IT Portal

IT Portal 4.0 User Guide

IT Portal 4.0 | support@it-portal.com

Table of Contents

Introduction 4

IT Portal Users 7

Login to the IT Portal 8

IT Portal Interface 9

- Mobile/Table/Desktop Friendly 9
- MSP (Multi-Company) Synopsis View 10
- Company Synopsis View 12
  - Searching 14
  - Command Line Interface 16
  - Add/Import Menu 18
  - Object Lists 20

Documenting a Generic Device 21

- Adding a Device 22
- Device Options Menu 24
  - Editing/Deleting Device 25
  - Updating Device 25
- Remote Access Info and Passwords 29
- Related Objects 31
- Assigned Configuration Objects 33
- Recorded Field Changes 33
- Review 34
- Securing Access 35

Documenting Routers & Firewall 36

- Configuration 36

Documenting Switches 37

Documenting Clusters 37

Documenting Agreements 41

Documenting Contacts 42

Documenting Configuration Objects 43

Documenting Documents 44

Documenting Sites 45
Documenting Facilities 46
Documenting Cabinets 46
Documenting IP Networks 46
Documenting KB Articles 48
Additional Information 49

Introduction

This document describes the procedures and best practices to successfully document infrastructure in the IT Portal. The best practices described should be considered guidelines for your users to quickly get familiar with the IT Portal. The guide discusses the IT Portal interface in detail to familiarize the end user with navigation. Then the document goes into the discipline of proper infrastructure documentation. This document was modelled after a discovery done by an MSP to onboard a new customer. All aspects of the infrastructure were documented by the onboarding team to ensure the helpdesk will have all they need to support the new customer. Below is a listing of items that are generally collected when doing documentation.

- **Company Synopsis**
  - Who the Customer is and their line of business (Company Synopsis Page, Options Menu)
  - Physical location(s) (Add Menu → Sites)
  - Hours of Operation (Company Synopsis Page, Notes)
  - Primary Contacts and Stakeholders (Company Synopsis Page, Options Menu to select an existing contact)
    - Email
    - Phone
  - After hours Contacts and IT Contacts (Company Synopsis Page, Notes)
    - Email
    - Phone
    - When to contact and Severity
  - **General Remote Access Information** (Company Synopsis Page, Remote Access Notes)

- **Logical Groupings of Contacts and Devices**
  - Sites (Add Menu → Sites)
  - Facilities within sites (Add Menu → Facilities)
  - IP Networks (Add Menu →IP Networks)
  - Network diagrams if applicable (Add Menu → Documents)

- **Vendor Information, Licensing, and Agreements** (Add Menu → Agreements)
  - Agreements expiration
  - Software subscriptions dates
  - Domain Name
  - SSL
  - Licensing
    - Keys
    - Login accounts
    - Support info/accounts
    - Device Warranties

- **Device Management**
  - Servers physical and virtual and roles (Add Menu → Devices)
  - Reboot dependencies (Add Menu → Lists or Documents w/ relationships defined)
  - Major application performance metrics (nice to have)
  - Workstations (Add Menu → Sites, Define number of workstation per site)
  - Printers (Add/Import Menu → Devices)
  - Firewall (Add Menu → Devices)
  - Routers (Add Menu → Devices)
  - Switches (Add Menu → Devices)
  - Storage (Add Menu → Devices)
  - Content Filters (Add Menu → Devices)

- **Documentation**
  - Specifically related to the customer goes in documents IE Internal products or policies and procedures (Add Menu → Documents)
  - Products we support goes in to knowledgebase. IE Symantec Cloud (Add Menu →KBs)

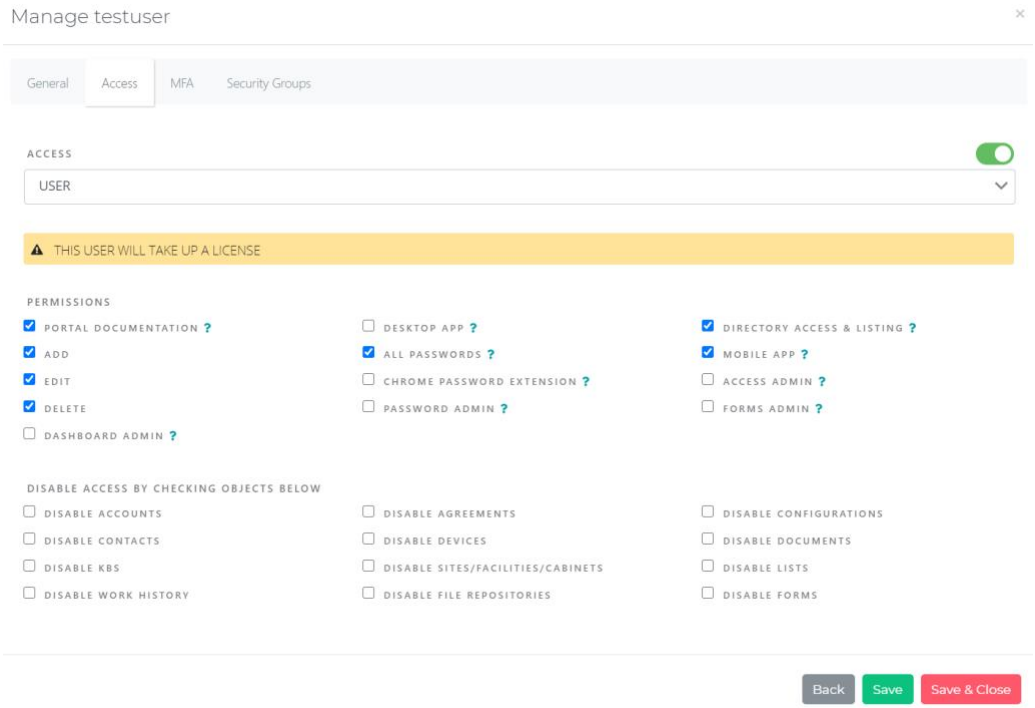
- **Accounts** (Add/Import Menu → Accounts)
  - Service accounts
  - AD accounts
  - Administrator accounts for DSM
  - Registrar account
  - Cloud services accounts

- **Configuration Items** (Add/Import Menu → Config Items)
  - Tangible items that are not IP addressable,
  - Application
  - LUNs (Defined Raid Sets on Storage Devices, not Servers)
  - Clusters
  - Databases
  - Web sites
  - Disks, and external drives
  - General DNS names
  - FTP sites
  - Group Policies
  - Map drives
  - Scheduled tasks
  - Services
  - SSID

IT Portal Users

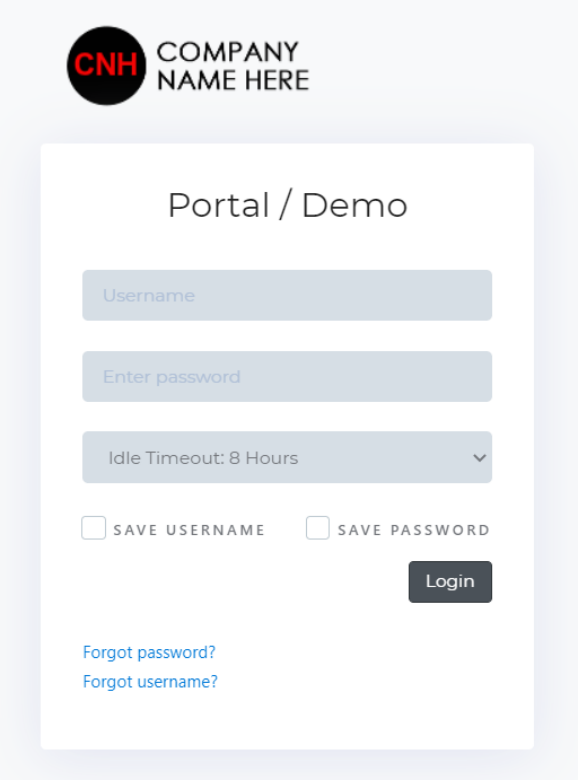
The IT Portal has different types of users and optional permissions

1. **Admins** have full access to all companies and administrative functions regardless of security restrictions in place.
2. **Regular users** by default can't configure the IT Portal but they have access to all companies. You may restrict access to companies if needed and it will apply to non-admin users.
3. **Restricted users** are restricted to a subset of companies.
4. **Company users** are user that are assigned to one company and are typically used by MSPs/Systems Integrators for their customers. Read only company users (Add/Edit/Delete Permissions disabled) do not count towards your user count if you are licensed for more than one IT Portal user.
5. **All Passwords** permission gives users access to all passwords. Otherwise the user should be given permission to the object to access its username and password.
6. **Password Admins** can run password list reports.
7. **Mobile App Access** sets access to the free iPhone/Android App.



Login to the IT Portal

To login you must provide your username and password.



Your IT Portal may be setup to require an optional Key. During setup, an encryption key is inputted to encrypt and decrypt all usernames and passwords. The optional key is used as an extra security measure to salt the existing key. If it is setup, you will be required to enter it at every login if you need access to usernames/passwords.

If you forget your password and your account is not active directory integrated, you can reset your password. If you forgot your username, you must contact your admin.

If the computer you are logging into is untrusted, it is recommended that you use a one-time password or Google Authenticator.

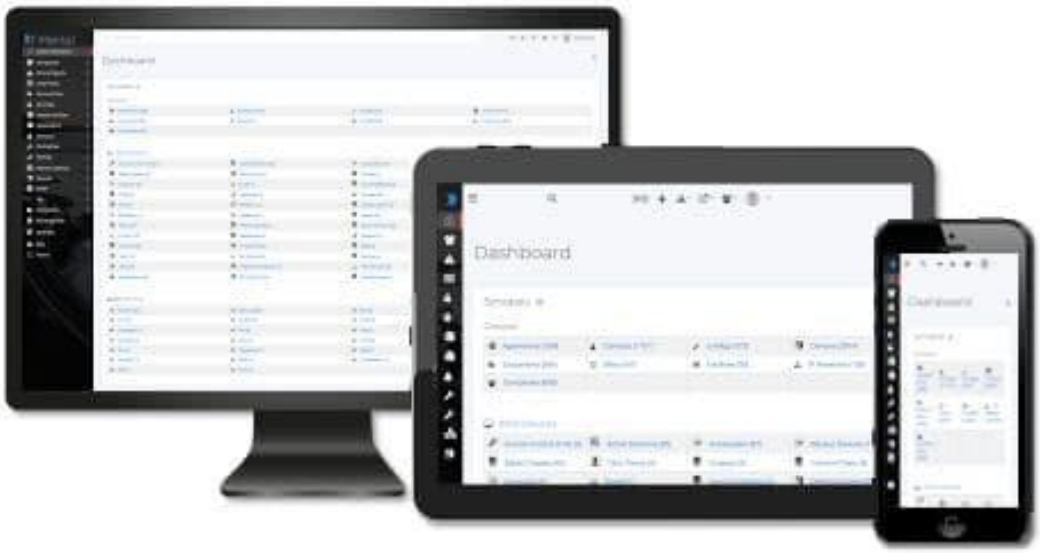
KB Setting up your one-time password
KB Google Two Factor Authentication.

Optionally save your username and password and set your timeout. For security reasons, you session expires if you login from another PC. You will be informed that someone logged in from another IP address.

IT Portal Interface

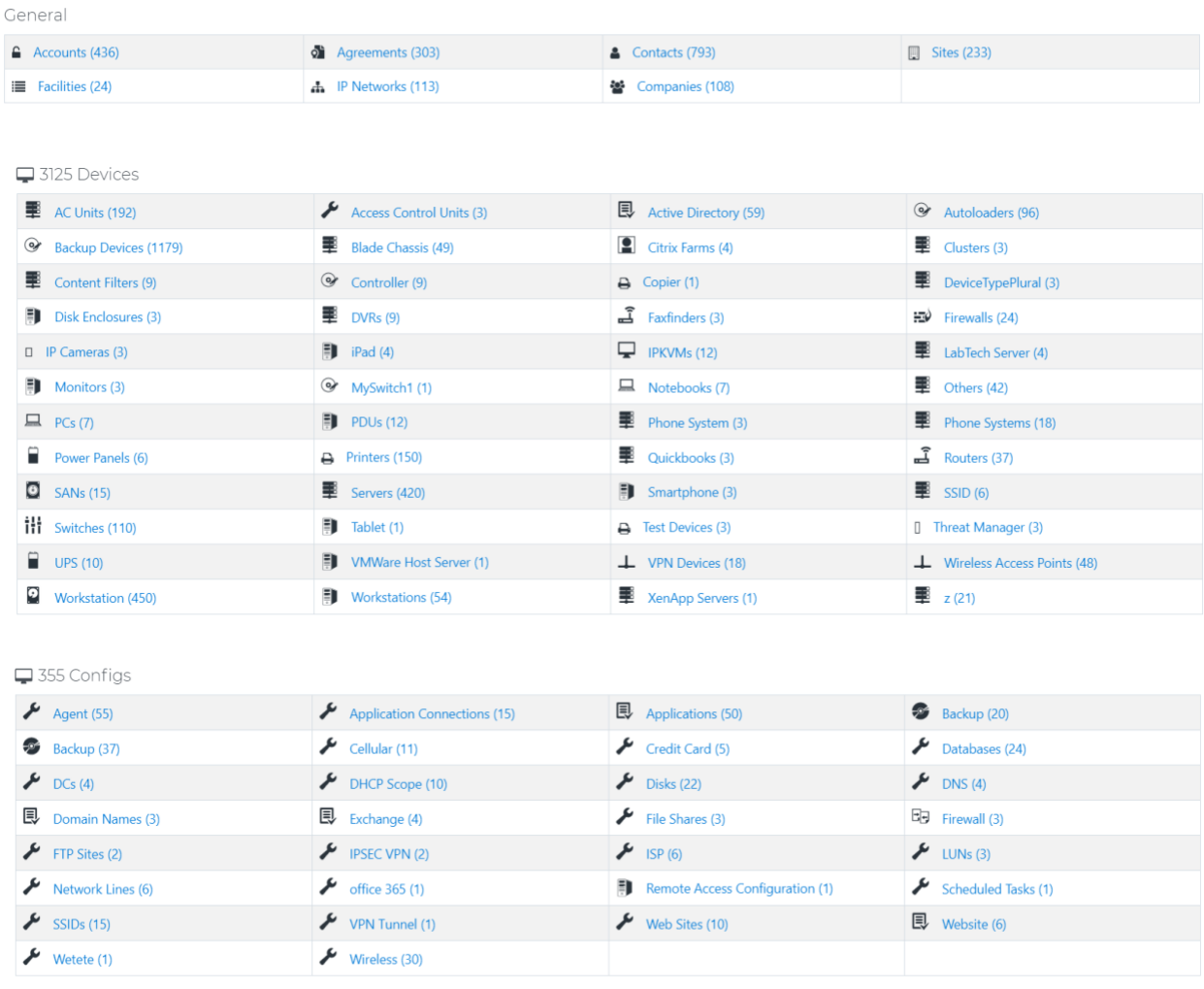
Mobile/Table/Desktop Friendly

The IT Portal is very device friendly. You should do most of your editing from a device with a larger screen like a tablet or a desktop, but the IT Portal will conform to the screen on your device. Below are examples of how the IT Portal will look at different resolutions from a full desktop, tablet, and smart phone. A fast searching mobile app is available at the App Store and Google Play as well.



MSP (Multi-Company) Synopsis View

If your IT Portal has more than one company defined, a multi-company synopsis view is presented at login. This view is an aggregate of all the objects in the IT Portal. This view provides a good understanding of your support environment as object counts are provided.



