Multi-Factor Authentication (MFA) User and Administrator Guide

MAY 11, 2018

Setting up MFA, Logging in to SD-WAN Management Tool, Managing Users
Version 1.0

Proprietary & Confidential
# SD-WAN Management Tool MFA, Login and Managing Users

## Table of Contents

1.0 First Time Accessing SD-WAN Management Tool Portal ................................................................................................................................. 3  
2.0 SD-WAN Management Tool (Multi-Factor Authentication) .......................................................................................................................... 6  
   2.1 Desktop Application Pairing .................................................................................................................................................................. 7  
   2.2 Mobile Application Pairing ............................................................................................................................................................. 11  
   2.3 SMS Text Messaging Pairing ......................................................................................................................................................... 19  
   2.4 YubiKey Hard Token Pairing .......................................................................................................................................................... 22  
3.0 User Login with MFA (Post-PingID Setup) ................................................................................................................................. 25  
   3.1 User Login with MFA .................................................................................................................................................................. 25  
   3.2 Desktop Authentication ............................................................................................................................................................. 27  
   3.3 Mobile Application Authentication ................................................................................................................................................ 28  
   3.4 SMS Messaging Authentication ..................................................................................................................................................... 29  
   3.5 Yubikey Authentication ............................................................................................................................................................. 30  
4.0 Un-pairing Devices ............................................................................................................................................................................. 31  
   4.1 Unpair Desktop Application ......................................................................................................................................................... 32  
   4.2 Unpair Mobile Device ................................................................................................................................................................. 35  
   4.3 Unpair SMS Messaging ............................................................................................................................................................... 37  
   4.4 Unpair Yubikey Hard Token ....................................................................................................................................................... 39  
5.0 Administration User Guide (MyIdentity Portal) ....................................................................................................................... 41  
   5.1 Access MyIdentity Portal ......................................................................................................................................................... 42  
   5.2 Manage Passwords ................................................................................................................................................................. 44  
   5.3 Manage User Access ............................................................................................................................................................... 46  
   5.4 View User ............................................................................................................................................................................... 49  
   5.5 Edit User ................................................................................................................................................................................... 50  
   5.6 Create User ............................................................................................................................................................................... 51  
   5.7 Disable User .............................................................................................................................................................................. 54  
   5.8 Enable User ............................................................................................................................................................................... 56
1.0 First Time Accessing SD-WAN Management Tool Portal

Logging into the SD-WAN Management Tool for the first time. Follow the 4 steps below.

1. Your Account should be registered via the early onboarding email received during the Order process. If further assistance is needed, contact Windstream Customer Care at 800-600-5050.

2. Users will be set up as an ‘Administrator’ or ‘Non-Admin’ with the SDWAN menu selected in the User permissions tree within Windstream Online.

3. Once your Account and User are set up in Windstream Online:
   b. Access the My Sites menu by selecting My Services → SDWAN → My Sites.
4. You are directed to a User Login screen for the SD-WAN Portal. Here you can:
   a. **Log In:** Enter Username and Password.
   b. **Change Password:** Click to change SD-WAN Portal password.
   c. **Forgot Password:** Click to reset forgotten Password.
   d. **Help** Click to access the MFA and User Admin Guide.

*Important!* Your Username and Password for the SD-WAN Portal may or may not be the same as your Windstream Online login credentials. To obtain login credentials for the **myIdentity Portal** and **SD-WAN Management Tool**, follow the User Administration section of this guide.
5. You may be prompted to complete Multi-Factor Authentication (MFA) to access the SD-WAN Management Tool.

User permissions:

- **None**: Default setting, User has no access to the portal.
- **View SD-WAN Monitor**: User can view pages in Monitor area; MFA not required.
- **View SD-WAN Configure**: User can view pages in Configure area; MFA not required.
- **Manage (Limited) SD-WAN Configure**: User has manage/edit capabilities in Business Policy and Firewall areas; MFA is required.
- **Manage (All) SD-WAN Configure**: User has full permissions to manage/edit all SD-WAN features and capabilities; MFA is required.

