

Purpose:

The purpose of this document is to provide greater clarity on configuring a StrideLinux company with the advanced user management features. This document uses an OEM/Machine/System Builder type business as an example with key information for their employee and customer users of the VPN routers in the systems they supply. For a general understanding of advanced user management, this [video](#) provides a quick overview highlighting the capabilities and configuration options.

Table of Contents

Steps to Configure the Use Case	2
Groups.....	3
Access Category.....	3
Roles	4
User	5
Device	5
Tying Things Together Part 1 – Devices to Groups	6
Tying Things Together Part 2 – Services and Licenses	7
Appendix A – Glossary.....	13

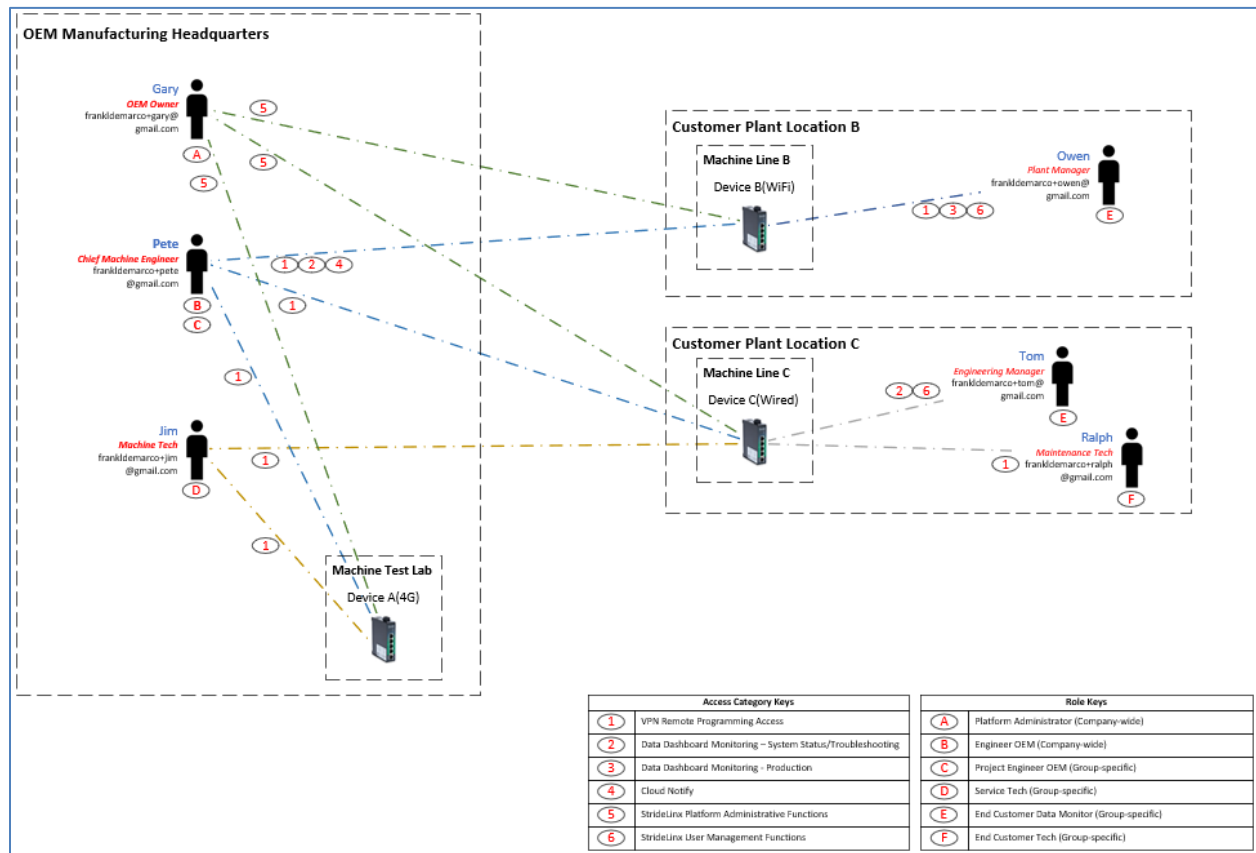
(Control-click on the above page numbers to jump to that section)

Glossary:

See [Appendix A](#) for a list of [terms](#) related to the VPN Cloud User Management.