279 Documents

ALL-FIELDS-EXAMPLE (5)	Assessment (1)	Assessment (36)	BDR Documentation (17)
Build Books (24)	contract1 (22)	dddddd (3)	Diagram (25)
Discovery (3)	Doc (3)	Documentation (10)	How to (2)
Install Doc (12)	Logos (27)	Network Diagram (3)	Policies (10)
Procedures (23)	Project Documents (3)	Remote Access Config (3)	Script (1)
Site Pics (5)	SOPs (13)	testing789123 (3)	User Termination Guide (3)
WOPIFiles (22)			

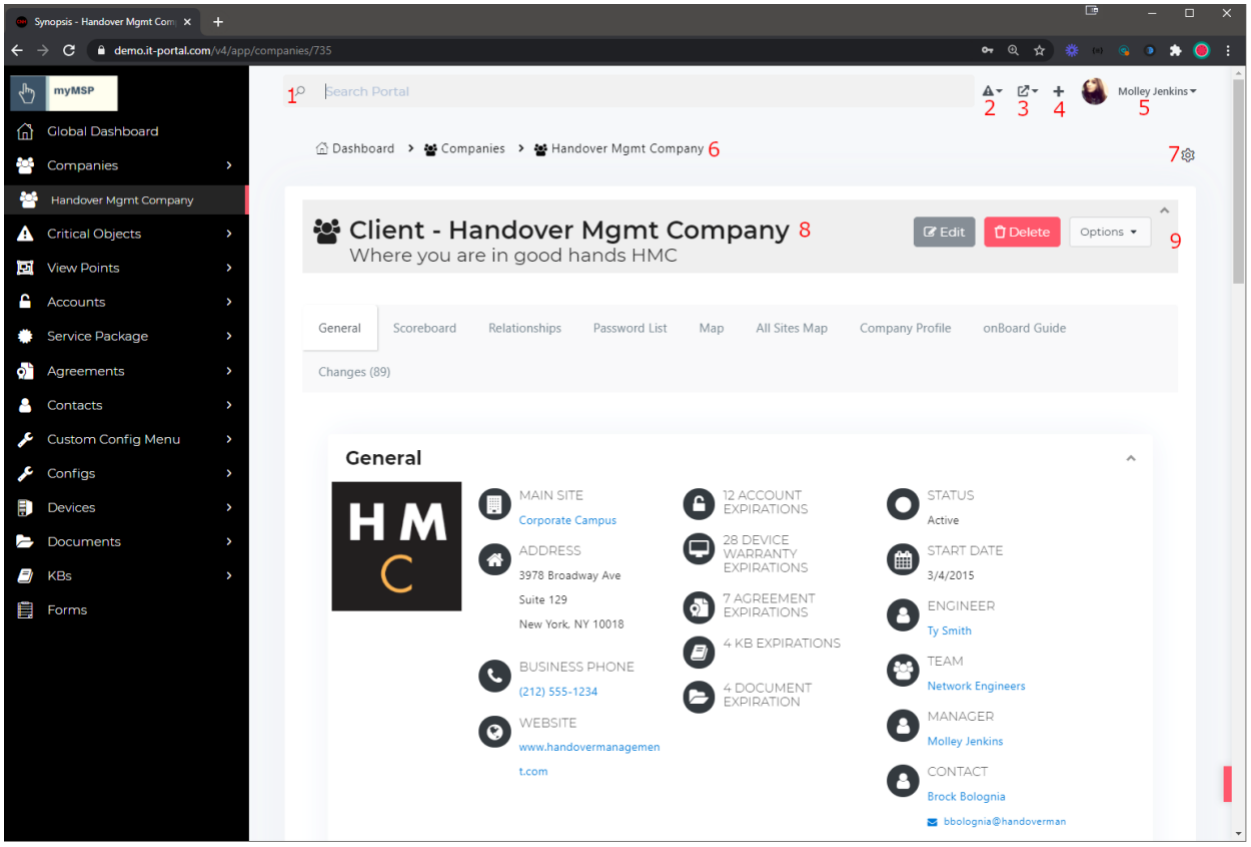
680 Services

BackEnd (24)	Backup (392)	BES (10)	Citrix (17)
DC (21)	DHCP (19)	DNS (22)	EDI (7)
Exchange (13)	Fax (9)	File (21)	FTP (12)
GuysApp (5)	IAS (13)	Print (22)	RAS (5)
SAV (6)	SharePoint (7)	SMS (3)	SQL (13)
Terminal (11)	UTM (2)	Virtualization (11)	vSphere (5)
Web (6)	Wins (4)		

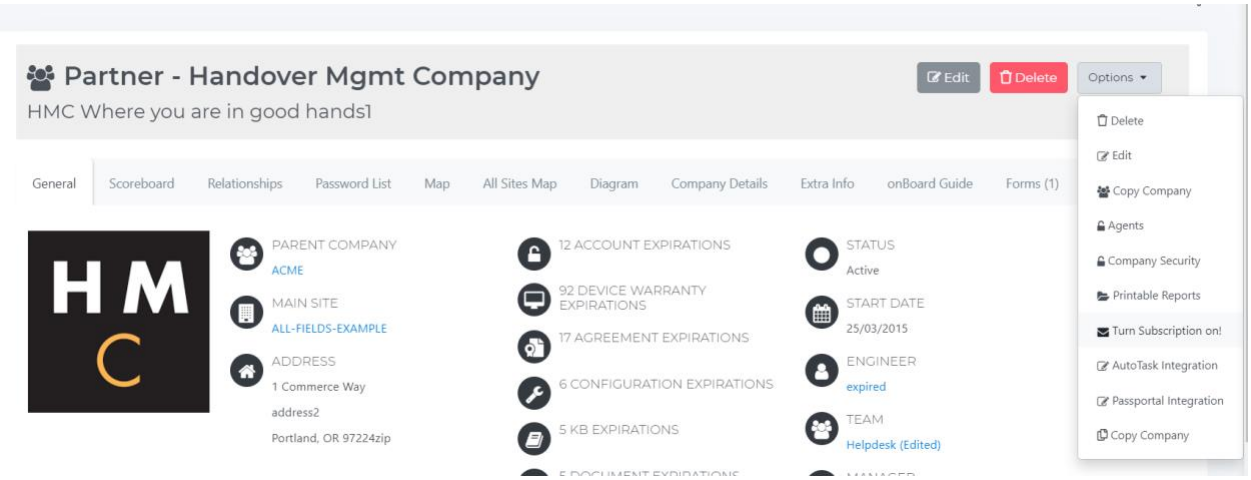
Company Synopsis View

Below is an outline of the synopsis screen for a single company

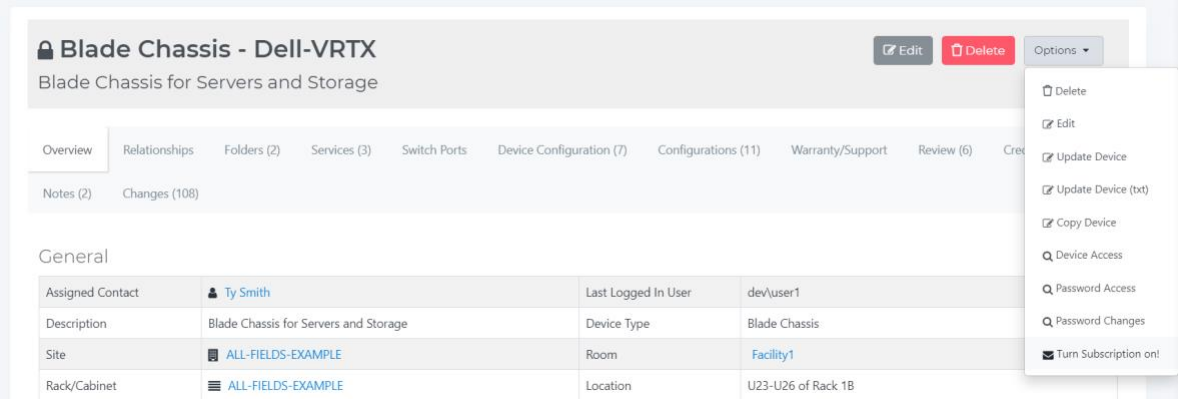
1. Powerful CLI/Keyword searching
2. Critical Objects (See #7)
3. Links Menu (Admin Settings > Site Settings > Links)
4. Add/Import Menu
5. Settings Menus
6. Breadcrumb/Navigation
7. Click the Gear icon to toggle Widgets on/off
8. Company Name
9. Options Dropdown



Turning subscriptions on for all objects in a company



Turning subscriptions on for an object in a company



Searching

As data sets grow, using an entire database search may not return a fast enough result. Hence, we have two options and both are described below.

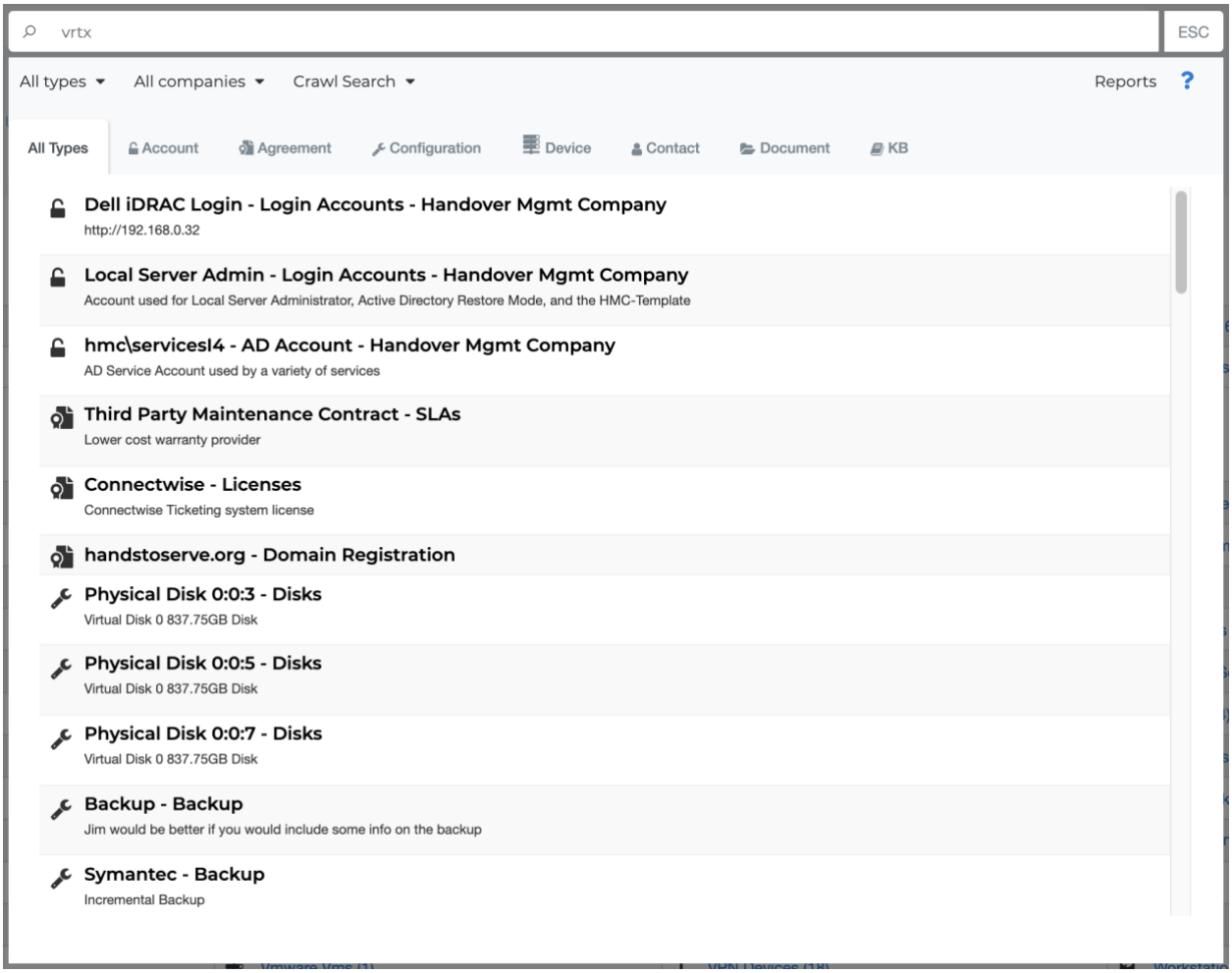
Crawl Search

Searches all data in the Portal.

Quick Search

Searches the specific Fields:

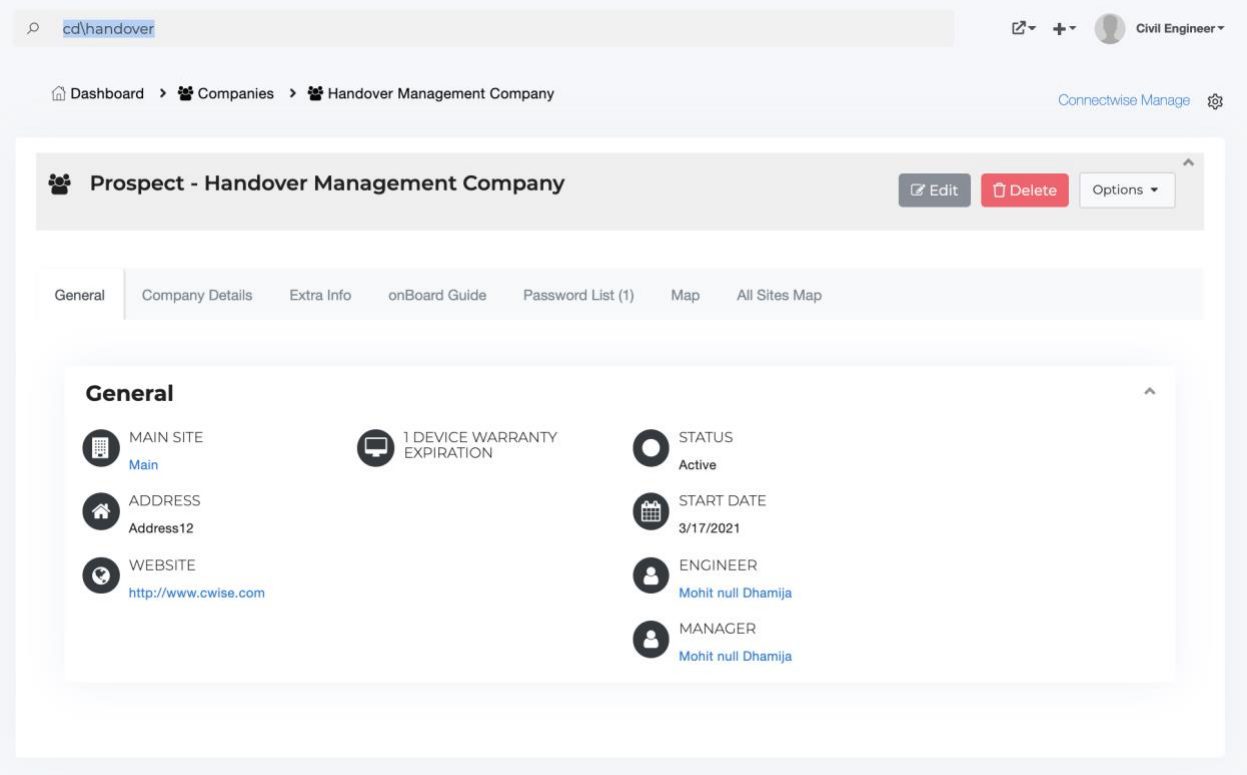
- Object Types, Names, and Descriptions for (Sites, Facilities, Rack Cabinets, IP Networks, Accounts, Agreements, Contacts, Configurations, Documents, Devices, KBs, and Forms)
- All Names
- All Descriptions
- Agreement Vendor
- Contact Phone Number
- Contact Email
- Device Serial
- Device Tag
- Device IP Address
- Device MAC Address
- Device Manufacturer and Model
- Optionally can enable username search in Password Policy



KB Search Overview & Video

Command Line Interface

The cursor always defaults to the CLI (Command Line Interface). The example below “cd\handover” took us to the handover management company.

