fingerprint of your PingOne signing certi	nter a URL to
2 3 4 5	Configure SS parameters Configure SS parameters Configure SS parameters Configure SS parameters Configure SS parameters Configure SS	Che Che Mod C SAM you C SAM you C SAM you C SAM you C SAM YOU C SAM YOU C SA SA SA SA SA SA SA SA SA SA SA SA SA	eck Single Sign On de: SAML ML SSO URL: https://sso.connect.pingidentity.com/sso/idp/SSO.samt2? ir IDP ID} os://sso.connect.pingidentity.com/sso/terminatesession?page=https://{er irect users to} ranges (optional): Leave blank for all IPs to use SSO. rtificate Fingerprint: Obtain the fingerprint of your PingOne signing certi	nter a URL to

f. Under 'Configure your connection' section, provide Zendesk ACS URL (replace \${accountname} with your Zendesk Domain). Similarly, provide Zendesk Entity ID (replace \${accountname} with your Zendesk Domain and prepend https://. For example, https://cloudsecure.zendesk.com). Click Continue to Next Step.

Figure 12 Configure SSO

configure your connection	
Assign the attribute values for single si	ign-on (SSO) to the application.
Upload Metadata o	Select File Of use URL
ACS URL	https://5{accountname].zendesk.com/
	Replace the parameter(a) "(accountrance)" above with your configuration information
Entity ID	\$(accountname).zendesk.com
	Replace the parameter(s) '\$(accountname)' above alth your configuration information.
Target Resource @	
Single Logout Endpoint @	example.com/slo.endpoint
Single Logout Response Endpoint @	example.com/sloresponse.endpoint
Primary Verification Certificate	Choose File No file chosen
Secondary Verification Certificate e	Choose File No file chosen
Force Re-authentication	6
PingOne dock URL	
Default PingOne dock URL	https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=e9a1bcee-4f4c-4fe2-a5b8- ec83d2a53491&idpid=673b5ebc-e6ce-4326-a445-999cf3fdd8ab Use Custom URL ●
NEXT: Attributo Mapping	Cancel Back Continue to Next Ste

g. Under Attribute Mapping section, leave default values and click Continue to Next Step.

Figure 13 Attribute Mapping

2	Ze	ndesk	SA	ML
. Attribute	Mapping			
Мар у	our identity bridge attri	butes to the attributes required by th	e application.	
	Application Attribute	Description	Identity Bridge Attribu	te or Literal Value
	SAML_SUBJECT	mad	SAML_BUBJECT	D As Literal (Advanced)
2	displayName	The user's name to be used for display purposes.	Name or Literal	10 As Literal Advanced
(B)	phone	A phone number, specified as a string.	Nome or Literal	
* Indica	ites a required attribute.			
	gOne App Customization - 2		1.00	incel Back Continue to Next St

h. Click Save and Publish in the next page.

Figure 14 Customize PingOne App

Logo @		
2030 0	Razen desk	
	Select image	
Icon 🛛	2	
	Select image	
Name 🛛	Zendesk	×
Description @	Zendesk simplifies your support team's workflow with custom automatic actions, meaningful organization, and streamlined systems for managing support content.	*
Category @	CRM	

i. Review Setup and click Finish.

Figure 15 Review Setup

view Setup			
Test your connection	to the application		
	Logo e	zendesk	
	icon o	22	
		Zandosk	
	Description w	Zandvisk simplifies your support to custom automatic inclores, meaning and streamlined systems for many context.	sgitul organutaliion.
	Category #	CRM	
You may need to con	ifigure these conner	ction parameters as well.	
	saasid	elia/bcee-4Hz-4Re2-a6b8-ec/83d2a	63491
	Issuer	Ingla migrage publisher uniquinents	ana-naoauthysanni-endpointu gi
	Signing Algorithm	R0A_9HA250	
	ACS URL	https://double.com/aik/com	Wall Contraction and public
	SP ontityid	Mgni Peloudsecurega zendarik, cen	oppersoner en el la filia de la companya de la comp
Initiate Single Si;	in-On (SSO) URL e	https://www.connect.progidentity.com wr.B3d2a534018ktpid=873b5ethc.co	muso/apredisco/twantel=e0u1bc.co-44kc-44u2-a6b4 6c.o-4336-a445-396c13fddRab
Single Sign-On (SSO) Relay State @	https://pingarie.com/1.tl/etfatboee-	the ite2-addi-ec83d2a63491
Sin	gle Logout Endpoint		
Single Logout	Response Endpoint	B	
Force	Re-authentication @	Tator	
	Signing Certificate	Download	
	SAML Motadata	Download	
Applica	tion Altribute	Description	Identity Bridge Attribute or Literal Value
1 SAML	suelect +	man	SAML_SUBJECT
a (0000 May 1	Vainie .	The user's name to be used for display purposes	
a phone		A phone number, specified us a arring	
• indicates a require	et attribute.		
Parameter Name	Descriptio	on -	Viduo
Administrator_Em	ail The account	email of an admin for your Zendesk a	(count_
Zendesk_Api_Tok	en The API Tok	en retrieved from Ziendeuk.	
Zendesk_Subdom	also The subdom	ain of your Zendesk account.	