View Users:

- Enter **USERNAME, PASSWORD** and click **Log In** (Step 4) to be passed directly to the SD-WAN Management Tool.

Manage Users:

- Enter **USERNAME, PASSWORD** and click **Log In** (Step 4).
- Complete initial PingID Setup or Login with MFA using **one** of the MFA options to be passed to the SD-WAN Management Tool.

⚠️ **Note**: Once a User has logged in, they can complete MFA without re-entering their SD-WAN Management Tool Username and Password if returning within 15 minutes of their last login.
To protect Customer critical data, Windstream has added additional security measures to make the SD-WAN Management Tool more secure.

Users with ‘Manage (Limited) SD-WAN Configure’ and ‘Manage (All) SD-WAN Configure’ permissions are required to complete Multi-Factor Authentication (MFA) to access the SD-WAN Management Tool.

Users have multiple options to set up MFA:

For Users not concerned about PCI-DSS compliance, a web client may be installed on the same device you use to login to the SD-WAN Management Tool.

1. **Install PingID app onto desktop.**

   For Users concerned about PCI-DSS Compliance, complete MFA using a device **physically separate** from the device used to log into the SD-WAN Management Tool:

   2. **Install PingID app onto an Apple or Android device.**

   OR

   3. **Receive One-Time Passcode via SMS Text Messaging**

      ✿ **Note:** Messaging rates may apply; limit up to forty (40) MFA codes generated within a 24-hour period, per user.

      OR

   4. **Use a YubiKey 4 Series that supports One Time Passcode (OTP).**
2.1 Desktop Application Pairing

For Users not concerned about PCI-DSS Compliance, install the PingID app directly onto the desktop.

To set up PingID using the Desktop App:

1. Access SD-WAN "My Sites" via Windstream Online.

2. Enter SD-WAN Management Tool USERNAME and PASSWORD, then click Log In.

✏️ Note: For first-time login or if password is unknown, click ‘Forgot Password?’ to complete the Account recovery process and obtain a new password.

3. Click ‘I want to use a different authentication method’.
4. Select ‘Authenticate using the desktop application’ and click Next.

5. Select the appropriate operating system and download the PingID desktop application.

6. Once the PingID Desktop app is installed:
   - Enter the Pairing Key from the pairing screen (Step 5).
   - Click Pair.
7. The PingID app prompts to **Create PIN**. Enter a 4-digit PIN and click **Next**.

   Re-Enter PIN and click **Done**.

8. The PingID passcode appears. Click **Copy**.

9. Return to the **Authentication** screen, paste the passcode and click **Sign On**.
10. An email is sent confirming the new device is added to identity.

11. Once the passcode is accepted, authentication completes and access to the SD-WAN Management Tool is granted.
2.2 Mobile Application Pairing

To set up PingID using an iOS or Android device:

1. Access SD-WAN "My Sites" via Windstream Online.

2. Enter SD-WAN Management Tool **USERNAME** and **PASSWORD**, then click **Log In**.

![Customer Login](image)

- **Note:** For first-time login or if password is unknown, click ‘Forgot Password?’ to complete the Account recovery process and obtain a new password.
3. Prompt to enroll in MFA via the PingID app (available for mobile phones and tablets using iOS or Android) appears.

From desktop browser:
- Enter Email Address accessible from the mobile device.
- Click ‘Get Download Link’.

Note: If the PingID app is already installed on the device, click ‘I already install the PingID app’.

From mobile device:
- Access and open email from PingID.
- Tap the appropriate app service for device.
4. Download the **PingID** app to the mobile device and tap **Open**.

5. PingID ‘**Terms of Service**’ displays. Tap **Accept**.
6. A pop-up informs the user that ‘push notifications’, ‘camera’ and ‘location’ prompts need to be allowed for secure authentication. Tap **I Understand**.