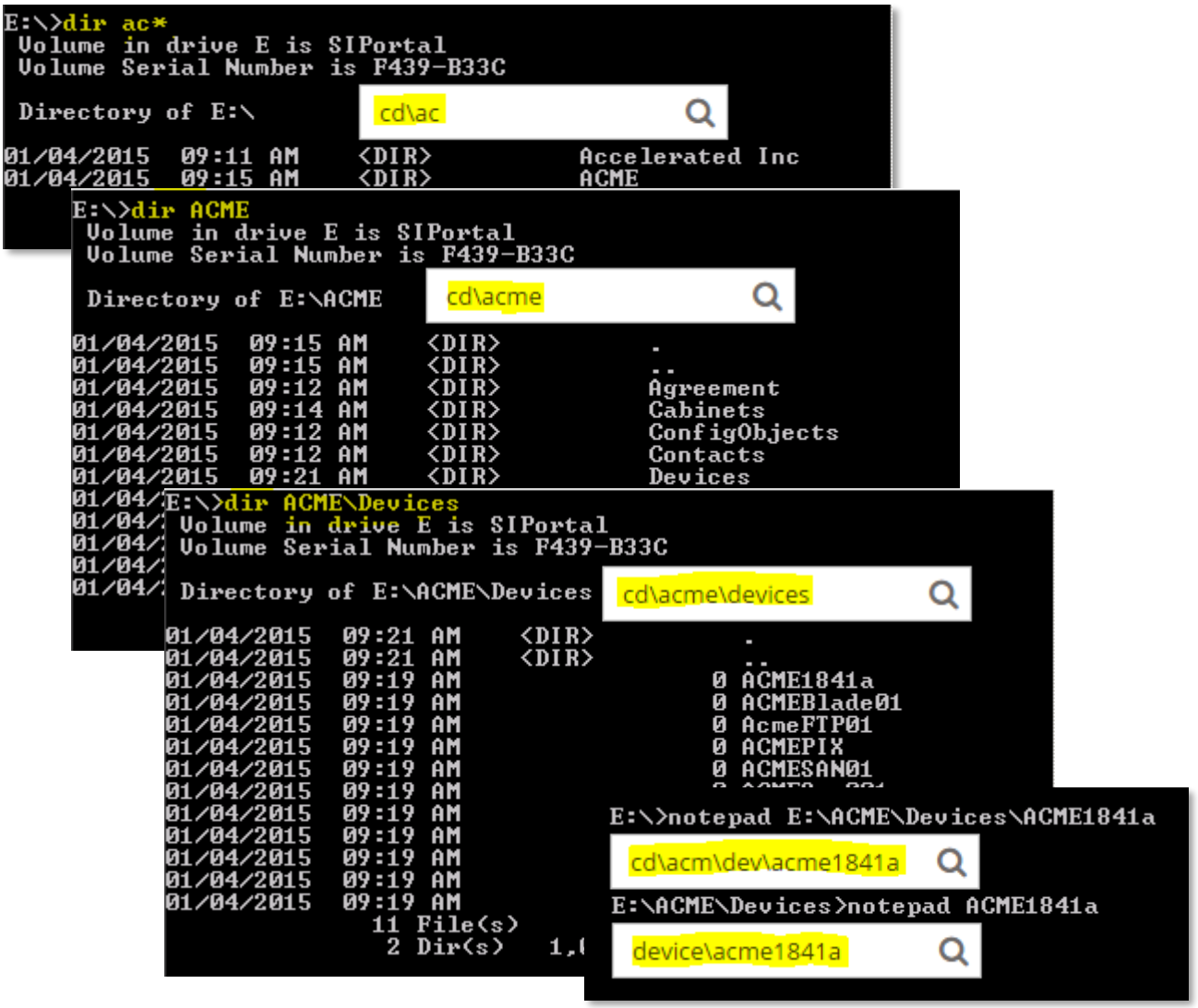


Examples:

1. Go to a firewall
    a. device\asa01 **AKA** dev\asa01
2. See a list of firewalls for company ACME
    a. cd\acme\devicetype\firewall **AKA** cd\acme\dt\firewall
3. Go to a of document
    a. document\network diagram

The CLI works much like a DOS command prompt. Unlike DOS, abbreviations are accepted in the commands and search criteria. If currently viewing a company, the searches are limited to that company.

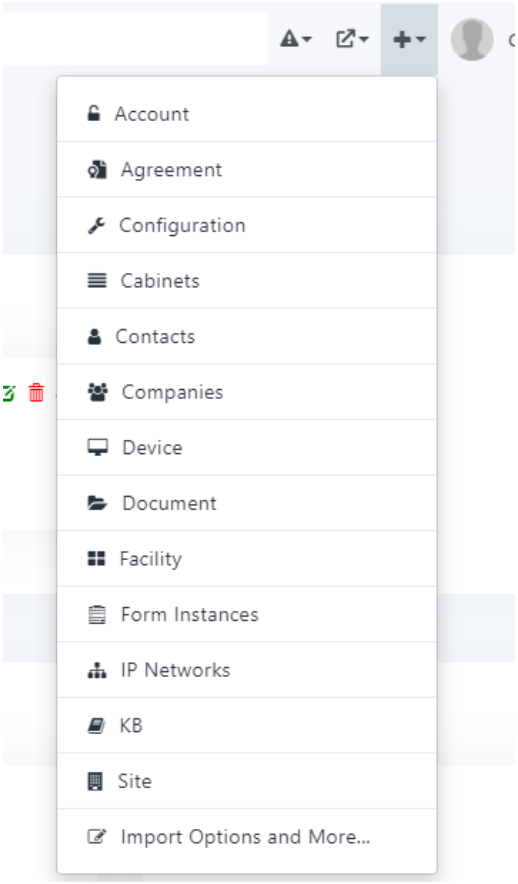
KB Describes the various Command Line Options



Add/Import Menu

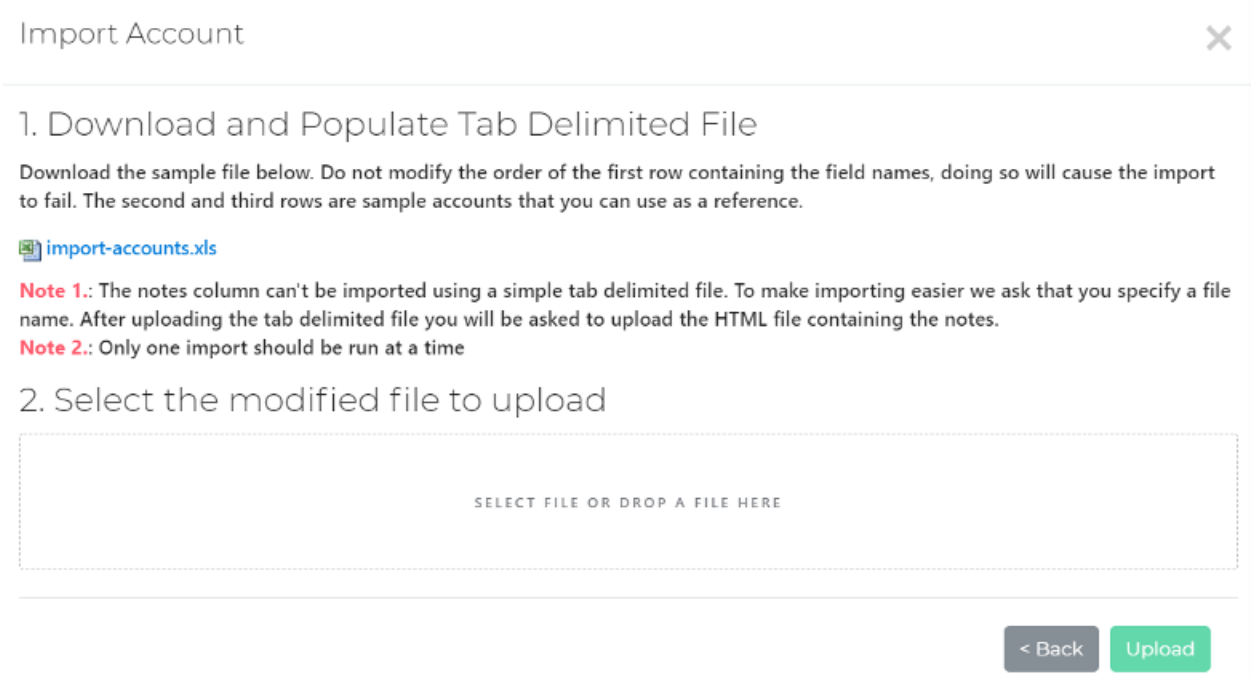
The **+** button will provide you options to add and import objects into the IT Portal.

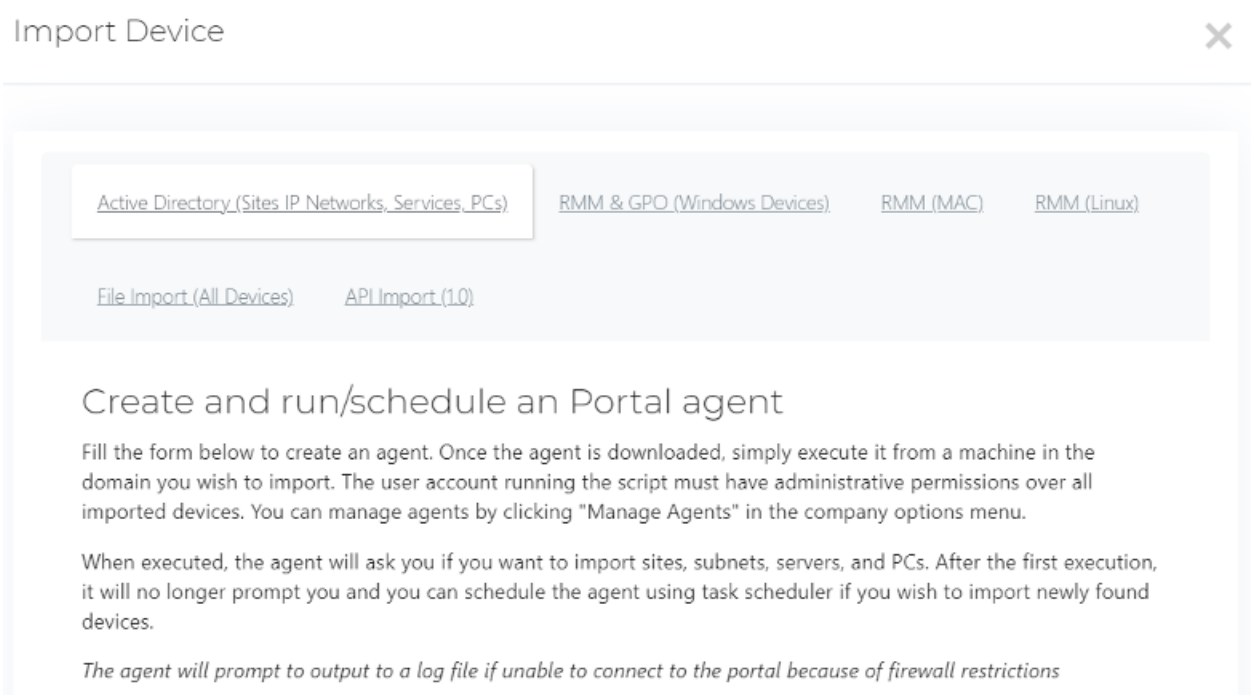
The “Add Objects” option allows you to manually create a single item. All objects can be imported via a tab delimited file.



The import process for devices also allows importing Servers, Workstations, and IP Networks from Active Directory. Be sure to update the description fields in AD so they get imported into the IT Portal.

You can also import/synchronize companies and contacts from Autotask and ConnectWise. Contact support@siportal.com for integration with your PSA if it has an API otherwise use the import options.

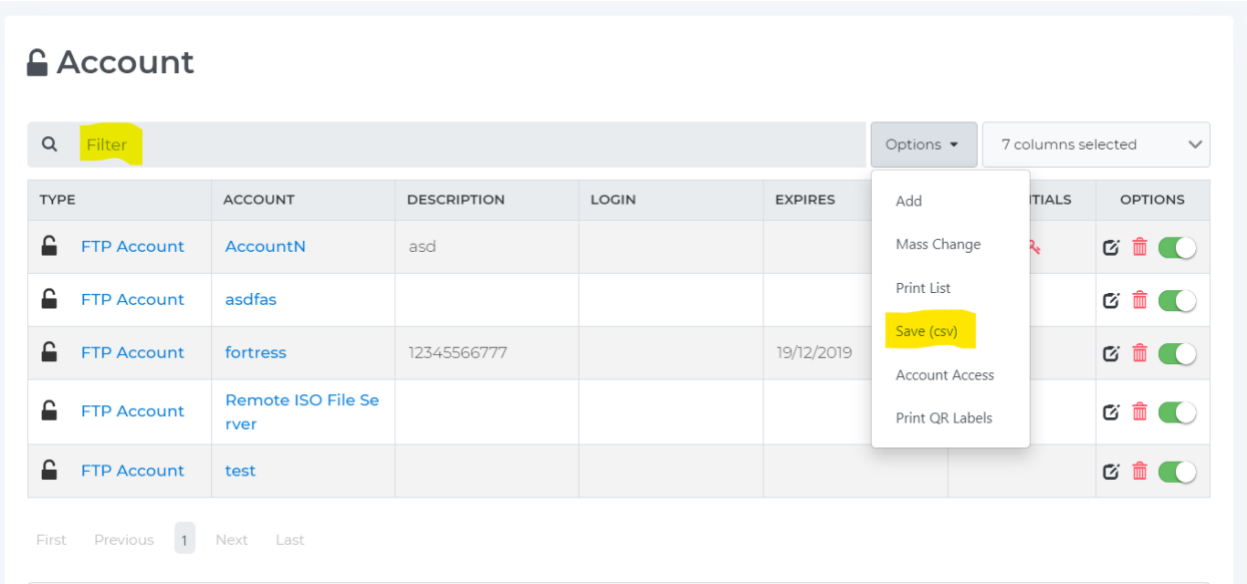

Import Account
1. Download and Populate Tab Delimited File
Download the sample file below. Do not modify the order of the first row containing the field names, doing so will cause the import to fail. The second and third rows are sample accounts that you can use as a reference.
import-accounts.xls
Note 1.: The notes column can't be imported using a simple tab delimited file. To make importing easier we ask that you specify a file name. After uploading the tab delimited file you will be asked to upload the HTML file containing the notes.
Note 2.: Only one import should be run at a time
2. Select the modified file to upload
SELECT FILE OR DROP A FILE HERE
< Back
Upload


Import Device
Active Directory (Sites IP Networks, Services, PCs)
RMM & GPO (Windows Devices)
RMM (MAC)
RMM (Linux)
File Import (All Devices)
API Import (1.0)
Create and run/schedule an Portal agent
Fill the form below to create an agent. Once the agent is downloaded, simply execute it from a machine in the domain you wish to import. The user account running the script must have administrative permissions over all imported devices. You can manage agents by clicking "Manage Agents" in the company options menu.
When executed, the agent will ask you if you want to import sites, subnets, servers, and PCs. After the first execution, it will no longer prompt you and you can schedule the agent using task scheduler if you wish to import newly found devices.
The agent will prompt to output to a log file if unable to connect to the portal because of firewall restrictions

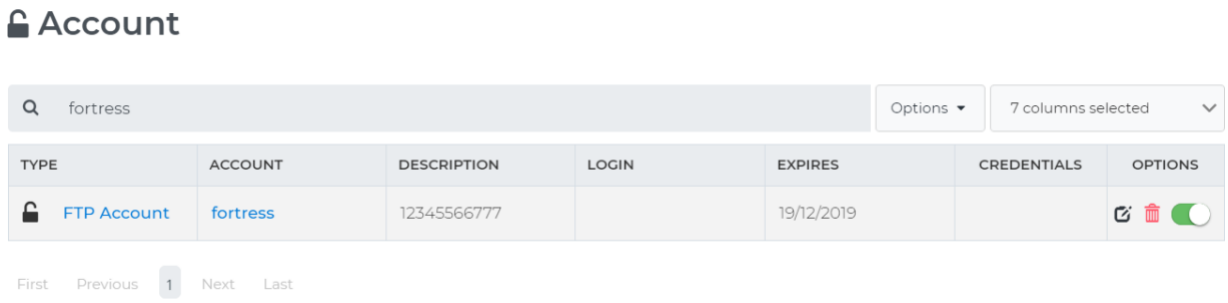
Object Lists

Below is a listing of the account objects in the IT Portal. Listing options include

1. The ability to copy the list to your clipboard
2. You can print the list
3. You can export the list to CSV, Excel, or PDF File
4. You can also limit the number of items listed on screen



You can use the filter field to find exactly what you are looking for. The above listing was filtered by searching for the “fortress” The filtering criteria simply has to be separated by a space.



Documenting a Generic Device

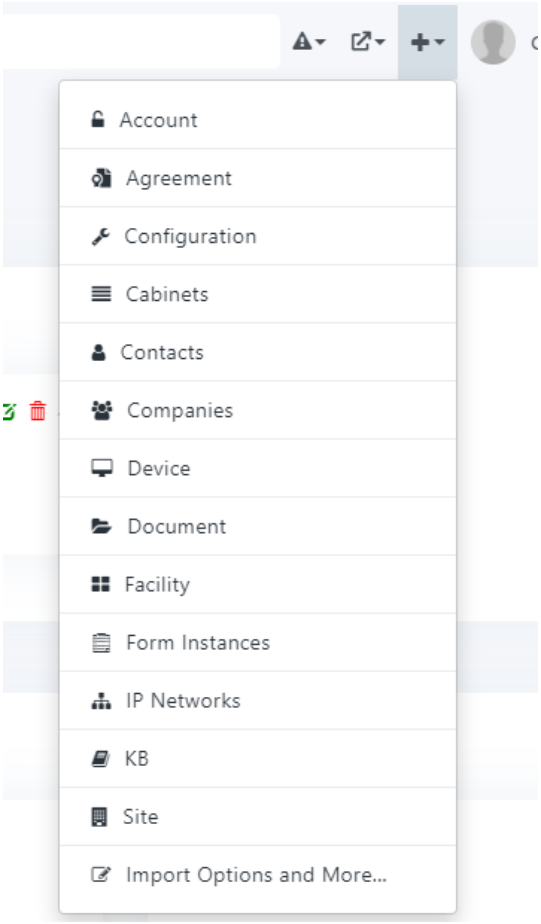
In the IT Portal, you can document Servers, Routers, Firewalls, and Switches. You also have custom devices like phone systems, KVM, backup drives, Clusters, Active Directories, or UPS Systems. Store vital information on these devices. Track information like configuration, running services, IP addresses, passwords, applications, and more.