 Navigate to Applications > My Applications and verify that Zendesk application got configured and is Active. Click on the Application. All the configuration details will be displayed. Download Signing Certificate and make a note of the idpid value from Initiate Single Sign-On SSO URL. These will be used to configure the Service Provider.

Figure 16 Download Signing Certificate



Zendesk Configuration

Zendesk should be enabled as SAML Service Provider for supporting Single Sign-On. For Cloud Secure solution:

- Register with Zendesk and create new Domain
- Configure SAML

Steps to Configure

Follow the below steps to configure Zendesk as Service Provider:

- 1. Register with Zendesk at https://www.zendesk.com/register#getstarted and create a new domain.
- 2. Log in to Zendesk domain as admin at https://<Zendesk Domain>/access/normal.
- 3. Navigate to Admin (Settings gear at the bottom left corner) > Security > Admin & Agents. Enable Single sign-on (SSO), and enable SAML. Configure following values:
 - a. SAML SSO URL = https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=<idpid> (Get idpid value from Step 9 of PingOne Configuration above)
 - b. Certificate fingerprint = <Certificate Thumbprint of PingOne Certificate> (Open PingOne Signing Certificate downloaded in Step 9 of PingOne Configuration above. Go to Details tab, scroll to the end. Copy and Paste the value of Certificate Thumbprint here)
 - c. Optionally configure **Remote logout URL**.
 - d. Click Save.

Figure 17 Enable SSO for Admin

25	* mt		8	-	۲
0	Chai Facebook Voice Widget mm API	Single sign-on (SSO) Adminu and opents we your 560 service to sign in to your Zendesk. Requires configuration. SAML SAML is an industry standard SSO framework typically used by large enterprises for communicating identities across the internet. Learn more.			
	Mobile SDV www Clarinet Integrations and	SAML SSO URL* https://www.examed.co/ngidenthy.com/amo/dp/SSD.swm/27dpid=86755574/ This is the URL that Zendesk will invoke to redirect users to your identity Provider. Note that our Assertion Consumer Service (ACS) URL https://cloudescurrega.zendesk.com/access/seal/			
	C SUSHESS RULES Thiggins Automations Service Level Agreements new	Certificate lingerprint* 85: 96 as 35 25 44 92 27 42 bc 38 60 ee 74 af db 22 fe 58 13 80 The SHA256 or SHA1 (deprecated) fingerprint of the SAML certificate. Obtain this from your SAML identity provider.			
	SETTRIGE	Remote logout URL https://ppsq-sse.pulsesecureacceuc.net/idma-ne/auth/logout.cgl This is the URL that Zendesk will redirect your users to after they sign out, e.g. https://www.yourcompany.com/services/zendesk_logout.asp			
	Subscription Security Schedule Tickets Agents	IP ranges Requests from these IP ranges will always be routed via remote authentication. Requests from IP addresses outside these ranges will be routed to the normal sign-in form. To route all requests through remote authentication, leave this blank. An IP range is in the format n. n. n. n, where n is a number or an asterisk (*) wild card. Separate multiple IP ranges with a space. Your current IP address is: 182.74,163.90			
dh Ø	Customers Benchmark Survey	JSON Web Token			

 Navigate to Admin (Settings gear at the bottom left corner) -> Security-> End-users. Enable Single sign-on (SSO). All the configurations made in Admin & Agents tab will get populated automatically.