7. Tap **Allow** or **OK** on each pop-up.

8. In the desktop browser, the pairing page displays.
9 Using the mobile device camera, scan the **QR Code** in the desktop browser and PingID automatically begins to verify the mobile device.

If unable to use the mobile device’s camera, click **Enter Pairing Key Manually** on the mobile device and enter the **Pairing Key** located on the pairing page in the desktop browser.

10 A success page displays on the mobile device. The mobile device is now paired with PingID.
11 The ‘Complete Your Profile’ page displays on the mobile device. Add a picture and/or nickname for the PingID profile and tap Done.

느 Note: Personalizing the PingID app helps ensure the sign-on page displayed on the mobile device is intended for the correct user.

12 On the mobile device, the PingID swipe mechanism displays. Move the slider Up to sign in.
13 A confirmation displays on the mobile device. Tap the ‘X’ in the upper right corner to close the message.

14 An email is sent confirming the new device is added to identity.
The mobile device is now ready for MFA. The services paired to the device (Windstream Online) and a one-time passcode display.

**Note:** If direct communication (swipe to MFA) between the PingID app and PingID service cannot be completed (i.e. device is on airplane mode), the PingID app automatically switches to offline authentication. Use this passcode once (1x) to MFA.

Allow the PingID app to run in the background for continuous authentication or a notification is received.

Going forward, when using the mobile device for MFA, an authentication request message from PingID service automatically displays on the paired device.

Once the passcode is accepted, authentication completes and access to the SD-WAN Management Tool is granted.
2.3. SMS Text Messaging Pairing

Windstream allows Users to receive one-time passcodes via SMS Text Message to enable MFA.

用水
- Messaging rates may apply.
- Limit up-to 40 passcodes generated within a 24hr period, per user.

Notes:

To setup PingID via an SMS Text Message:

1. Access SD-WAN "My Sites" via Windstream Online.

2. Enter SD-WAN Management Tool USERNAME and PASSWORD, then click Log In.

3. Click 'I want to use a different authentication method'.
4 A prompt to pair a device using an alternative method displays.

- Select **Receive passcodes via SMS**.
- Enter your mobile **phone number**.
- Click **Next**.

5 Retrieve the **PingID authentication code** from the SMS Text Message.

Ề Note: The originating number of the SMS message may vary due to factors such as, but not limited to: network carrier, device, server availability and location.

6 Enter the one-time passcode and click **Verify**.

Ề Notes:
- Click **Edit** to change the phone number.
- Click **Resend passcode** to resend the SMS message.
7 An email is sent confirming the new device is added to identity.

8 Once the passcode is accepted, authentication completes access to the SD-WAN Management Tool is granted.
2.4 YubiKey Hard Token Pairing

To complete MFA to the SD-WAN Management Tool, Users who do not wish to use their personal mobile device can set up PingID using a YubiKey hard token.

If the User chooses to use a YubiKey, they must purchase a YubiKey 4 series that supports One-Time Passcode (OTP). YubiKeys are available via the manufacturer’s website or other electronics retailers.

To set up PingID using a YubiKey Hard Token:

1. Access SD-WAN "My Sites" via Windstream Online.

2. Enter SD-WAN Management Tool USERNAME and PASSWORD, then click Log In.

3. Click ‘I want to use a different authentication method’.

Note: For first-time login or if password is unknown, click ‘Forgot Password?’ to complete the Account recovery process and obtain a new password.
4. A prompt to pair a device using an alternative method displays. Select **Authenticate with YubiKey** and click **Next**.

![Alternative Authentication](image)

5. Insert the YubiKey (Hard Token) into desktop/laptop and press down on the YubiKey to get a verification code and click **Verify**.

![YubiKey Setup](image)

6. A confirmation displays in the desktop browser.

![Authenticated](image)
7. An email is sent confirming the new device is added to identity.

8. Once the YubiKey code is accepted, authentication completes and access to the SD-WAN Management Tool is granted.
3.0 User Login with MFA (Post-PingID Setup)

For Users with ‘Manage’ access to the SD-WAN Portal, MFA is needed to access their Sites. Users must first complete the steps above in section 2.0 to setup the PingID using Mobile App, SMS Messaging, YubiKey or Desktop App.