* General Information is used to identify the device
* Document Network Interfaces and what switch they are plugged into
* Document login and management info
* Links to contacts, devices, documents, agreements, and emails are displayed to show how the device relates to the organization.
* Import WMI information from windows devices using the Option button after adding/editing

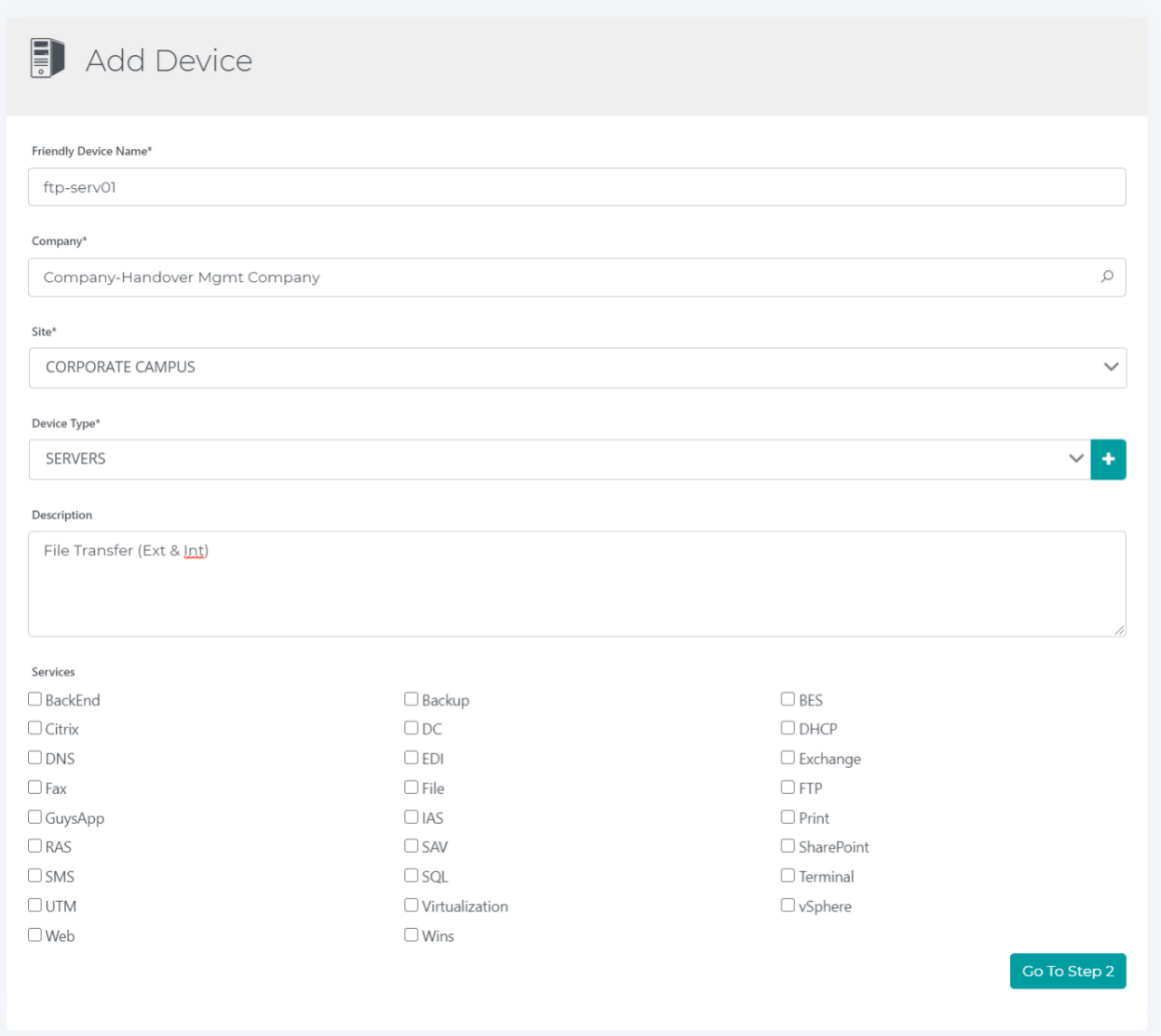
Below I will describe the process used to document an FTP server for an organization. Though this is an FTP server, the process of documenting any device is pretty much the same. As information is acquired, you should consider documenting it. In this scenario, an FTP server was setup previously and an engineer was asked to document it.

Adding a Device

We start the process by clicking the plus (+) button to get the add objects context menu and then select “Device.” You can also go to the bottom left Add Menu and select “Device.”

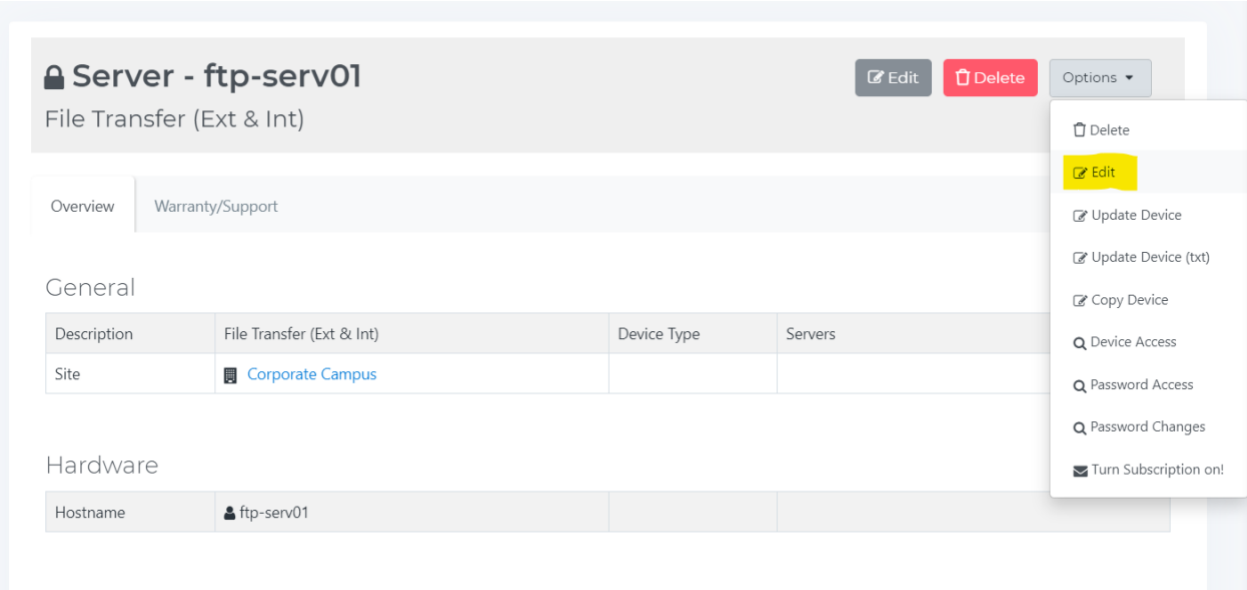


1) Enter the Device Name.
2) Select the Company and Site that the device will exist in.
3) Select the type of device and a description of the device.



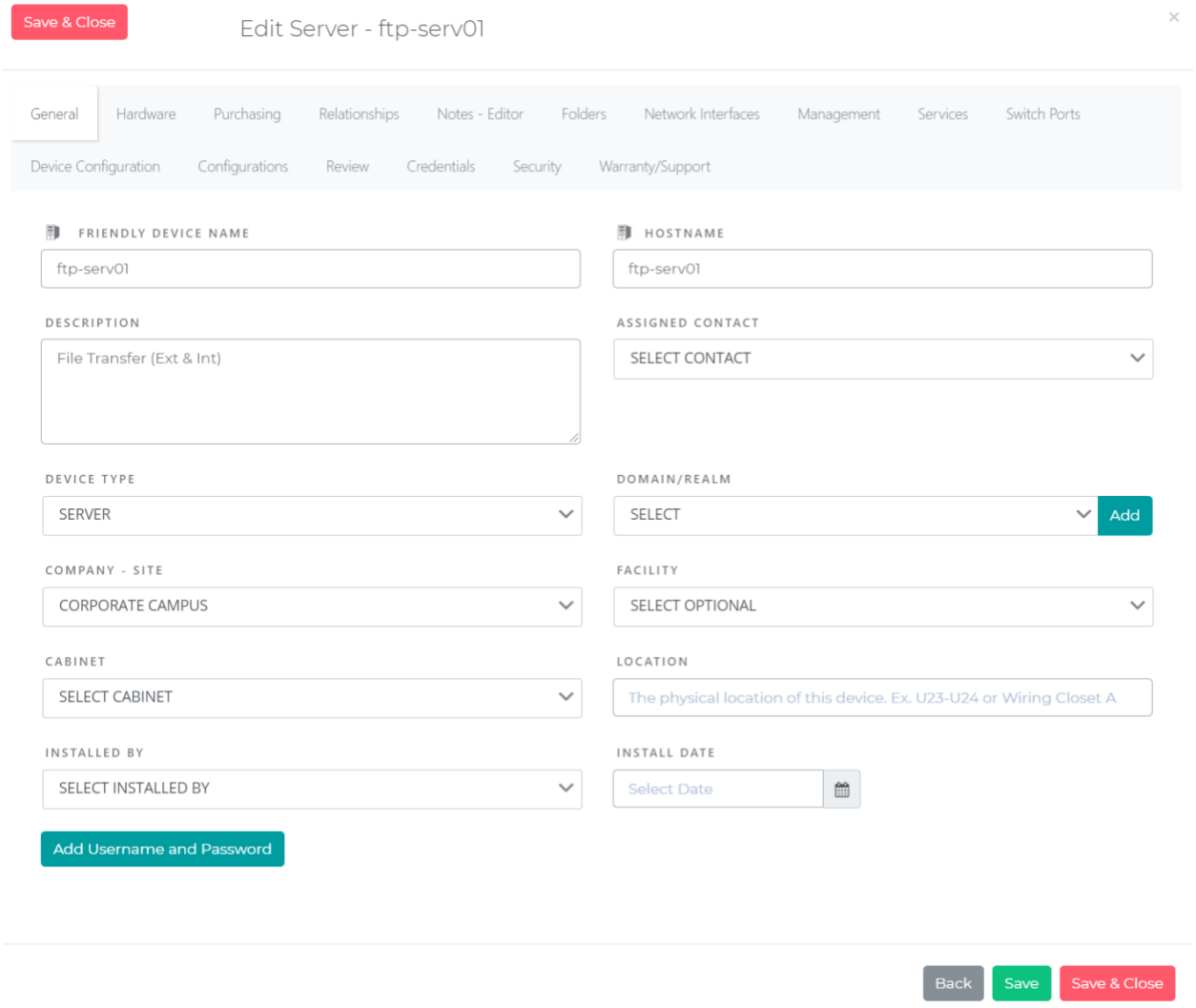
Device Options Menu

At this point, not much is documented. While viewing the device, you can go to options menu to edit, delete, update, or enable subscriptions to updates for this device. You can also access the options menu when viewing a list of devices.



Editing/Deleting Device

As changes are made to a device, the device should be edited to include those changes. Changes are recorded and documented. Hence feel free to make the needed changes knowing that your changes won't result in loss of data.



Updating Device

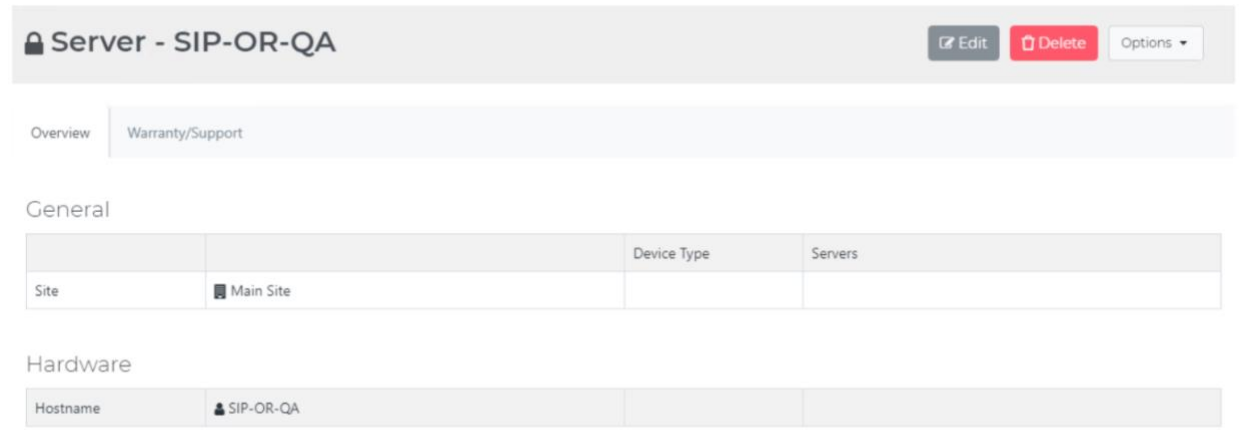
Options Menu → "update device" is used to collect hardware information via WMI calls. This will download a script that will

automatically collect the data and send it to the IT Portal. Note, if you run the script again, it will not modify any fields that already have data populated. WMI information will be overwritten.

Pre-Requirements for update device to work include

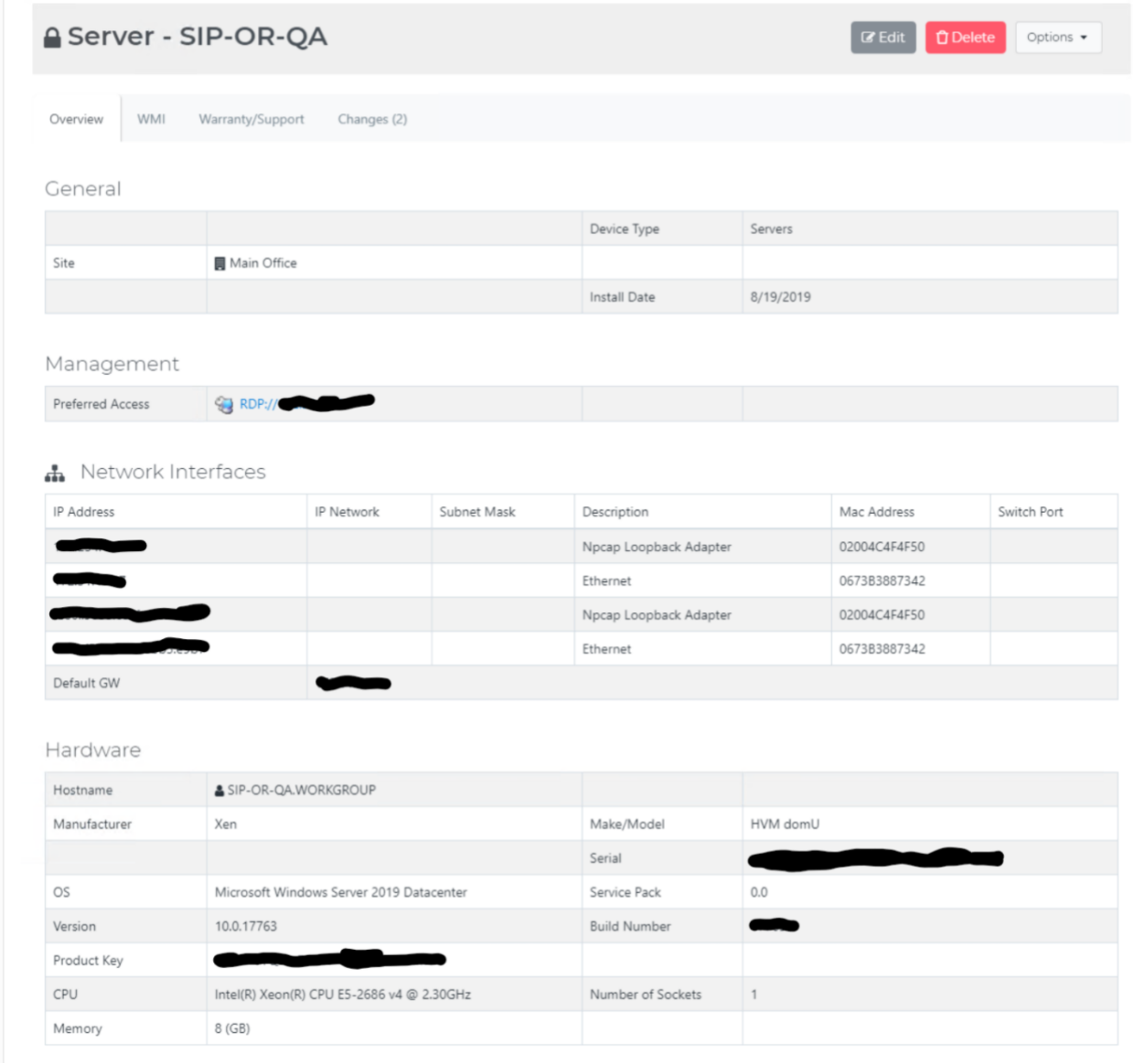
You must be logged into a machine that is on the domain and your active directory user account must have administrative permission to the machine. Alternatively, if the machine is not domain joined, you can login to the machine and run the "Update Device" script.