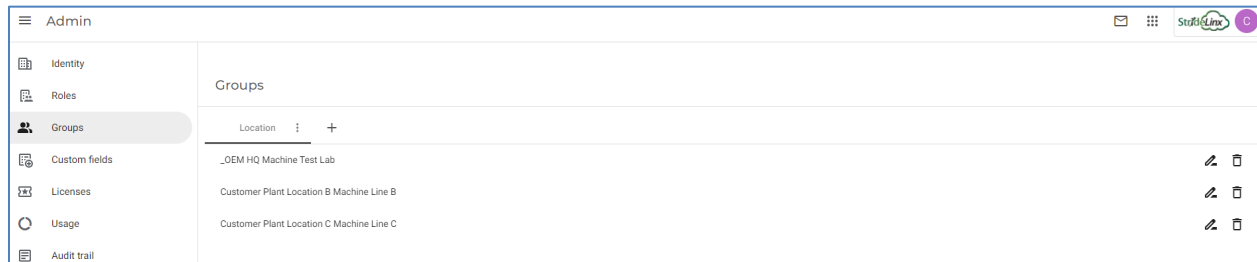
Steps to Configure the Use Case

This Use Case shows an OEM Manufacturing HQ along with two(2) of their customer locations:



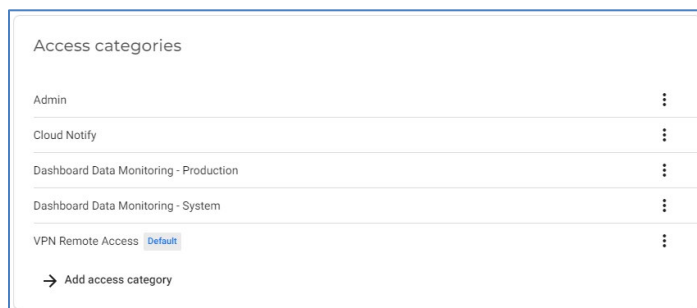
Groups

First, create placeholders in the **Admin app** called **Groups** which are a selection of devices and users. You can divide groups into different group types. For this Use Case, the Group type is named **Location**. Groups are shown in the Use Case are listed as OEM HQ Test Lab, Customer Plant Location B Machine Line B and Customer Plant Location C Machine Line C:



Access Category














Access Category is the mechanism to give permission to **Users** to view **Pages** (dashboards) and **Services** (VPN, HTTP, VNC). With the above Use Case as a model, under the **Admin app**, select **Roles**, and add **Access Categories** (names are created here – category usage is shown later):



Note: one way to name these categories is based on anticipated usage of the services that are available in the platform. But it is not necessary to create an admin access category because an administrator role is given access to all Access Categories. In addition, each service or page can only be assigned to one access category so assigning them to the admin access category will not allow them to be assigned to another access category.

Roles

Roles determine what permissions a particular **User** will have in the StrideLinux Cloud platform. There are **Company-wide** and **Group-specific** roles. Again, using the Use Case as a model, add new **Role** placeholders by selecting **Admin, Roles → Add role**:

Roles			
Name	Type	Access category	
Customer Engineering Manager	Group/Device-specific	Dashboard Data Monitoring - System	 
Customer Maintenance Tech	Group/Device-specific	VPN Remote Access	 
Customer Plant Manager	Group/Device-specific	Dashboard Data Monitoring - Production, VPN Remote Access	 
OEM Engineer	Company-wide	Cloud Notify, Dashboard Data Monitoring - System +1	 
OEM Owner 	Company-wide	-	 
OEM Tech	Group/Device-specific	VPN Remote Access	 
→ Add role			

Each role must have a name, Company-wide or Group-specific scope, and ADMIN/DEVICES/LOG IN permissions associated with that role. To create an admin for a specific group, ADMIN → Manage users can be selected allowing the user to invite additional users with the access permissions up to the same level. The Devices permissions point to the previously created Access Categories. Example:

Edit role

Name *
Customer Engineering Manager

CREATED AS
Group-specific or Device-specific role
User has limited access, only to a specific group or a specific device

