## How to create MFA policy for PingOne?

To configure the PingOne MFA policy in SanerNow, you need the Environment ID, Client ID, and Authentication Path from your organization's PingOne account. SanerNow supports three authentication methods to verify your identity:

- SMS
- Email
- Authenticate app from PingOne
- 1. Go to Control Panel on the right corner.



## 2. Click on New Policy.

3. Select PingOne from the drop-down. By default, MFA Provider selects PingOne.

Control Panel   All Organizations - Image your multi-factor authentication Policies   Manage your multi-factor authentication Policies   Manage your multi-factor authentication policies   Manage your multi-factor authentication policies   Devices Image   Devices Scanning   Active Directory Sync   Manaal Import   Agents   Agents Configuration   Network Scanner   Summary	New Policy		
All Chranitations • in interventions • in interventions • interventinterventinterventions • interventions • int			
Uters       Image: Comparison of the compari			
Image: Second Secon			
Decovery     Dicovery     Dicovery	Action		
Discovery     Authenticator App       Discovery     Authenticator App       Discovery     Markal Ingot       Agent Discovery Synch     Showing 1 to 1 of 1 entries       Agent Discovery     Description (*)       Other Station     Description (*)       Agent Discovery     Description (*)       Okta     Description (*)       Okta     Description (*)       Okta     Description (*)       Okta     Description (*)			
Device Scaming     Mins I to 1 of 1 entries       Active Directory Sync.     Showing 1 to 1 of 1 entries       Manual Import     Policy Name (*)       Agent Deployment     Description (*)       Agent Configuration     Authentication Path (*)       Network Scanner     Client ID (*)       Summary     Client ID (*)			
Mutual import     PingOne       Agents     Policy Name (1)       Agent Supplyment     Description (1)       Agent Configuration     Authentication Path (2)       Network Scamer     Client (D) (2)       Summary     Client (D) (2)			
Agents     Policy Name (*)     Ping D       Agent Diployment     Description (*)     Otta       Agent Configuration     Authentication Path (*)     Image: Configuration       Network Scanner     Client (D (*)     Image: Client (D (*)	Previous 1 Next		
Agent Deployment     Description (*)     Okta       Agent Configuration     Authentication Path (*)     Image: Configuration       Network Scamer     Client (D (*)     Image: Configuration			
Agent Configuration Authentication Path (*) Authentication Path (*) Client (D (*)			
Authentication Path (*) Network Scanner Summary Client (D (*)			
Summary Client (D (*)			
Scanners			
Scin Configuration Environment (D (*)			
Scan Policy PingOne Username   Login ID Custom			
Posture Anomaly			
Posture Anomaly Scanner Cancel Craste			
Authentication			
Single Sign-On 🙎			
Multi-Factor			
• Settings			

Note: Refer to this document to fetch the details of mandatory fields from the PingOne account:

<u>How to fetch the details of the mandatory fields from the PingOne account? – SecPod –</u> <u>Documentation</u>

- 4. Enter the Policy Name, a unique name to identify the policy.
- 5. Enter the Description about the policy, this is an optional field.
- 6. Enter the Authentication Path from your organization PingOne account.
- 7. Enter the Client ID from your organization PingOne account.
- 8. Enter the Environment ID from your organization PingOne account.

Sanernow All Organizations *								Mon Mar 13 11:34:42	AM (Ö)	👂 🚨 Priyanka Hiremath 🗠		
Control Panel		Multi-F	Factor Authentication	Policies eferences.						D	New Policy	
All Organizations *									Search			
Users	2											
4 Deployment			Name	Multi-Factor Authen	Multi-Factor Authentication Policy			MFA Provider		Action		
Discovery			Authenticator App					Any TOTP Authenticator App				
Device Scanning Active Directory S	ync	Showing 1 to	o 1 of 1 entries	MFA Provider	PingOne *	•					1 Nex	
Manual Import				Policy Name (*)								
Agents Agent Deployment				Description (*)								
Agent Configuratio	n			Authentication Path (*)								
Network Scanner Summary				Client ID (*)								
Scan Configuration				Environment ID (*)								
Scan Policy				PingOne Username	Login ID      Custom							
Posture Anomaly Posture Anomaly S	icanner				c	ancel Cre	ate					
- Authentication	٠				_							
Single Sign-On	2											
Multi-Factor												
<ul> <li>Settings</li> </ul>	*											

9. Select **Login ID** or **Custom**: This option is selected depending on the SanerNow and PingOne username mapping.

- Login ID: Select this option if your PingOne username and SanerNow login ID are identical. By default, this option is selected.
- Custom: Select this option if your PingOne username and SanerNow login ID are different.

## 10. Click on **Create**.

Note: Users need to enter the valid inputs in each field, if invalid inputs are entered it throws an error message as Invalid **Multi-Factor Authentication Input**.

11. Your MFA policy will reflect on 'Multi-Factor Authentication Policies' page.

Now you know how to create MFA policy for PingOne.