Before



After

** **Note:** Some fields have been redacted for security reasons, but every field you see that is covered has data in the field.*



Server - SIP-OR-QA

Edit | Delete | Options

Overview | WMI | Warranty/Support | Changes (2)

General

		Device Type	Servers
Site	Main Office		
		Install Date	8/19/2019

Management

Preferred Access	RDP://[redacted]		

Network Interfaces

IP Address	IP Network	Subnet Mask	Description	Mac Address	Switch Port
[redacted]			Npcap Loopback Adapter	02004C4F4F50	
[redacted]			Ethernet	0673B3887342	
[redacted]			Npcap Loopback Adapter	02004C4F4F50	
[redacted]			Ethernet	0673B3887342	
Default GW	[redacted]				

Hardware

Hostname	SIP-OR-QA.WORKGROUP		
Manufacturer	Xen	Make/Model	HVM domU
		Serial	[redacted]
OS	Microsoft Windows Server 2019 Datacenter	Service Pack	0.0
Version	10.0.17763	Build Number	[redacted]
Product Key	[redacted]		
CPU	Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz	Number of Sockets	1
Memory	8 (GB)		

The WMI information below was also collected. You may be tempted to constantly update the device, but consider the information found below as a baseline. The information below is a point in time of how this server looked when it was first documented. As time goes by you can use this information to compare the baseline disks, shares, software, and services to those that currently exist on the production server. Hence you can project the growth of a server and see how it has changed.

WMI Tab

This particular view has a lot of sections you can review. This sample screenshot is the Services section.

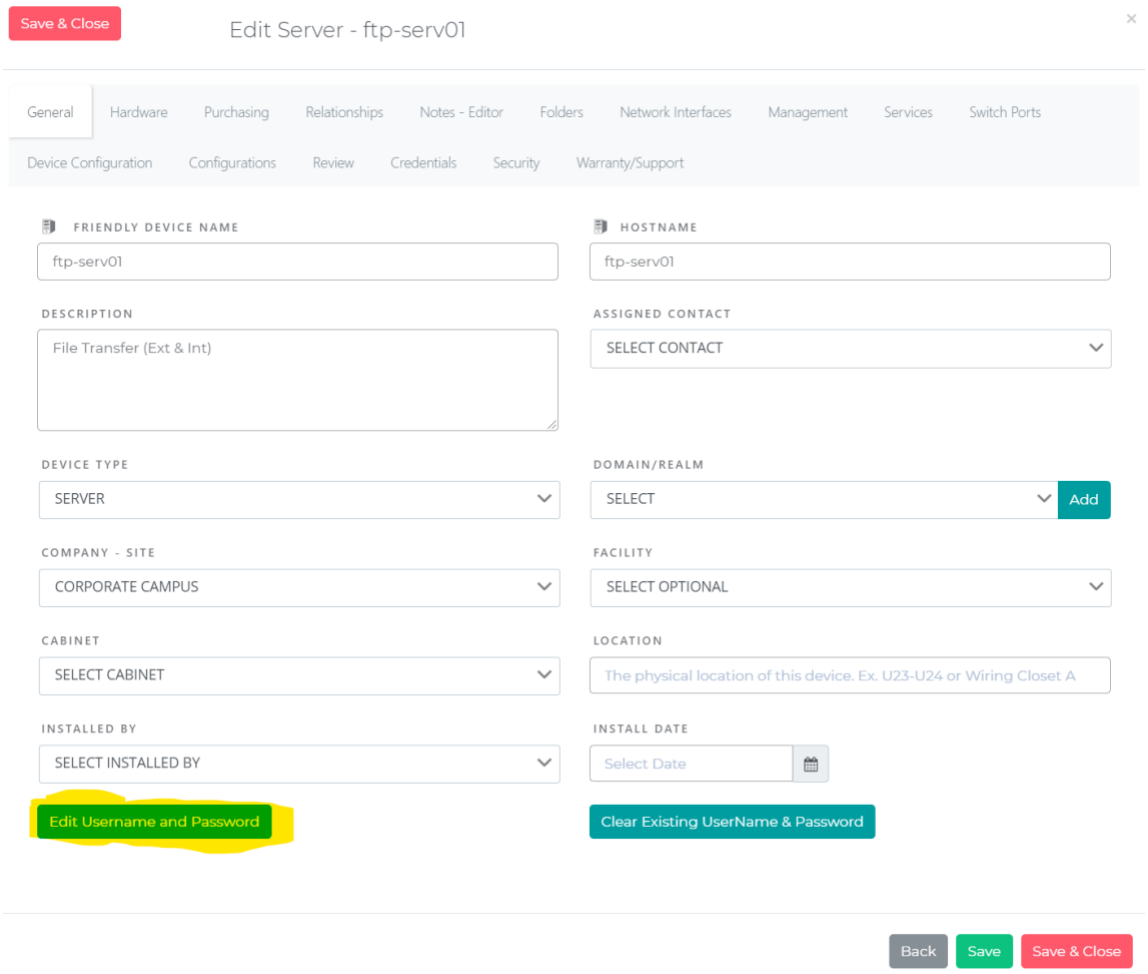
SERVICE NAME	STATUS	STARTUP TYPE	LOG ON AS	SCAN DATE
ActiveX Installer (AxInstSV)	Stopped	Disabled	LocalSystem	9/17/2020
AllJoyn Router Service	Stopped	Manual	NT AUTHORITY\LocalService	9/17/2020
Amazon SSM Agent	Running	Auto	LocalSystem	9/17/2020
App Readiness	Stopped	Manual	LocalSystem	9/17/2020
Application Host Helper Service	Running	Auto	localSystem	9/17/2020
Application Identity	Stopped	Manual	NT Authority\LocalService	9/17/2020
Application Information	Stopped	Manual	LocalSystem	9/17/2020
Application Layer Gateway Service	Stopped	Manual	NT AUTHORITY\LocalService	9/17/2020
Application Management	Stopped	Manual	LocalSystem	9/17/2020
AppX Deployment Service (AppXSVC)	Stopped	Manual	LocalSystem	9/17/2020
ASP.NET State Service	Stopped	Manual	NT AUTHORITY\NetworkService	9/17/2020
Auto Time Zone Updater	Stopped	Disabled	NT AUTHORITY\LocalService	9/17/2020
AVCTP service	Stopped	Manual	NT AUTHORITY\LocalService	9/17/2020
AWS Lite Guest Agent	Running	Auto	LocalSystem	9/17/2020
Background Intelligent Transfer Service	Stopped	Manual	LocalSystem	9/17/2020
Background Tasks Infrastructure Service	Running	Auto	LocalSystem	9/17/2020
Base Filtering Engine	Running	Auto	NT AUTHORITY\LocalService	9/17/2020
Bluetooth Audio Gateway Service	Stopped	Manual	NT AUTHORITY\LocalService	9/17/2020
Bluetooth Support Service	Stopped	Manual	NT AUTHORITY\LocalService	9/17/2020
Capability Access Manager Service	Stopped	Manual	LocalSystem	9/17/2020
CaptureService_2315c3	Stopped	Manual		9/17/2020
CaptureService_58b5a	Stopped	Manual		9/17/2020
Certificate Propagation	Running	Manual	LocalSystem	9/17/2020

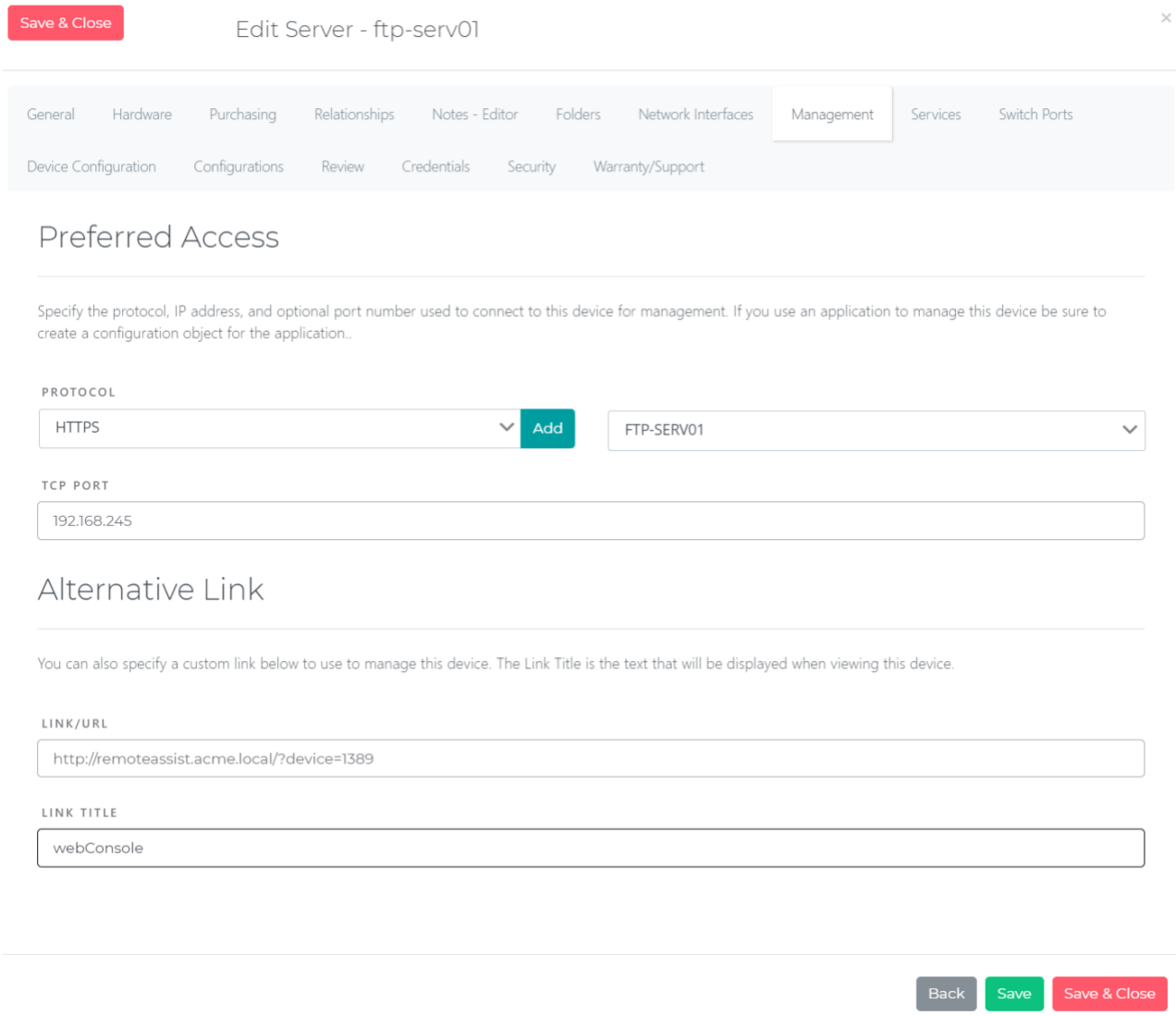
Remote Access Info and Passwords

To record management information about this device, two fields are provided. “Preferred Access” to note the protocol/application used and the IP address. If you prefer, you can specify a URL to be displayed instead. The link title is the text that will be displayed. When the user clicks the text, the URL will be accessed.

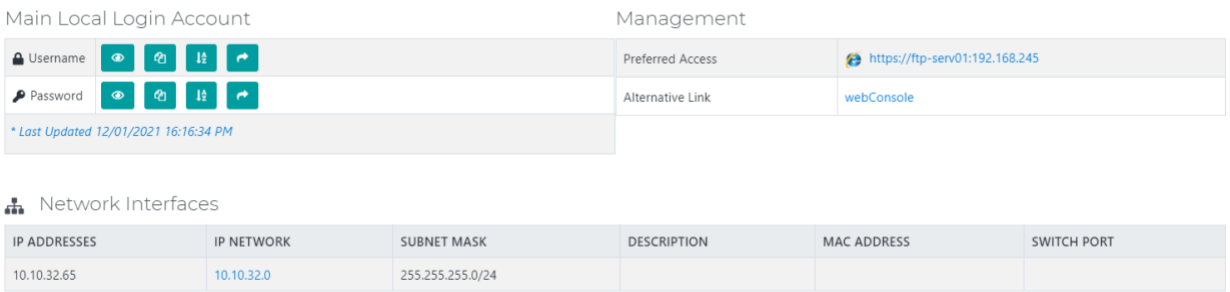
The username and password fields are used to access this device. Other login accounts that are used for monitoring or exec level access can be documented as separate accounts and linked to this device. That will be covered next.

Editing a device access info





Viewing a device access info



Related Objects

The accounts below were documented that related to this device. While editing the device, you can link these accounts. The last column is used to provide information regarding the relationship between the account and the device. Below we see support information for the FTP software, a few FTP accounts that were setup, and an AD account used to start the service.

Related Accounts

NAME	TYPE	DESCRIPTION	RELATIONSHIP
Cerberus	Support Accounts		Website for Support
sftp	FTP Account		National Student Clearing House Account
sftp-nslc	AD Account		Account used to run the FreeSSHD Service
UC-Backups	FTP Account		Cisco Login Account

Agreements were documented that relate to this device. The FTP software license was documented in case the application needs to be reinstalled. A public key was also saved, used by a particular user to login to the FTP server.

Related Agreements

NAME	TYPE	DESCRIPTION	RELATIONSHIP
Cerberus	Licenses		FTP Server License
NSCL Public Key	SSL Certificates		National Student Clearing House Public Key

Documented the vendors and users that have been involved in the setup of this FTP server.

Related Contacts

NAME	TYPE	DESCRIPTION	RELATIONSHIP
Anita Tata	Vendor	Unix Admin	Uses User SFTP for SPEEDE Transfer
David Badhri	Vendor	Consultant	SalesForce SFTP User Contact
Michael Rhodes	Users	Receives SFTP files from Clearing House	Reviews the National Clearing House files

Documented the devices that are related to this ftp server. The relationship field notes the ports allowed for this FTP Server.

Related Devices

NAME	TYPE	DESCRIPTION	RELATIONSHIP
Itb-2921	Routers	Internet going-thru	Allowing 22 and 990 on IP 71.40.181.202

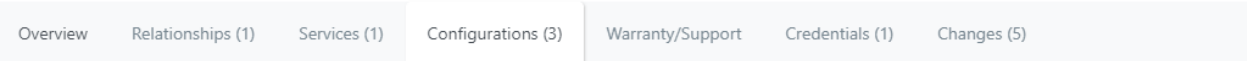
Documented the Install guides, testing procedures, and a build book that has detailed the install and discusses the business requirements that were met by using this particular FTP Server.

Related Documents

NAME	TYPE	DESCRIPTION	RELATIONSHIP
Parchment Guide	Install Doc		
SFTP Server	Documentation	SFTP Server Config Info	SFTP Server
Testing SFTP	Documentation	Testing SFTP on FPUSFTP	

Assigned Configuration Objects

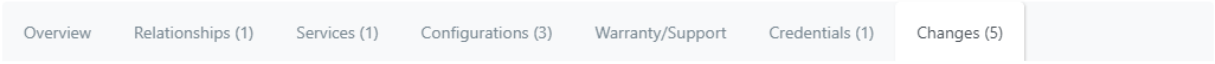
Configuration Objects can be linked but they can also be specifically assigned to a device. In this case they were assigned. Below are applications installed on the FTP Server and the DNS name for the FTP Server.



CONFIG TYPE	CONFIGURATION	DESCRIPTION
Application	Cerberus FTP Server	Used for SPEED and SalesForce FTPS Transmissions
Application	freeSSHd	(Decommissioned) Used for SPEEDE SFTP Transmission
FTPsite	ftp.acme.local	Site used by users to access files remotely

Recorded Field Changes

Field Changes were recorded as the device was updated in the IT Portal.