3.1 User Login with MFA

Once PingID enrollment is complete, use these steps to access the SD-WAN Portal:

1. Access SD-WAN "My Sites" via Windstream Online.

2. Enter SD-WAN Management Tool USERNAME, PASSWORD and click Log In.

3. Prompt for MFA via PingID displays for Users with ‘Manage’ permissions.
   - Complete Authentication with MFA using the option chosen upon pairing to PingID.
   - If a new authentication option is needed, setup PingID.

 demás: If password is unknown, click ‘Forgot Password?’ to complete the Account recovery process and obtain a new password.
4. User is directed to the SD-WAN Management Tool.

Note: Once a User has logged in, they can complete MFA without re-entering their SD-WAN Management Tool Username and Password if returning within 15 minutes of their last login.

Authentication with MFA (Post-PingID Setup)

Once a device is paired to PingID, it is remembered on the User’s identity.

Note: Users can have up-to two devices paired to their PingIdentity at one time.

Select an option to view the authentication steps after PingID is set up:

- Desktop App Authentication
- Mobile App Authentication
- SMS Messaging Authentication
- YubiKey Authentication
3.2 Desktop Authentication – Web Client

To authenticate with a paired Desktop App:

1. Complete Steps in 3.1 for User Login with MFA.

2. In the browser, **Authenticating with Desktop** displays.

3. From the Desktop shortcut or Start Menu, launch the **PingID Desktop App**.

4. Enter your **PIN** and click **Next**.

5. **Copy** passcode from the Desktop App Authentication screen in the browser and click **Sign On**

6. **Authenticated** confirmation displays and the SD-WAN Management Tool is accessed.
3.3 Mobile Application Authentication

To authenticate with a paired iOS or Android device:

1. Complete Steps in 3.1 above for User Login with MFA.

2. In the browser, Authenticating on [mobile device name] displays.

3. A push notification appears on the mobile device. **Swipe** to open PingID app.

4. Slide the swipe mechanism **Up**.

5. **Authenticated** appears on in the app/browser and the SD-WAN Management Tool is accessed.
3.4 SMS Messaging Authentication

To authenticate with a paired SMS device:

1. Complete Steps in 3.1 above User Login with MFA.

2. In the browser, Authentication screen displays.

3. Access the device with SMS messaging and retrieve the passcode.

4. Enter the passcode in the browser Authentication page and click Sign On.

5. Authenticated appears on in the browser and the SD-WAN Management Tool is accessed.
3.5 Yubikey Authentication

To authenticate with a paired YubiKey Hard Token:

1. Complete Steps in 3.1 above for User Login with MFA.

2. **Yubikey Authentication** displays. **Insert the YubiKey** and **press the button** to authenticate.

3. **Authenticated** appears on in the browser and the SD-WAN Management Tool is accessed.
4.0 Un-pairing Devices

Only 2 active pairings are permitted per user so if a third pairing is required, then one of the original two pairings must be un-paired. If a user no longer has change control permissions within the SD-WAN, it is recommended that they un-pair previously paired devices.

Users are able to un-pair a device to remove it from their PingIdentity.

- Unpair Desktop Application
- Unpair Mobile Device
- Unpair SMS Messaging
- Unpair YubiKey Hard Token

Notes:
- For issues unpairing a device or you no longer have the device, contact Customer Care at 800-600-5050 to have the device unpaired.
- Once the device is unpaired, on the next login attempt, the PingID authenticator prompts to pair a device. After pairing, the User is authenticated into SD-WAN Management Tool.
4.1 Unpair Desktop Application – Web Client

1. Complete Steps 1-2 in 3.1 for User Login with MFA but do not authenticate.

2. From the Authentication screen, click **Settings**.

3. Click the **down arrow** next to the device(s) you wish to unpair.

4. A pop-up displays that you must authenticate via PingID to unpair the device(s). Click **Continue**.

5. **Authentication with Desktop** displays. Enter the passcode from the PingID Desktop App. (Step 6) and click **Sign On**.
6. To retrieve a passcode:

Launch the PingID Desktop App from Start Menu or Desktop shortcut.