ADMIN
Manage users ⓘ ☒

DEVICES
Configure devices ☐
Services, pages and notifications linked to - Admin ☐
Services, pages and notifications linked to - Cloud Notify ☐
Services, pages and notifications linked to - Dashboard Data Monitoring - Production ☐
Services, pages and notifications linked to - Dashboard Data Monitoring - System ☒
Services, pages and notifications linked to - VPN Remote Access ☐

LOG IN
Enforce two-factor authentication ⓘ ☐

Cancel Confirm

User

The most basic entity that can participate in the platform is the **User**. To add them, go to the **Portal** app, **Users**, **Invite Users**:

Name	E-mail address	Last active	Roles	Two-factor authentication
Company Owner	frankdemarco@gmail.com	15 minutes ago	OEM Owner	Off
Gary G	frankdemarco@garyg@gmail.com	—	OEM Owner	Off
Jim J	frankdemarco@jimj@gmail.com	—	OEM Tech at OEM HQ Machine Test Lab	Off
Owen O	frankdemarco@owen@gmail.com	—	Customer Plant Manager at Customer Plant Location B Machine Line B	Off
Pete P	frankdemarco@petep@gmail.com	—	OEM Engineer	Off
Ralph R	frankdemarco@ralphr@gmail.com	—	Customer Maintenance Tech at Customer Plant Location C Machine Line C	Off
Tom T	frankdemarco@tomt@gmail.com	—	Customer Engineering Manager at Customer Plant Location C Machine Line C	Off

Enter the e-mail address of the User you want to invite, along with an invitation message. **Company-wide**, **Group-specific**, and **Device-specific** users can be added to provide access to all users and devices in the company, a group of specific devices and users, or only one device:

Invite users

Enter e-mail addresses...

Invitation message

Access level: ☒ Company-wide ☐ Group-specific

Role: [dropdown]

Cancel Send Invite

Invite users

Enter e-mail addresses...

Invitation message

Access level: ☐ Company-wide ☒ Group-specific

Group: [dropdown] Role: [dropdown]

+ Add another role

Cancel Send Invite

Temporary users can also be invited – you can set an end date to which access will expire. Group-specific **Access levels and Roles** need to be configured beforehand so you can select them as required. After filling out the fields, a **Send Invite** button will appear that will send an invite to the user to join the company. **Users** will need to follow the email instructions to join. After a User has accepted the invitation, they may be given multiple roles as shown in the above Use Case.

Device

The most common way to add **Devices** to the platform is using the configuration tool under **Tools** in the **Fleet Manager** app. This [article](#) provides instructions to configure a router by USB flash drive or there are [videos](#) on the AutomationDirect.com webstore. Or, if you have routers in other companies you want to use, you'll need to [transfer](#) them.

For this use case, the devices are listed below:

Devices						
Status	Name ↑	Last online	Serial number	MAC address	Firmware version	
●	Customer Plant Location B [DEV B]	Now	17086998	C0:D3:91:31:E3:19	3.20.1	Connect
●	Customer Plant Location C [DEV C]	Now	17074991	C0:D3:91:31:60:25	3.20.1	Connect
●	OEM Headquarters [DEV A]	Now	17088834	C0:D3:91:31:F6:D5	3.20.1	Connect

Tying Things Together Part 1 – Devices to Groups

There are several components that need to be configured for the devices in your company. The **Group** that the device belongs to can be set up/confirmed in the **Fleet Manager** app. Add devices to **Groups** created previously (*to allow visibility for those users with group specific roles*). Select **Fleet Manager**, **Devices**, select an individual device, and select **Info**. Under Groups, select a Group name for each device. Assure each device is assigned to the correct Group. For instance, Device A belongs in Group **OEM Headquarters Machine Test Lab**:

General

Name

OEM Headquarters [DEV A]

Edit

Description

4G Router at Machine Test Lab

Edit

Location

–

Edit

Groups

Location

_OEM HQ Machine Test Lab




Edit

Once the group has been assigned, the **Role** definitions for that group are listed for each user. Individual services for the device must still be assigned (following), but this provides the maximum list of users with access to the router:

Access		
Name	Role	
Company Owner	OEM Owner	
Gary G	OEM Owner	
Jim J	OEM Tech at _OEM HQ Machine Test Lab	
Pete P	OEM Engineer	