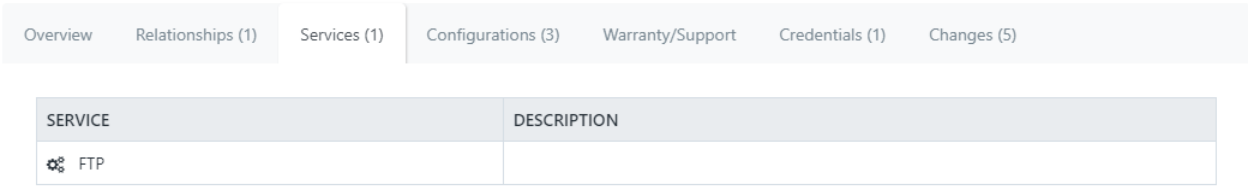


Field Changes

Old Value	New Value
Date/Time: 09/03/2021 15:02:33 PM **Changed By:** Cam LeBlanc **Field Name:** altlinkdescription web	**Date/Time:** 09/03/2021 15:02:33 PM **Changed By:** Cam LeBlanc **Field Name:** altlinkdescription webConsole
Old Value	**New Value**
Date/Time: 09/03/2021 15:02:28 PM **Changed By:** Cam LeBlanc **Field Name:** altlinkdescription webConsole	**Date/Time:** 09/03/2021 15:02:28 PM **Changed By:** Cam LeBlanc **Field Name:** altlinkdescription web
Old Value	**New Value**
Date/Time: 09/03/2021 15:01:48 PM **Changed By:** Cam LeBlanc **Field Name:** Description File Transfer (Ext	**Date/Time:** 09/03/2021 15:01:48 PM **Changed By:** Cam LeBlanc **Field Name:** Description File Transfer (Ext & Int)

Services

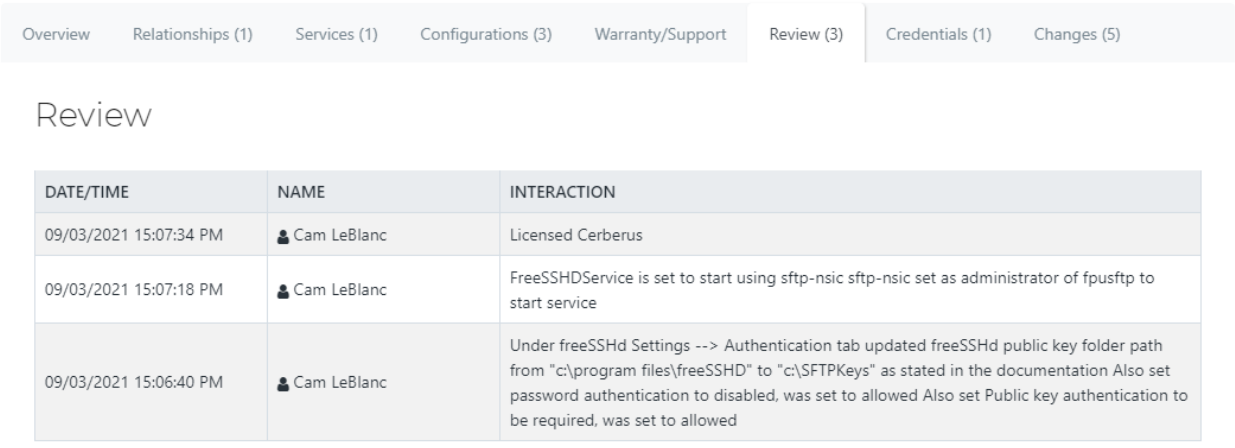
Documented that this server is running the FTP Service. This allows for services to be enumerated in the synopsis page.



Synopsis Page Listing Services

Review

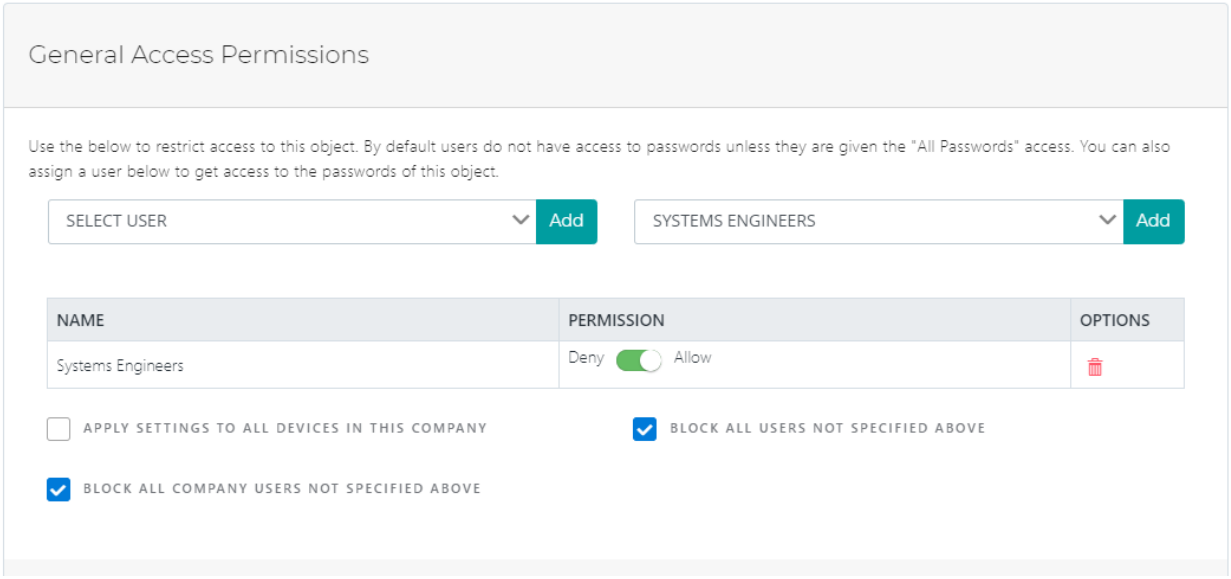
After the server was put into production, changes that occurred on the server were recorded via the Review tab



Securing Access

While editing this device, restrictions were put in place to ensure that only a group of users can access it. All other regular users were denied access via the “Block all users..” checkbox. Company users were also blocked. Company users are usually restricted from accessing login accounts used by your engineers. By default, all company objects can be accessed by users. You can set restrictions at a company level, object type level (i.e. Devices), or at an object level.

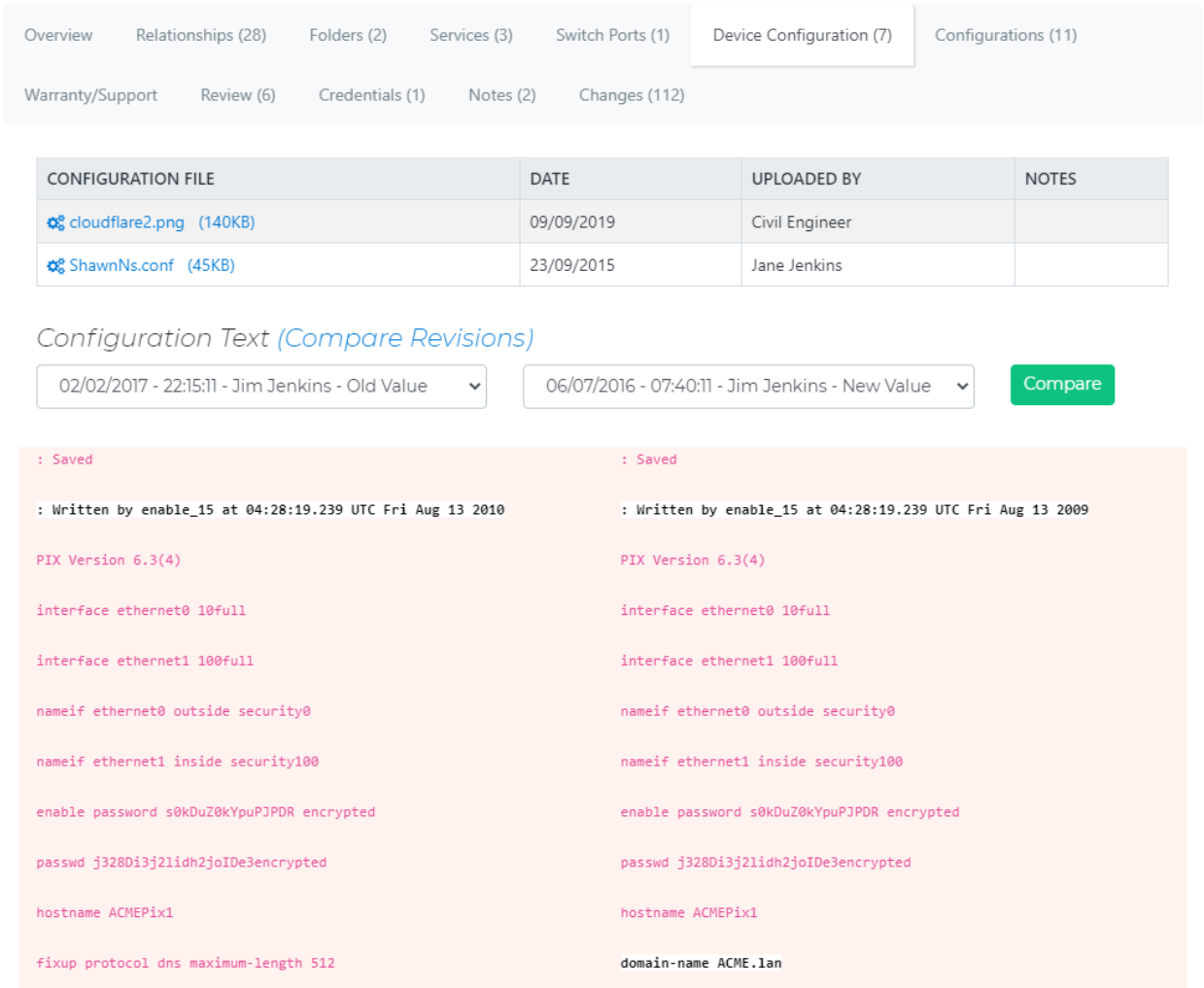
See KB for more information



Documenting Routers & Firewall

Configuration

The IT Portal has a configuration field for all devices. But the configuration fields are most helpful for Routers and Firewalls. As configurations are updated, each prior configuration is saved. You can use the compare feature to see how a configuration has changed over time. Below is an example of a firewall configuration. Highlighted in black are the differences between two sample configurations.



Documenting Switches

You can define groups of ports for switches. While editing the switch or a network interface for a device you specify where it is connected. For modular switches, ports can be defined with optional FPC and slot numbers.

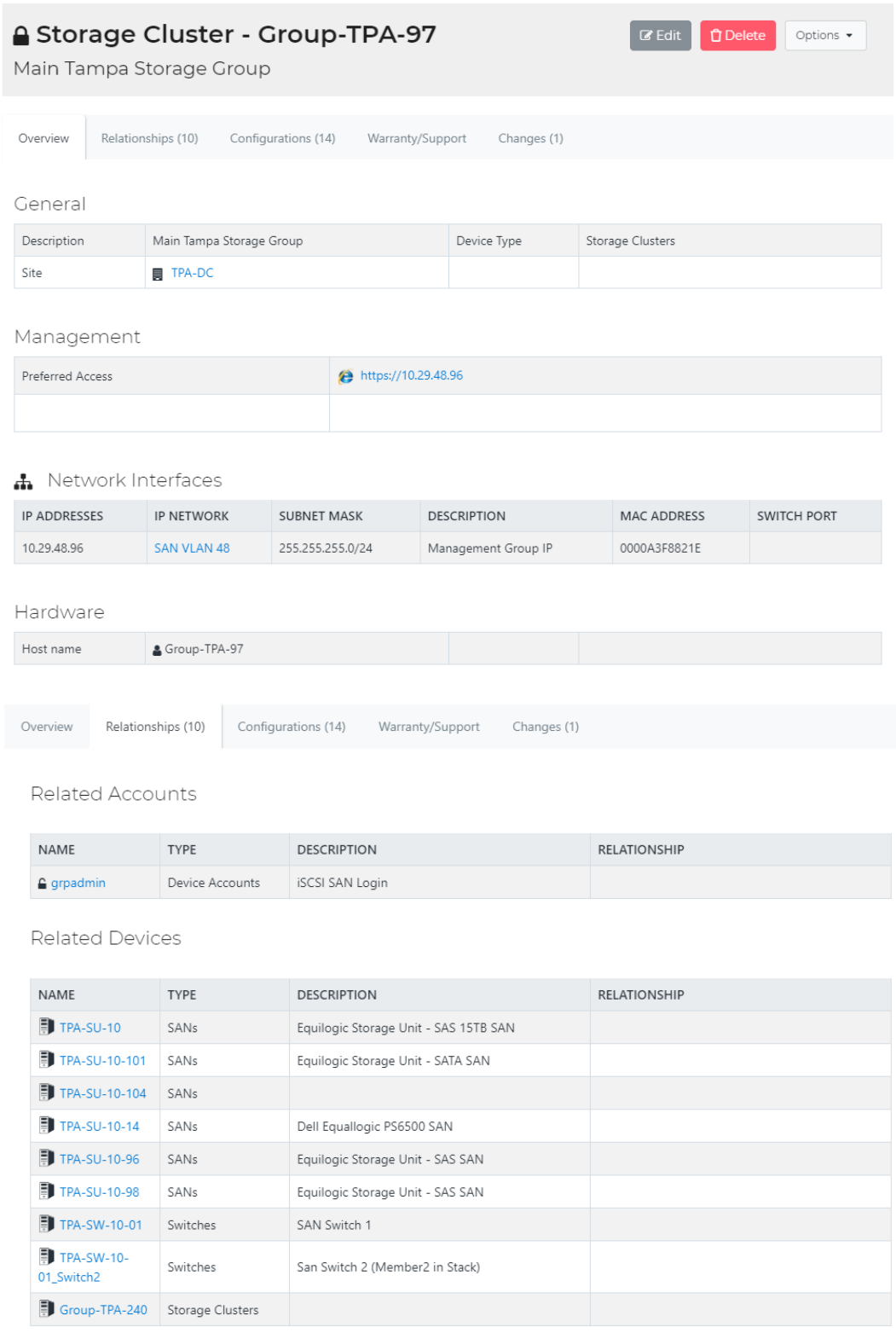
Network Interfaces

IP ADDRESSES	IP NETWORK	SUBNET MASK	DESCRIPTION	MAC ADDRESS	SWITCH PORT
					Dell-VRTX - 8 External Ethernet Ports - 1/0/1
					Backup Server - 1-8 - 3
192.168.59.212	10.10.32.0	255.255.255.0/24	Management IP	0005068A5F11	HP Switch 2 - HP2 - 21
192.168.59.55	Orlando Switch	255.255.255.0/24	t1313	1212132312	FailoverAC - 1010 - 123456/1/14

Documenting Clusters

Clusters are virtual devices that is hosted by multiple devices. They usually have an IP address for accessing the resource that is hosted by the cluster. Clusters can be services like databases, virtualization, file, and print services. Storage can also be shared in a clustered network raid environment or shared in a group management. When documenting all types of clusters be sure to document the virtual IPs and cluster resources as configuration objects. Be sure to link the devices that are

part of the cluster and the accounts used to login to the cluster.