Enter Desktop App PIN and click Next.

→ Copy passcode to Authentication screen in the browser and Sign On (Step 5).

7. Authenticated appears on the screen.

8. Click the down arrow on the device(s) and click the Trash Bin icon to remove the device.
9. A pop-up asks to confirm device removal. Click Remove.

10. The device is removed from the list.

Note: A new device can be added from this screen by clicking Add or by pairing a new device.
4.2 Unpair Mobile Device

1. Complete Steps 1-2 in 3.1 for User Login with MFA but do not authenticate.

2. From the Authentication screen, click **Settings**.

3. Click the **down arrow** next to the device(s) you wish to unpair.

4. A pop-up displays that you must authenticate via **PingID** to unpair the device(s). Click **Continue**.

5. A prompt for authentication displays on the mobile device. **Swipe to open** the PingID App.

![Swipe Up](image)

7. **Authenticated** appears in the App and Desktop browser.

![Authenticated](image)

(Desktop) (Mobile)

8. Click the **down arrow** on the device(s) and click the **Trash Bin** icon to remove the device.

![Trash Bin](image)

9. A pop-up asks to confirm device removal. Click **Remove**.

![Remove Device](image)

10. The device is removed from the list.

![Removed Device](image)

☞ **Note:** A new device can be added from this screen by clicking **Add** or by pairing a new device.
4.3 Unpair SMS Messaging

1. Complete Steps 1-2 in 3.1 for User Login with MFA but **do not** authenticate.

2. From the Authentication screen, click **Settings**.

3. Click the **down arrow** next to the device(s) you wish to unpair.

4. A pop-up displays that you must authenticate via **PingID** to unpair the device(s). Click **Continue**.

5. SMS Authentication displays. Enter the received in the SMS Message and click **Sign On**.
6. **Authenticated** appears on the screen.

7. Click the **down arrow** on the device(s) and click the **Trash Bin** icon to remove the device.

8. A pop-up asks to confirm device removal. Click **Remove**.

9. The device is removed from the list.

☞ **Note:** A new device can be added from this screen by clicking **Add** or by pairing a new device.
4.4 Unpair YubiKey Hard Token

1. Complete Steps 1-2 in 3.1 for User Login with MFA but **do not** authenticate.

2. From the Authentication screen, click **Settings**.

3. Click the **down arrow** next to the device(s) you wish to unpair.

4. A pop-up displays that you must authenticate via **PingID** to unpair the device(s). Click **Continue**.
5. **Yubikey Authentication** displays. **Insert the YubiKey** and **press the button** to authenticate.

![Yubikey Authentication display](image)

6. **Authenticated** appears on the screen.

![Authenticated screen](image)

7. Click the **down arrow** on the device(s) and click the **Trash Bin** icon to remove the device.

![Device removal](image)

8. A pop-up asks to confirm device removal. Click **Remove**.

![Remove device](image)

9. The device is removed from the list.

![Device removed](image)

*Note: A new device can be added from this screen by clicking **Add** or by pairing a new device.*
5.0 Administration User Guide (myIdentity Portal)

Effective 5/11/2018, all existing SD-WAN Customer login and password information has been moved from Windstream Online to the MyIdentity Portal. For New and Existing SD-WAN Customers who need access to the SD-WAN Management Tool, Global Account Admins and Windstream Enterprise employees can assist with user administration in the MyIdentity Portal.

Note: A ‘Global Account Admin’ User Identity is created for the “Primary Authorizing Contact” listed on the install Order during Early Onboarding. Additional Admins can be created through the MyIdentity Portal as needed.
5.1 Access MyIdentity Portal

1. - Access Account in Windstream Online.
   - Select My Services → SDWAN → Administer Users.