Tying Things Together Part 2 – Services and Licenses

Define the features for each device in the company and assign the pages and services to the appropriate **Access Category**. For the devices of this Use Case as reference, the following features are defined:

SERVICES/LICENSES		DEVICES			
		OEM Machine Test Lab Device A(4G) 	Customer Plant Location B Device B(WiFi) 	Customer Plant Location C Device C(Wired) 	
ACCESS CODES		FEATURE ENABLED			CONFIGURATION DETAILS
1	VPN Remote Programming Access	YES	YES	YES	This Service is given to a Device with Access Category: VPN Remote Access. Admin Roles have VPN Remote Access by default.
2	Data Dashboard Monitoring – Machine/Process Health Status	YES	YES	YES	For data resident in a PLC - set up by: (a) adding Cloud Logging License to Device, (b) adding a Modbus Data Source, and adding Variables with proper address pointing to discrete and numeric data to be displayed. Use Studio to create pages with data in question.
3	Data Dashboard Monitoring – Production Status		YES		Same a #2 above but with data centered in production information rather than health monitoring.
4	Cloud Notify		YES		For data resident in a PLC - set up by: (a) adding Cloud Notify License to Device, (b) adding a Modbus Data Source, and adding Variables with proper address pointing to discrete and numeric data to be alarmed. Then configure Alarm Triggers for those Variables that require alarming.
5	StrideLinux Platform Administrative Functions	YES			Name of a Company-wide Role assigned to User – not strictly an Access Code.
6	StrideLinux User Management Functions		YES		ADMIN service given Users with Roles: Customer Monitor(Data and Platform Admin

To assign each device's services or pages to an Access Category, go to the **Fleet Manager** app, **Devices**, and select a Device. For OEM Headquarters (OEM Test Lab) Device A, assign "VPN Connect" under SERVICES to the **VPN Remote Access** Access category:

VPN connect

Access category *

VPN Remote Access

Note: a user with manage devices or configure devices rights is able to set up a VPN connection without having access to the access category selected above.

Confirm changes

Access

Name

Role

Jim J

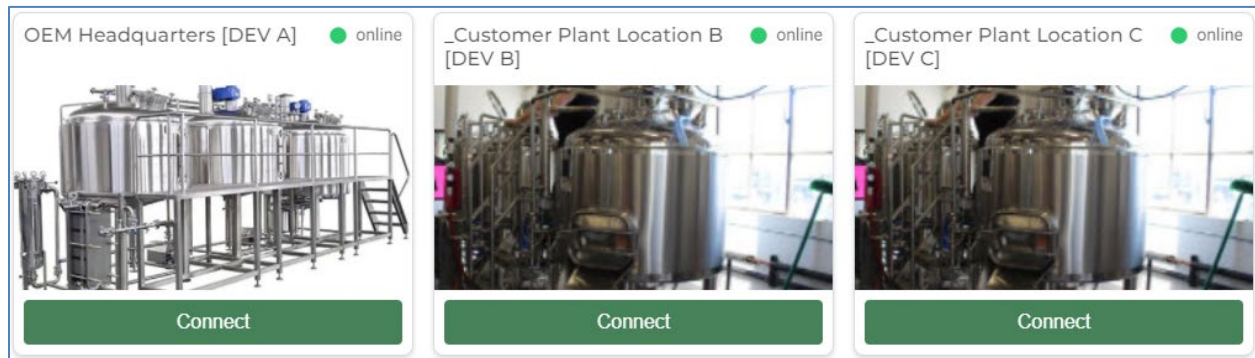
OEM Tech at _OEM HQ Machine Test Lab

Pete P

OEM Engineer

Additional services (HTTP, VNC, Websocket Server) can be added and assigned to an access category under SERVICES for that router.