Storage Cluster - Group-TPA-97

Edit | Delete | Options

Main Tampa Storage Group

Overview | Relationships (10) | Configurations (14) | Warranty/Support | Changes (1)

General

Description	Main Tampa Storage Group	Device Type	Storage Clusters
Site	TPA-DC		

Management

Preferred Access	https://10.29.48.96

Network Interfaces

IP ADDRESSES	IP NETWORK	SUBNET MASK	DESCRIPTION	MAC ADDRESS	SWITCH PORT
10.29.48.96	SAN VLAN 48	255.255.255.0/24	Management Group IP	0000A3F8821E	

Hardware

Host name	Group-TPA-97		

Overview | Relationships (10) | Configurations (14) | Warranty/Support | Changes (1)

Related Accounts

NAME	TYPE	DESCRIPTION	RELATIONSHIP
grpadmin	Device Accounts	iSCSI SAN Login	

Related Devices

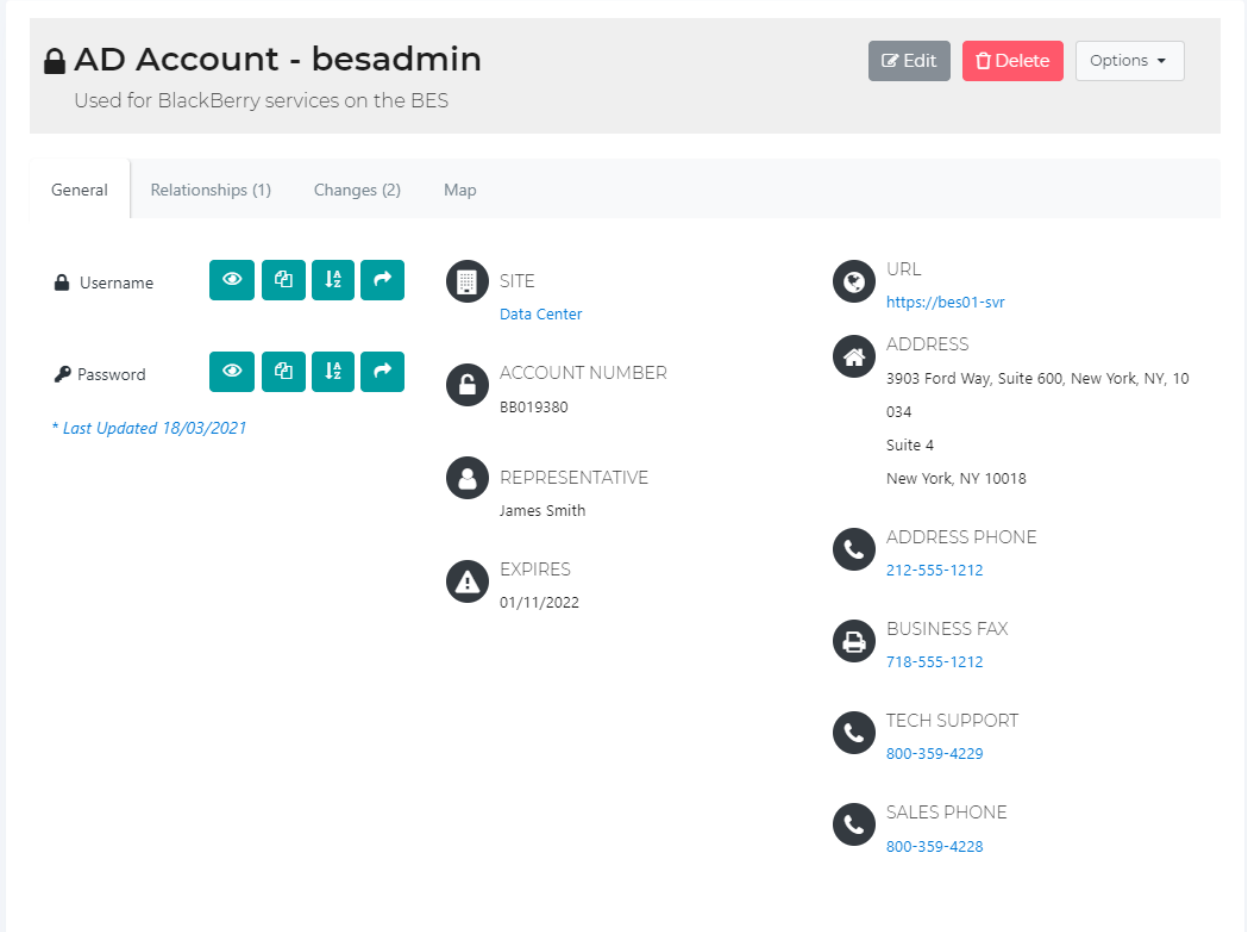
NAME	TYPE	DESCRIPTION	RELATIONSHIP
TPA-SU-10	SANs	Equilogic Storage Unit - SAS 15TB SAN	
TPA-SU-10-101	SANs	Equilogic Storage Unit - SATA SAN	
TPA-SU-10-104	SANs		
TPA-SU-10-14	SANs	Dell Equallogic PS6500 SAN	
TPA-SU-10-96	SANs	Equilogic Storage Unit - SAS SAN	
TPA-SU-10-98	SANs	Equilogic Storage Unit - SAS SAN	
TPA-SW-10-01	Switches	SAN Switch 1	
TPA-SW-10-01_Switch2	Switches	San Switch 2 (Member2 in Stack)	
Group-TPA-240	Storage Clusters		

Overview | Relationships (10) | Configurations (14) | Warranty/Support | Changes (1)

CONFIG TYPE	CONFIGURATION	DESCRIPTION
LUNs	VMStore-50	100TB LUN - Virtual Machines
LUNs	VMStore-51	100TB LUN - Virtual Machines
LUNs	VMStore-52	100TB LUN - Virtual Machines
LUNs	VMStore-53	100TB LUN - Virtual Machines
LUNs	VMStore-54	100TB LUN - Virtual Machines
LUNs	VMStore-55	100TB LUN - Virtual Machines
LUNs	VMStore-60	120GB LUN - Processes the Incoming Jobs
LUNs	VMStore-61	1.22TB LUN - SQL Quorum
LUNs	VMStore-62	500TB LUN - Data Warehouse 1
LUNs	VMStore-63	500TB LUN - Data Warehouse 2
LUNs	VMStore-64	500TB LUN - Data Warehouse 3
LUNs	VMStore-65	500TB LUN - Data Warehouse 4
LUNs	VMStore-66	500TB LUN - Data Warehouse 5
LUNs	VMStore-ISOs	ISOs and Templates

Documenting Accounts

Below is an example account used to manage a blackberry enterprise environment. Accounts are typically used to record login, subscriptions, and support accounts used by a company.

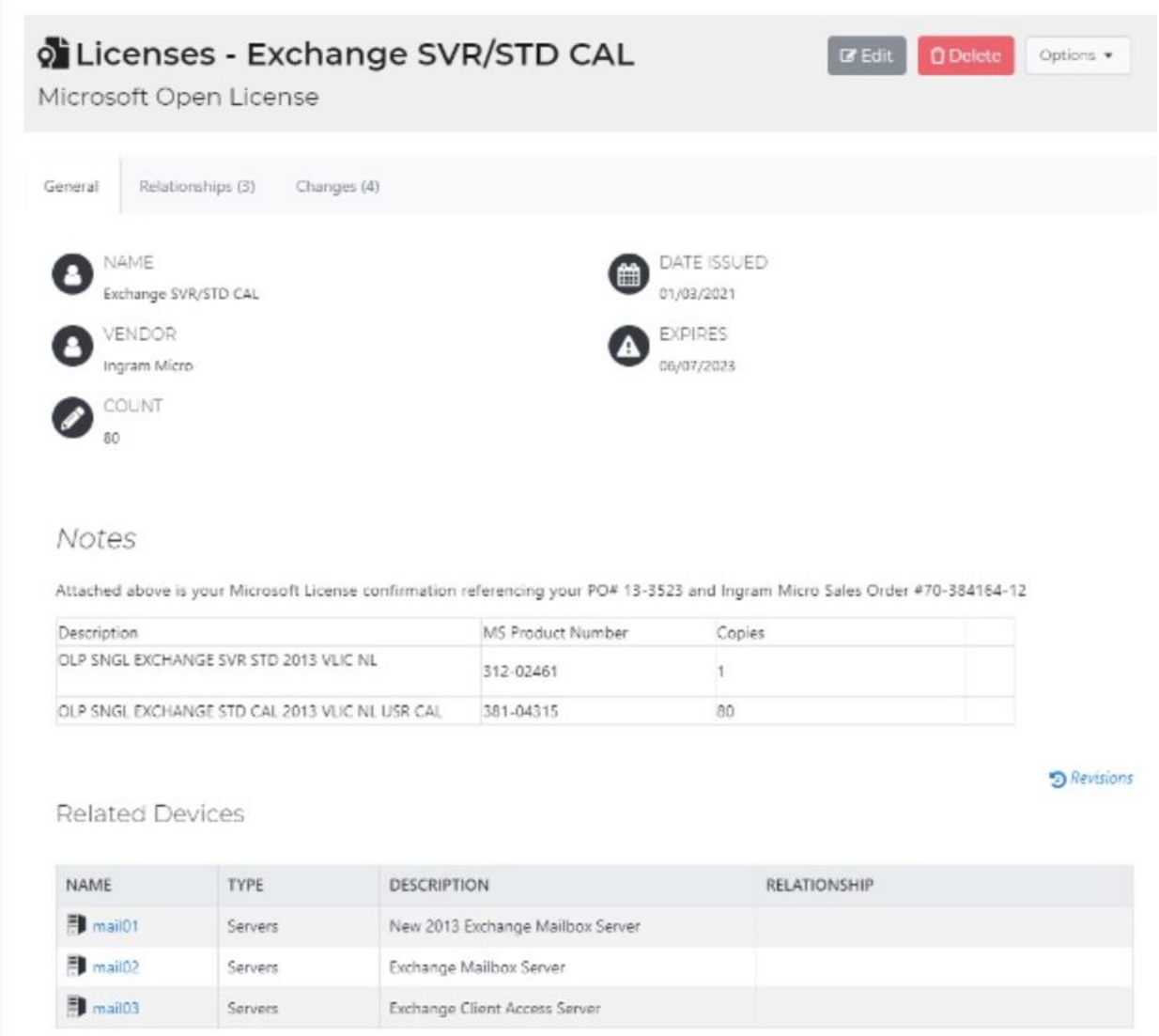


Related Devices

NAME	TYPE	DESCRIPTION	RELATIONSHIP
bes01-srv	Servers	New BlackBerry Enterprise Server	

Documenting Agreements

Below is a sample license from Microsoft for an exchange server environment. Keep track of agreements like licenses, support contracts, and SLAs. Ensuring you always have access to the needed info when renewing or rebuilding.



Licenses - Exchange SVR/STD CAL

Edit Delete Options

Microsoft Open License

General | Relationships (3) | Changes (4)

NAME
Exchange SVR/STD CAL

DATE ISSUED
01/03/2021

VENDOR
Ingram Micro

EXPIRES
06/07/2023

COUNT
80

Notes

Attached above is your Microsoft License confirmation referencing your PO# 13-3523 and Ingram Micro Sales Order #70-384164-12

Description	MS Product Number	Copies	
OLP SNGL EXCHANGE SVR STD 2013 VLIC NL	312-02461	1	
OLP SNGL EXCHANGE STD CAL 2013 VLIC NL USR CAL	381-04315	80	

Revisions

Related Devices

NAME	TYPE	DESCRIPTION	RELATIONSHIP
mail01	Servers	New 2013 Exchange Mailbox Server	
mail02	Servers	Exchange Mailbox Server	
mail03	Servers	Exchange Client Access Server	

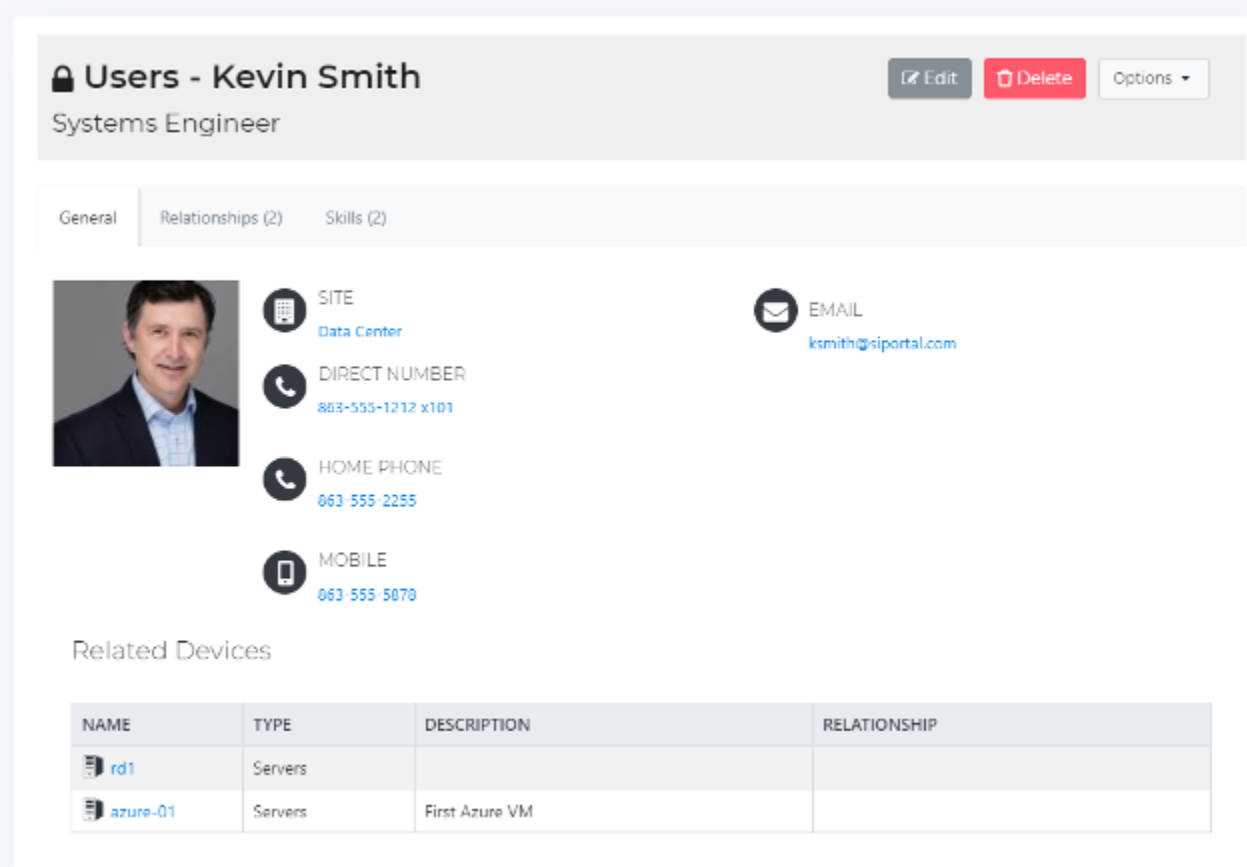
Documenting Contacts

Below is a sample contact for a user at a company. Record information regarding users and consultants that relate to a company.

* Link contacts to devices they may manage

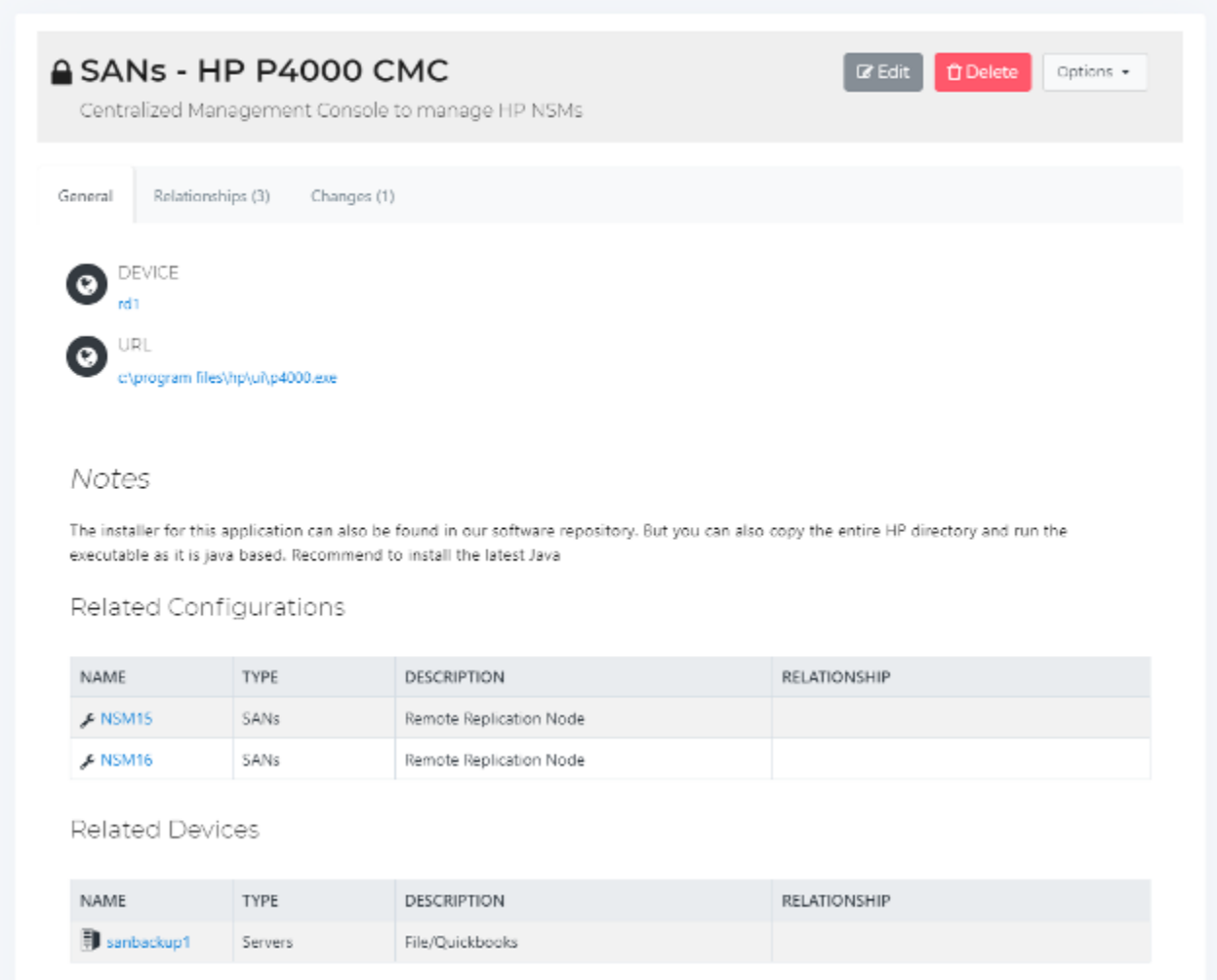
* Assign skill sets to contacts to quickly find expertise