   - Enter SD-WAN Management Tool **USERNAME**, **PASSWORD** and click **Log In**.
2. The MyIdentity Portal dashboard displays.

**Global Account Admins**

From the MyIdentity Portal, Global Account Admins can:

- Manage Passwords
- Manage User Access
- View User
- Edit User
- Create User
- Disable User
- Enable User

**Non-Admins:**

Non-Admin only have limited options to manage their own User Identity MyIdentity including:

- Manage Passwords
- Manage My Access
- View User
- Edit User

*Note: User search steps are skipped for Non-Admin Users since they can only manage their own User Identity.*
5.2 Manage Passwords

Manage Passwords allows Admins to change a password for a User Identity. User passwords expire after 90 days. An email is sent to the User daily in the 10 days prior to password expiration.

Once the password is changed, an additional email is sent to the User confirming the change.

Note: Users can update their password by clicking the ‘Forgot Password’ link on the login screen.

To Manage Passwords:

1. Access the MyIdentity Portal.

2. From the MyIdentity Portal dashboard, click Manage Passwords.

Search Identities to locate the User and click Manage

Notes:
- You can search by Name, Login ID or Email; partial searches are allowed.
- This step is skipped for Non-Admins since they can only manage their own User Identity.
3. Password(s) details display. Click **Change**.

3. Enter **New Password**, **Confirm Password** and click **Submit**.

**Note:** Click the **Password Constraints** info view the password policy.

4. The request processes and **Action Status** updates to ‘Completed’.
5.3 Manage User Access

Manage User Access allows Admins to add, modify and remove SD-WAN Management Tool permissions to a User Identity.

To Manage User Access:

1. Access the MyIdentity Portal.

2. From the MyIdentity Portal dashboard, click Manage User Access.

3. - Use the Search Users tab to locate the User.
   - Click the ✔ to select User.
   - Select the Manage Access tab.

**Notes:**
- You can search by Name, Login ID or Email; partial searches are allowed. More than one User can be selected and managed at a time.
- This step is skipped for Non-Admins since they can only manage their own User Identity.
4. Select a tab and modify User Access as needed:
   a. **Add Access** Tab – select the ✔ on the permission to add to User’s access.
   b. **Remove Access** Tab – click the x on the existing user permissions to remove from User’s access.

   ![Image of Manage User Access screen]

   **Note:** User permissions can be added and removed (modified) in the same step.

5. Select the **Review** tab to confirm changes. Click **Submit** to process or **Cancel** to revert changes.

   ![Image of Manage User Access screen with Add Access and Remove Access options]

6. The change is processed and a confirmation message displays when changes are complete.

   ![Image of successful message]

   ![NAVIGATION BAR WITH SECTIONS]
7. Customer also receive an email notification with permission changes.

**View Users:**

```
Dear Steven Samick,
The following permissions have been added to your account.
SD-WAN - View Monitoring
Thank You,
myidentity@Windstream
```

**Manage Users:**

```
Dear User,
The following permissions have been added to your account.
SD-WAN - Modify Full Configure **
** These permissions require you to allow Multi-Factor Authentication (MFA). For instructions regarding MFA, please see MFA.
Thank You,
myidentity@Windstream
```
5.4 View User

View User displays the User Identity details.

To View User:

1. **Access the MyIdentity Portal.**

2. From the MyIdentity Portal dashboard, click **View User.**

3. **Search Identities** to locate the User and click **Manage.**

   ![Image of MyIdentity Portal dashboard with View User option highlighted.](image)

**Notes:**
- You can search by Name, Login ID or Email; partial searches are allowed.
- This step is skipped for Non-Admins since they can only manage their own User Identity.

4 **Identity Details** display.

   ![Image of Identity Details showing attributes of the user.](image)

**Note:** The sidebar menu can be used to **Manage:** Edit Identity, Access or Passwords.
5.5 Edit User

Edit User allows Admins to edit a User Identity.  