VPN connection to the devices is shown on the **Portal** page under **Devices**(shown here with newly created **Cards** for this Company):



The devices for these companies (businesses) are set up as follows:

Device A 4G VPN LAN: X.X.X.6 (Test Lab)	Device B WiFi VPN LAN: X.X.X.7 (Location B)	Device C Wired VPN LAN: X.X.X.7 (Location C)
PLC: P1-540 LAN:X.X.X.30	PLC: P2-550 LAN:X.X.X.35	PLC: BRX LAN:X.X.X.60
Cloud Logging: n/a Cloud Notify: ZZZ-ZZZ-ZZZ-ZZZ(not used)	Cloud Logging: ZZZ-ZZZ-ZZZ-ZZZ Cloud Notify: trial	Cloud Logging: trial Cloud Notify: n/a

For Device B (WiFi), the previous chart (in Page 7) lists **Dashboard Data Monitoring** and **Cloud Notify**, configured here in **Fleet Manager** by purchasing and assigning license numbers, purchased from AutomationDirect.com, or by starting a free trial, if desired:

Cloud Logging
Gain insight into your machines with reports and live dashboards.

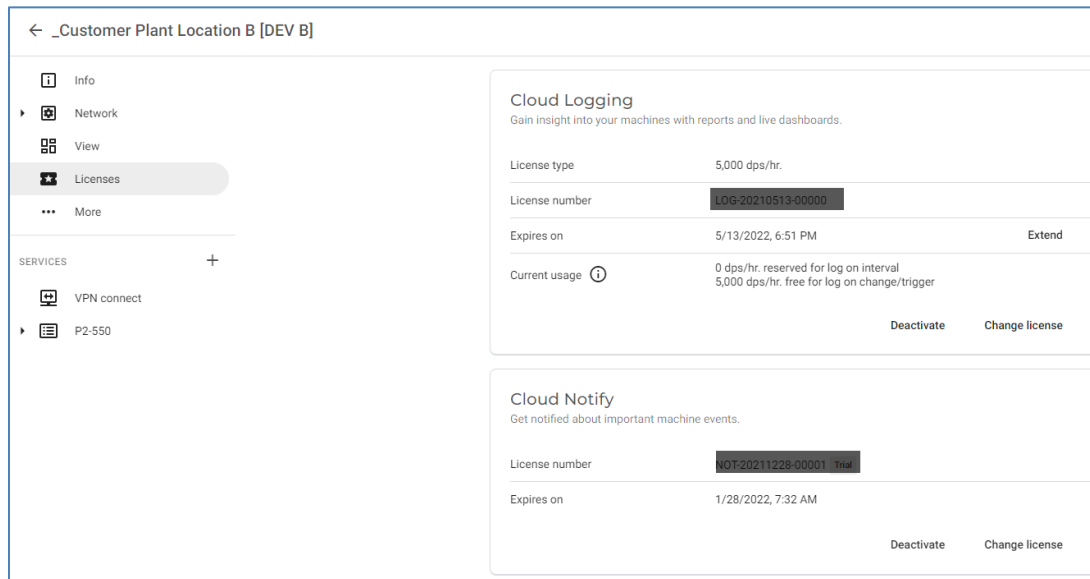
Free trial

Activate

Cloud Notify
Get notified about important machine events.

Free trial

Activate



Note: license numbers would normally appear in blacked out boxes.

Both of these licensed services require a **Data source** (usually from a PLC) to supply the discrete or numeric data called **Variables**. For Device B (WiFi), the following information is shown as an example:

WiFi VPN LAN Location B
PLC: P2-550 LAN:X.X.X.35
Protocol: Modbus
Variables: Clock Hours – 300101 (16bit Int) Clock Minutes – 300102 (16bit Int) Clock Seconds – 300103 (16bit Int) Water Pressure – 400101 & 2 (32bit float) Water Temperature – 400103 & 4 (32bit float)

One Variable for Device B (WiFi) using **Modbus protocol** is shown below as the Data source:

Data source
Modbus

Name *
P2-550

Identifier *
P2-550

IP address
35

Port *
502

Slave
1

Byte order *
CDAB

Polling sleep time
None

Remove
Confirm changes

For **Dashboard Data Monitoring**, the following **Variables** are created corresponding to tags in the AutomationDirect.com Productivity PLC P2-550 PLC:

Variables							Run test	Stop test	Export to CSV-file	Import from CSV-file
+ Add a filter										
<input type="checkbox"/>	Name ↑	Identifier	Type	Address	Factor	Unit	Latest value			
<input type="checkbox"/>	Clock_Hours	clock-hours	Int16	4.100	1	hr.	–		Edit	Remove
<input type="checkbox"/>	Clock_Minutes	clock-minutes	Int16	4.101	1	min.	–		Edit	Remove
<input type="checkbox"/>	Clock_Seconds	clock-seconds	Int16	4.102	1	sec.	–		Edit	Remove
<input type="checkbox"/>	Water_Pressure	water-pressure	Float32	3.100	1	PSIG	–		Edit	Remove
<input type="checkbox"/>	Water_Temperature	water-temperature	Float32	3.102	1	DEG F	–		Edit	Remove

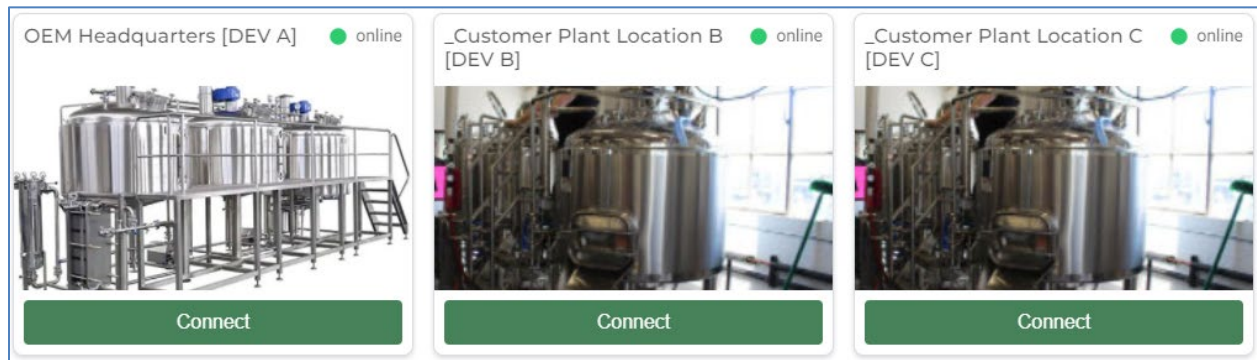
Word of Caution: the “Address” shown above is somewhat unique, requiring attention and consisting of a **[Modbus function code].[Register Offset]**. Examples for the above Modbus addresses:

Clock_Hours: VPN Address – 4.100 = Mod Start – 300101

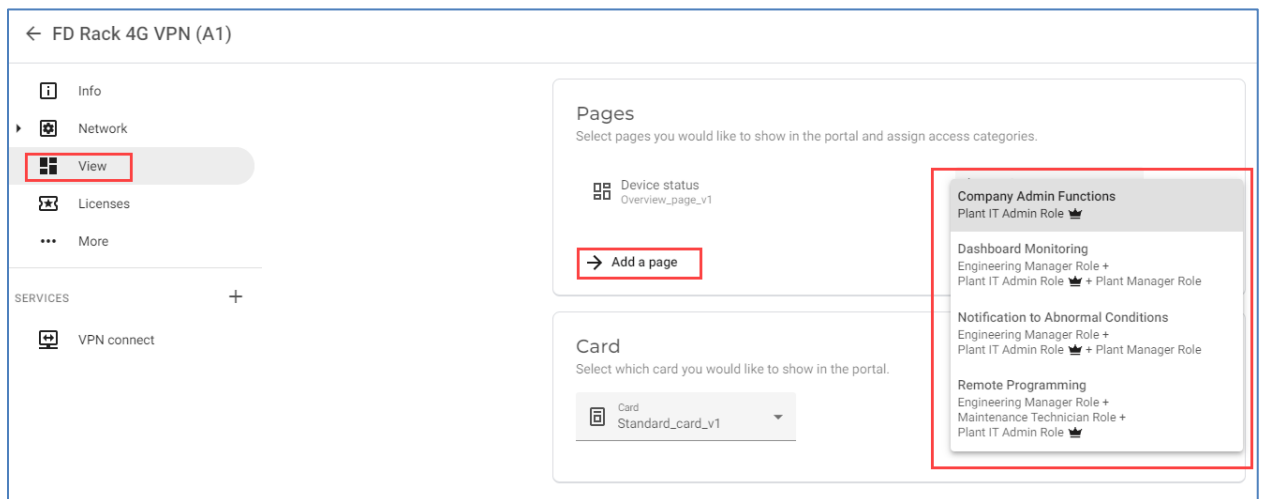
Water_Pressure: VPN Address – 3.100 = Mod Start – 400101