* Assign a picture for verification of individuals entering data centers



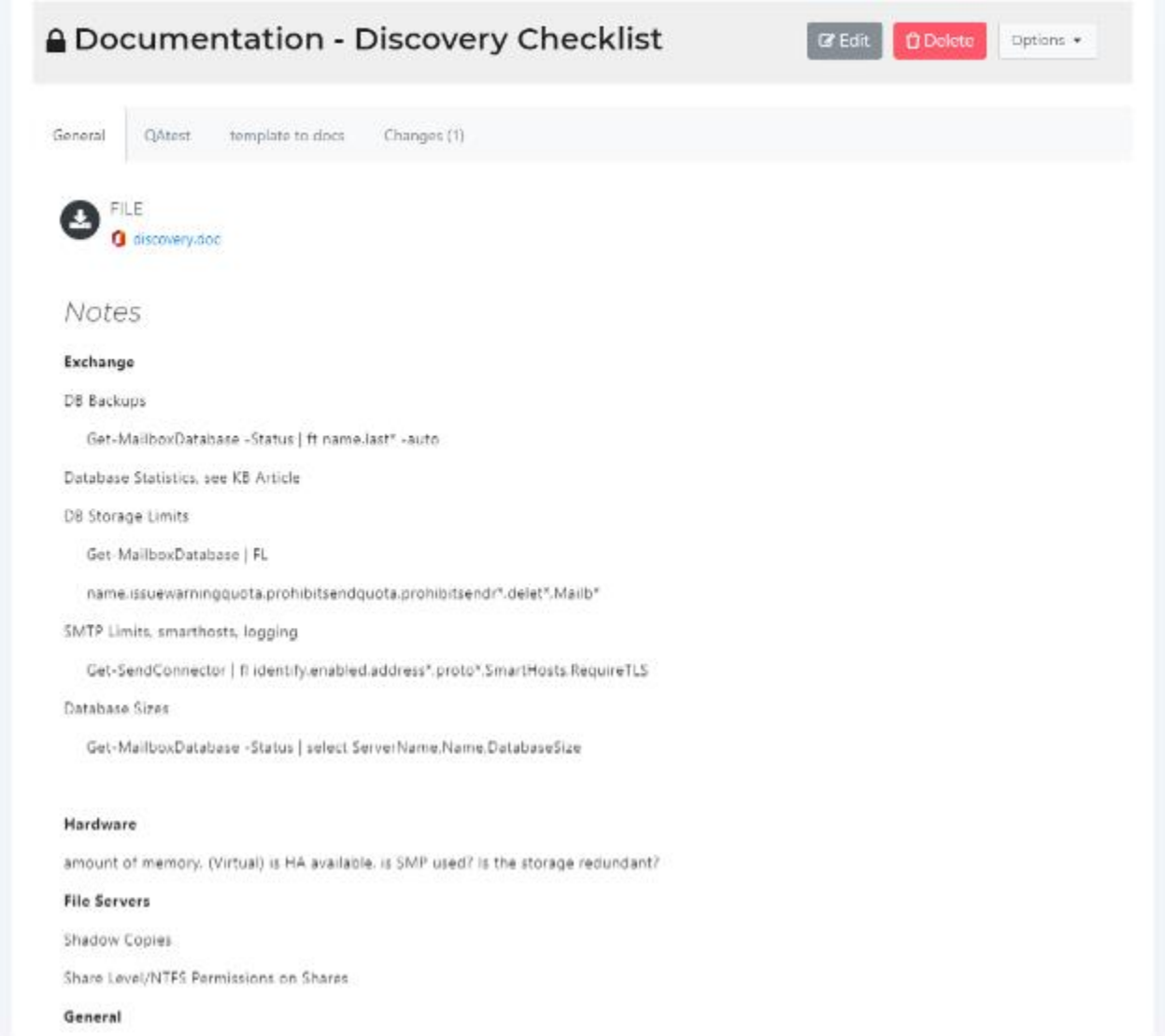
Documenting Configuration Objects

Below is a sample application documented in the IT Portal. Configuration Objects are tangible and non-objects that are usually assigned or to attached to devices. Examples of configuration objects includes websites, disks, LUNs, applications, and Scheduled Tasks.



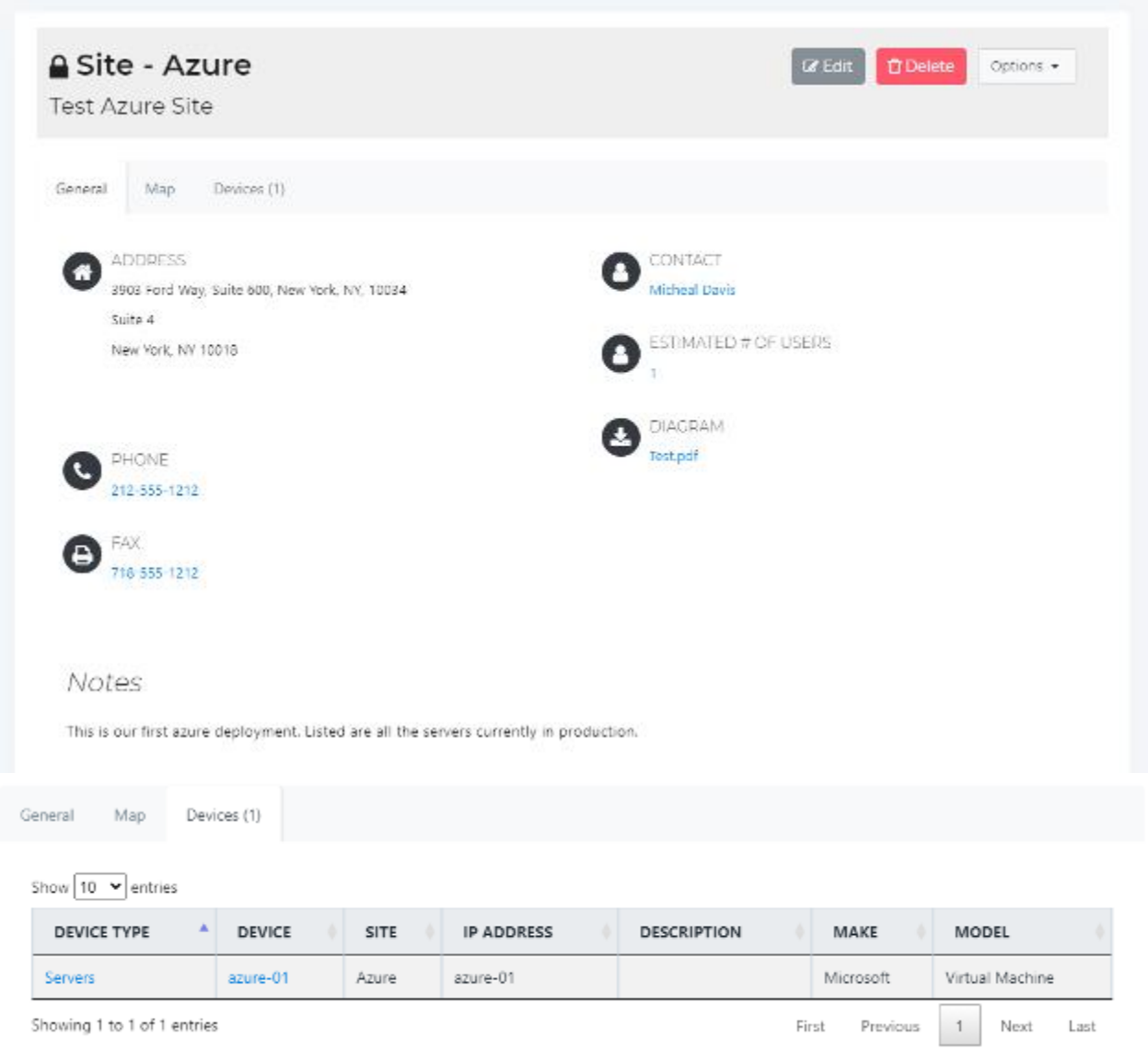
Documenting Documents

Save important files, images, and notes about your environment as documents. Link them to devices and other objects. Sample Documents include Build Books, Diagrams, Check Lists, Forms, DR Documentation, and Policies and Procedures.



Documenting Sites

Sites are groupings of devices. A site can be a physical site like a company office, a data center, or a campus. Access a site to view address information, network diagrams, IP networks, devices, and services running on those devices.



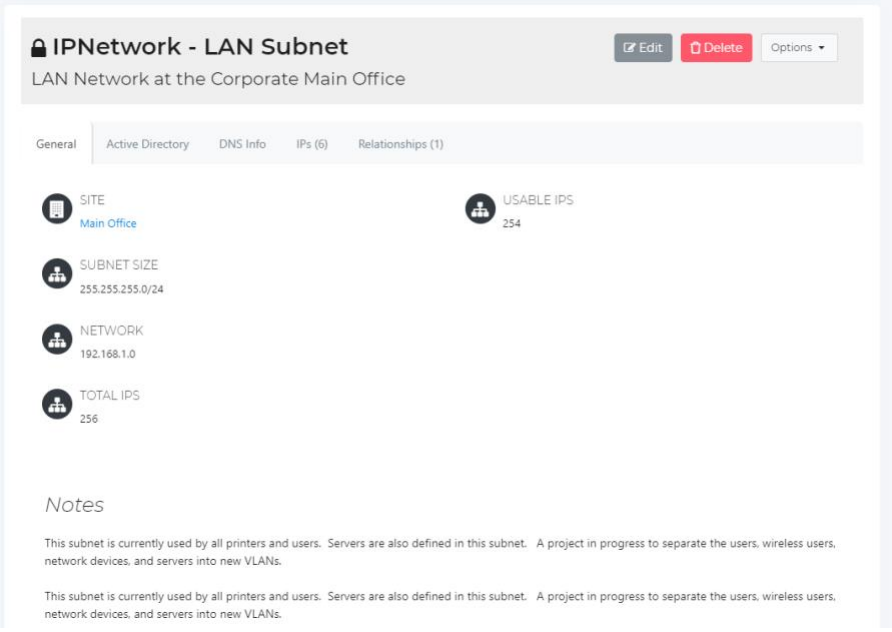
Documenting Facilities

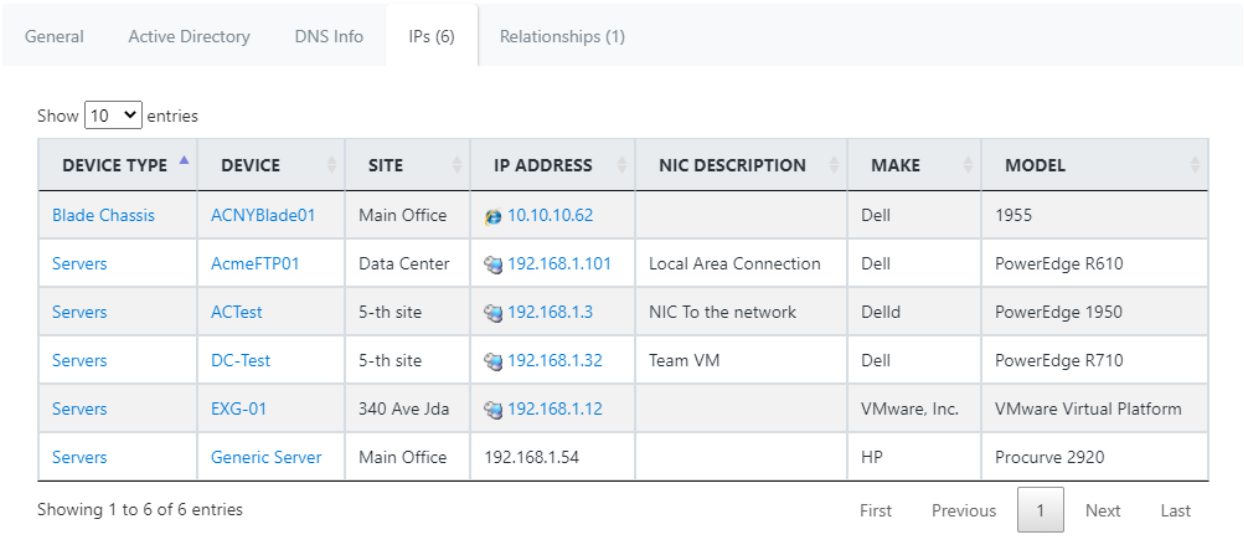
Facilities are groupings of devices that exist in a site. If a site was considered a campus, a facility can be a building in that campus, a floor, a suite, etc. Viewing a facility in the IT Portal is like a site as shown above.

Documenting Cabinets

Cabinets are groupings of devices that exist in a Rack/Cabinet. When editing a device, you can define what cabinet it is located in. This can be handy when locating where a device is physically housed in a rack. Viewing a cabinet is in the IT Portal is like a site as shown above.

Documenting IP Networks

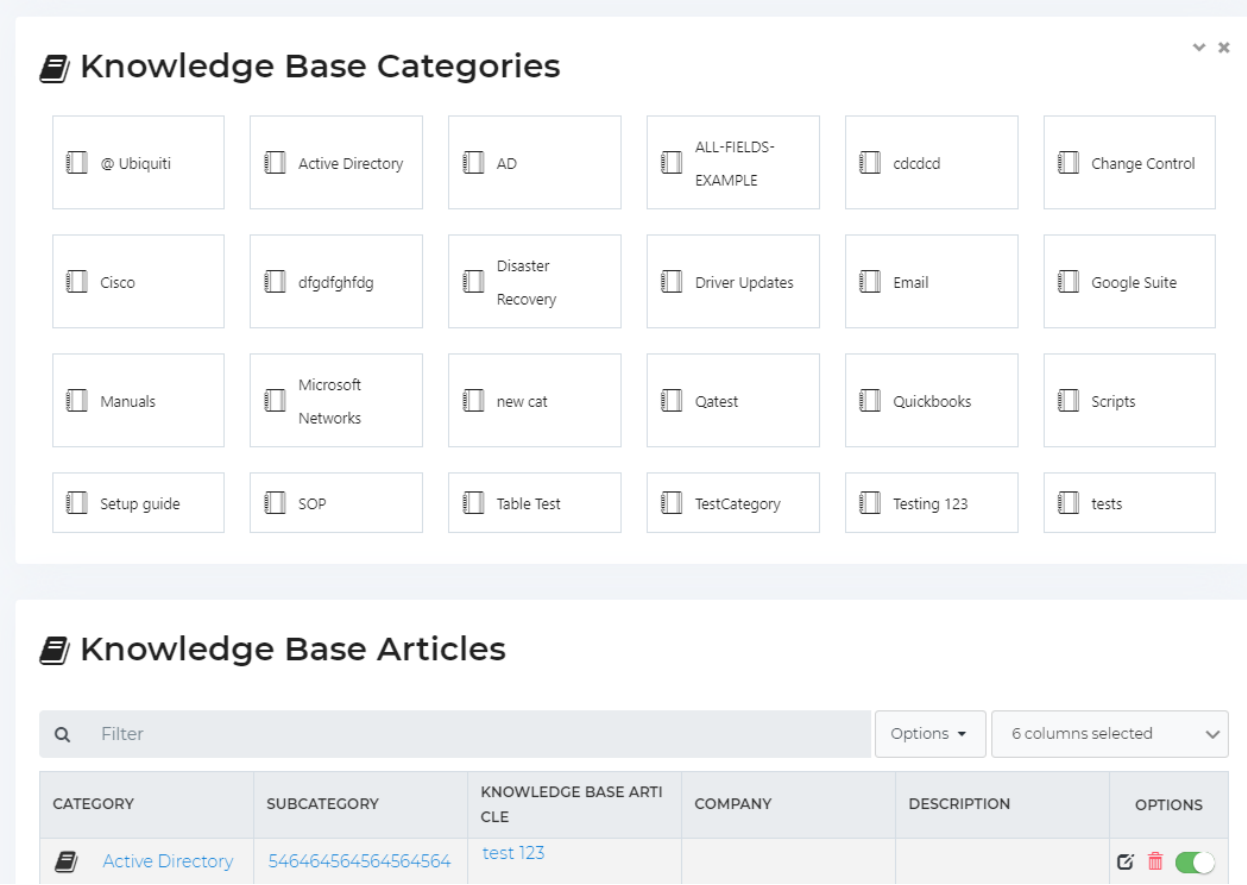




IP Networks let you group devices by logical IP Subnets. You can specify the IP Network for a device while editing it. You can also use the “Move Devices” wizard shown below.

Documenting KB Articles

Create searchable knowledge base articles in the IT Portal. KB articles should be used as general how to guides regarding the technologies that you use to support your infrastructure. Information relating directly to a company should be saved as a document. For example, a script to install pre-requirements for a product can be in the KB, but a document showing the results of running the script for a device should be kept under documents.



Additional Information

If you need additional information, be sure to review our website located at https://www.it-portal.com/v4/

We would also welcome you to view:

Administrator Guide

https://kb.siportal.com/?U=oKOqA2A2

Administrator Training

https://www.youtube.com/watch?v=bREqqqnBQWs

Onboarding Guide

https://www.it-portal.com/releases/IT-Portal-Onboarding-Guide.pdf