⚠️ **Note:** The Global Account ID cannot be edited by Admins on an existing User Identity. To have the Global Account ID updated, contact Customer Care at 800-600-5050.

To Edit User:

1. **Access the MyIdentity Portal.**

2. From the MyIdentity Portal dashboard, click **Edit User.**

3. **Search Identities** to locate the User and click **Manage.**

    ![Edit User Interface](image)

**Notes:**
- You can search by Name, Login ID or Email; partial searches are allowed.
- This step is skipped for Non-Admins since they can only manage their own User Identity.

4. **Update User** details as needed and click **Submit.**

![User Details](image)

⚠️ **Note:** Non-Admins are not able to select the **Global Account Admin** checkbox; this can only be modified by an Admin.
5. The change processes and a confirmation message displays when changes are complete.

5.6 Create User

Create User allows Global Account Admins to add and remove User Identities. Once an Identity is created, User Access can be added to the Identity.

--- Note: This option is not available for Non-Admins.

To Create a User

1. **Access the MyIdentity Portal.**

2. From the MyIdentity Portal dashboard, click **Create User.**

3. Complete the **Create Identity** form and click **Submit.**
   a. **Login ID:** required field. Username to log into the SD-WAN Management Tool; this can be the email address.
   b. **First Name:** required field.
   c. **Last Name:** required field.
   d. **Email:** required field.
   e. **Phone Number:** optional field.
   f. **Mobile Phone Number:** optional field.
   g. **Is Global Account Admin:** optional field. Select checkbox to designate the User as a Global Account Admin who can add, modify or remove other SD-WAN Management Tool Users.
   h. **Global Account Id:** completed by Windstream, not editable by the User. For assistance, contact Customer Care at 800-600-5050.
   i. **Unique ID & User Type:** These fields are locked and automatically completed by the system.
<table>
<thead>
<tr>
<th>Input Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create User</td>
<td>If you would like to create a new user, please fill in the fields below.</td>
</tr>
<tr>
<td>Username</td>
<td>First Name **</td>
</tr>
<tr>
<td>Email</td>
<td>Last Name **</td>
</tr>
<tr>
<td>Phone Number</td>
<td>Mobile Phone Number</td>
</tr>
<tr>
<td>Password</td>
<td>Security Questions</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>User Type</td>
</tr>
<tr>
<td>User Notes</td>
<td>🍃</td>
</tr>
</tbody>
</table>
4. Request processes and a confirmation displays.

5. The Customer receives an email confirming ‘New Account Created’.

   a. Login ID
   b. User Name
   c. Email
   d. Password Link: Temporary link allows the User the set their SD-WAN Management Tool password.

Test User,

Your account for Windstream myIdentity has been created.

Login ID: testuser20180501a
Email: testuser20180501a@test.com

To set your password [click here]

Thank You,

myIdentity@Windstream
5.7 Disable User

Disable User terminates the User Identity and all assigned permissions.

☞ Note: This option is not available for Non-Admins.

To Disable a User:

1. Access the MyIdentity Portal.

2. From the MyIdentity Portal dashboard, click Disable User.

3. Filter by Identity Name or use the Advanced Search to locate the User. Select the User by clicking on the row.

4. 'Are you sure you want to disable user?' displays. Click Submit to process the request or Cancel to revert.

5. 'Disable User request submitted'. If needed, click Return to Dashboard to continue User Management.
<table>
<thead>
<tr>
<th>Disable User request submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return to Dashboard</td>
</tr>
</tbody>
</table>
5.8 Enable User

Enable User reinstates Identity and previously assigned privileges.

Note: This option is not available for Non-Admins.

To Enable User:

1. Access the MyIdentity Portal.

2. From the MyIdentity Portal dashboard, click Enable User.

3. Filter by Identity Name or use the Advanced Search to locate the User. Select the User by clicking on the row.

4. ‘Are you sure you want to enable user?’ displays. Click Submit to process the request or Cancel to revert.
5. ‘Enable User request submitted’. In needed, click Return to Dashboard to continue User Management.