This data could show up on a **Component** on a **Page** or **Card** created with the **Studio App**. How to edit pages is shown here: <https://support.stridelinx.com/hc/en-us/articles/360019030317-How-to-edit-pages-> How to edit cards is shown here: <https://support.stridelinx.com/hc/en-us/articles/360019029817-How-to-edit-cards->

An example of custom **Cards** created for this Use Case, opening the **Portal** page shows the 3 **Devices** below (shown previously):



To link **Access Categories** to **Pages**, select **Fleet Manager**, **Devices** and select the device in question then Select **View**, then **Add a Page**, and select **Access category** :



Custom **Pages** can be created for each device in the platform. And a default Status **Page** exists similar to this:

The screenshot displays the 'Device status' page for 'OEM Headquarters [DEV A]'. The interface includes a navigation bar at the top with a back arrow and a star icon. The main content area is divided into several sections:

- Device status**: A header section with a green smiley face icon and a welcome message: 'Welcome to StrideLinux. StrideLinux is all about collaboration with one goal: to create most value out of IoT. For any help visit our [support page](#)'.
- Cloud connection status**: A section with tabs for 'Status', 'Logbook', and 'VPN data usage'. It shows three connection statuses: 'VPN connection' (NE01), 'Configuration connection' (AM02), and 'Data logging connection' (AM02).
- VPN**: A section with a progress bar and a 'Connect' button.
- Remote access**: A section with a blank area for remote access.
- OEM Headquarters [DEV A]**: A section showing the device's status as 'online' and a list of details: '4G Router at Machine Test Lab', 'Serial number: 17088834', 'Firmware: Version 3.20.1', 'Hardware: StrideLinux PRO VPN router 3.0 4G', and 'Location: OEM HQ Machine Test Lab'.
- Event log**: A table showing a list of events with columns for 'Who', 'When', and 'What'.

Who	When	What
Company Owner	December 28, 2021 7:43:28 AM	Changed the configuration
Company Owner	December 27, 2021 1:19:23 PM	Changed the configuration
Company Owner	December 27, 2021 11:01:53 AM	Changed details
Company Owner	December 27, 2021 10:25:56 AM	Changed the configuration
Company Owner	December 27, 2021 10:17:20 AM	Pulled the device to this company
Company Owner	December 27, 2021 10:17:19 AM	Changed details

For help in setting up Data Dashboard Monitoring, refer to the following: <https://support.stridelinx.com/hc/en-us/articles/360019029617-Visualize-your-data>

For help in setting up Cloud Notify Service, refer to the following: <https://support.stridelinx.com/hc/en-us/articles/360019145018--FAQ-Cloud-Notify-All-you-need-to-know>