Figure 18 Enable SSO for End-users

Overview	Admins & Agents End women SSL Globel		
O APPS	End-user sign-in authentication		
Marketplace Manoge	By default, your end-users are authenticated and signed in using Zendesk user authentication. You can bypass this and require your end-users to sign in using Google or a single sign-on solution using INT (Team, Professional, and Enterprise) or SAML (Professional and Enterprise).		
C WANNE	Zendetsk Your customers sign is with their Zendesk accounts.		
People	Single sign-on (SSO)		
User #Jelds	Single sign-on (SSO) War cathere se such SSO) while the print a year 2enteest. Requires cardigateden		
Organization Pleids			
Views	98 SAME		
Macros	SAML is an industry standard SSO framework typically used by large enterarises for communicating identities across the internet. Learn more		
Tech			
Ticket Finish	SAMUSSO URL* https://sec.com/entping/dwittp.com/sec/idu/SSC/aa/HZTRIpId/Re/9750/57-64		
Oynumic Content			
	This is the URL that Zendesk will invoke to redirect users to your identity Provider. Note that our Assertion Consumer Service (AC5) URL is https://cloudsecurega.sendesk.com/access/san1/		
CHANNELS	Centificate fingerplint* 89 9# #5 82 44 92 27 42 bc d8 08 ## 74 ef do 22 fe 58 13 89		
cital	The SHA256 or SHA1 (deprecated) fingerprint of the SAML certificate. Obtain this from your SAML identity		
Twittini	ine strats or strat togenetaely ingerprint of the strate, obtain this from your state, obtain this from your state, obtained		
Chill	Remote legiour URL https://porage.sso.puble.se.cures.coms.met/dena-nailauth/logout.cg/		
Pacebook.			
Linese	This is the URL that Zendesk will redirect your users to after they sign out, e.o.		

End-User Flow on Mobile Devices

Once the administrator completes the above configurations and creates a new user in Pulse Workspace, user has to follow the below steps to register the mobile device with Pulse Workspace and get seamless secure Single Sign-On access to Zendesk Application.

- 1. User receives Welcome Mail with registration details.
- 2. Follow the instructions in the mail and register the user device.
- 3. Once registration of mobile device with Pulse Workspace is successful, configured profile will get installed on the device along with VPN certificate.
- 4. Install Zendesk managed application when prompted.
- 5. Install Pulse Client on the mobile device. VPN profile will get configured automatically on Pulse Client.
- 6. Access Zendesk Application and provide the domain details.
- 7. VPN tunnel will automatically get established.
- 8. Single Sign-On will happen and user will get access to the Zendesk domain.

End-User Flow on Desktops

Once the administrator completes the above configurations, user can access Zendesk domain through browser from Windows/MAC OS X Desktops. Follow the below steps to enable Secure Single Sign-On browser-based/thick app based access to Zendesk Cloud Service.

- 1. Launch Pulse Client and establish a VPN session with PCS.
- 2. Open any web browser on the desktop.
- 3. Access SSO enabled Zendesk domain.
 - If user has an existing VPN session, 'Re-use existing Pulse Session' will kick in, PCS will send SAML response to PingOne.
 - If user did not establish Pulse VPN session as mentioned in Step 1, user will be redirected to PingOne which in turn redirects the request to Pulse Connect Secure user login page or user will be prompted to select user certificate for authentication depending on the PCS configuration. Once authenticated, PCS will send SAML response to PingOne.
- 4. PingOne forwards the SAML response to Zendesk and user will be granted access to Zendesk Cloud Service.

Troubleshooting

Single Sign-On for a Zendesk user can fail due to configuration issues on Pulse Connect Secure, PingOne,, Zendesk Service Provider, Pulse Mobile Client or Pulse Workspace. To troubleshoot issues with Single Sign-On:

- On PCS, under Maintenance > Troubleshooting, enable the event codes "saml, auth" at level "50" and collect debug logs. Enable Policy Tracing and capture the Policy traces for the specific user.
- Check System > Log/Monitoring > User Access > Log for SAML AuthNRequest and Response for the specific user. Verify if 'Subject Name' is proper in the SAML Response.
- Log in to PingOne Domain as admin. Navigate to Dashboard-> Reports. Check the notifications to debug the failures.
- On mobile device, open Pulse Client and Send Logs to your administrator.