Appendix A – Glossary

Item	Definition																																				
Access Category	Is the mechanism to give permissions to Users and to view Pages and Services . The Role of every User determines what permissions that user has. Access Categories are a selection of Pages and Services that can be added to a role. All users with that role will then have permission to view and use those pages and services.																																				
Access Level	Broad category of user access as either Company-Wide or Group-specific																																				
Card	You can easily see information about multiple machines in one screen using the card view. You can add one card to every machine, and the cards from all machines will be visible when you use card view in the Portal app. Only one card is allowed per Device.																																				
Cloud Notify	Method to receive notifications from your connected machines re. alarm conditions or warnings of impending problems																																				
Dashboard Data Monitor	The use of customizable pages to view real-time or historical data from devices																																				
Data Source	The origin of variable data along with the communication protocol and related addressing scheme																																				
Device	Name given to a StrideLinux router.																																				
Group	A selection of devices and users; you can divide groups into different group types . An example might be to have a Group Type names Location .																																				
License	Optional purchase in AutomationDirect.com webstore, to add Cloud Logging and/or Cloud Notify																																				
Page	Fully customizable platform dashboard which provides data components relevant to that User . (Requires Studio App engagement)																																				
Roles	<div>There are Company-Wide roles and Group-specific roles summarized below:</div> <table><thead><tr><th>Permission</th><th>Details</th><th>Company-wide role required</th></tr></thead><tbody><tr><td>Configure company identity</td><td>Make changes to the branding and company info.</td><td>Yes</td></tr><tr><td>View audit trail</td><td>You can see a log of all changes that have been made in your company.</td><td>Yes</td></tr><tr><td>View licenses</td><td>You can see whether Cloud Logging and Cloud Notify licenses are active.</td><td>Yes</td></tr><tr><td>Manage roles, access categories and group types</td><td>Make changes to user management.</td><td>Yes</td></tr><tr><td>Manage groups</td><td>Make changes to the groups in your company.</td><td>Yes</td></tr><tr><td>Can manage pages and cards</td><td>You can create, edit and remove all dashboards in your company.</td><td>Yes</td></tr><tr><td>Manage users</td><td>You can add or remove new users within your group and edit the roles and groups that apply to them.</td><td>No</td></tr><tr><td>Manage devices</td><td>You can manage all existing devices in your group and add new devices.</td><td>No</td></tr><tr><td>Manage device templates</td><td>You can create, edit and remove all device templates.</td><td>Yes</td></tr><tr><td>Access categories</td><td>You can give every role permission to all your access categories.</td><td>No</td></tr><tr><td>Enforce two-factor authentication</td><td>You can enforce 2FA for all users with a certain role. You need to turn on 2FA yourself to apply this permission</td><td>No</td></tr></tbody></table>	Permission	Details	Company-wide role required	Configure company identity	Make changes to the branding and company info.	Yes	View audit trail	You can see a log of all changes that have been made in your company.	Yes	View licenses	You can see whether Cloud Logging and Cloud Notify licenses are active.	Yes	Manage roles, access categories and group types	Make changes to user management .	Yes	Manage groups	Make changes to the groups in your company.	Yes	Can manage pages and cards	You can create, edit and remove all dashboards in your company.	Yes	Manage users	You can add or remove new users within your group and edit the roles and groups that apply to them.	No	Manage devices	You can manage all existing devices in your group and add new devices.	No	Manage device templates	You can create, edit and remove all device templates.	Yes	Access categories	You can give every role permission to all your access categories .	No	Enforce two-factor authentication	You can enforce 2FA for all users with a certain role. You need to turn on 2FA yourself to apply this permission	No
Permission	Details	Company-wide role required																																			
Configure company identity	Make changes to the branding and company info.	Yes																																			
View audit trail	You can see a log of all changes that have been made in your company.	Yes																																			
View licenses	You can see whether Cloud Logging and Cloud Notify licenses are active.	Yes																																			
Manage roles, access categories and group types	Make changes to user management .	Yes																																			
Manage groups	Make changes to the groups in your company.	Yes																																			
Can manage pages and cards	You can create, edit and remove all dashboards in your company.	Yes																																			
Manage users	You can add or remove new users within your group and edit the roles and groups that apply to them.	No																																			
Manage devices	You can manage all existing devices in your group and add new devices.	No																																			
Manage device templates	You can create, edit and remove all device templates.	Yes																																			
Access categories	You can give every role permission to all your access categories .	No																																			
Enforce two-factor authentication	You can enforce 2FA for all users with a certain role. You need to turn on 2FA yourself to apply this permission	No																																			
Service	<div>Device capabilities tied into an Access Category for the VPN router:</div> <ul style="list-style-type: none">• VPN Connect• VNC Server• HTTP Server• WebSocket Server• Connection Alarms (VPN, Router, Data Logging)• Alarm Triggers (Tag alarms)																																				
Tag	Tags describe how you wish to log your variables. You can choose to log them at a static interval (100mS to 1 hour), when their value changes, or on a custom trigger. You may also define how long the data should be stored.																																				

Item	Definition
User	Is an invited membership of the company(the overall account for VPN devices and the configuration, thereof). Users are assigned Roles and Groups to determine to which VPN Device(router) they can execute their permissions.
Variable	Incoming data from networked device by field protocol – EtherNet/IP, Modbus TCP, Siemens S7, Bacnet, MELSEC, OPC-UA
VPN Remote Access	This is the StrideLinux router's connection that enables remote and safe access to your machines as if one is on-site