Remote Support VPN Requirements and Capabilities

The Vectra Remote Support VPN may be enabled in the Cognito Detect platform. A Cognito Detect brain device with Remote Support VPN enabled allows authorised Vectra Support and Analyst personnel access to the Cognito Detect appliance. It is important to outline the scope of the Remote Support VPN, what it can and can't do and the requirements necessary to enable it.

The Remote Support VPN is a required component of the Vectra Sidekick service, it may also be utilized by Vectra Support and Analyst personnel when remote support is beneficial in addressing a platform support issue.

Remote Support VPN Scope

While the Remote Support VPN is enabled and operational, authorised Vectra Personnel will have access to only the following components.

Cognito Detect UI

This is the same web UI accessible from the local network by local users, the dedicated Vectra Admin (vadmin) account has administrative privileges on the Cognito Detect UI but all actions are audited and logged. This access grants no further access to any part of the customer environment.

Cognito Detect Shell

The Cognito Detect Shell is a Bash (Bourne Again Shell) command line system. It is only used for low level administrative work or troubleshooting. Vectra Support or Analyst personnel may use this to assist in support matters, debug any errors with the customer appliance, investigate detections or connectivity issues on customer request. It may only be used from a secure central system inside the Vectra corporate network. This central system requires 2FA in order to log in and all activity is logged and audited. The credentials used to access this system are centrally controlled and access can be revoked at any time. All credentials are also subject to minimum strength, complexity and uniqueness requirements.

Users accessing the Cognito Detect Shell only have access to the local system and have no further access to any part of the customer environment. Updates and additional software may only be applied from secure authorized Vectra repositories.

Requirements

In order to enable Remote Support VPN the following actions are required.

Your Internet access should permit:

- TCP port 443 to vpn.vectranetworks.com (74.201.86.229)
- UDP port 9970 to vpn.vectranetworks.com (74.201.86.229)

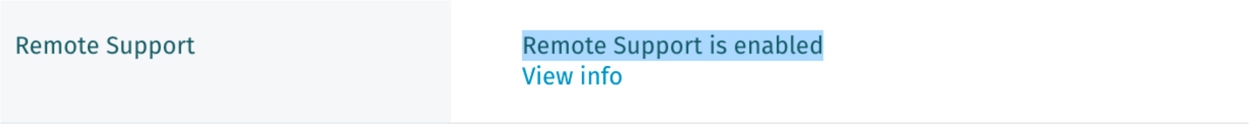
For security reasons the Cognito Detect appliances validate SSL certificates for all Remote Support VPN connections. Any SSL inspecting firewalls must disable SSL inspection for these connections as SSL interception will cause the connections to fail.

Customers with mandatory proxies in the Internet connection pipeline, where no direct access to the Internet is possible, should contact Vectra Support to discuss implementation options.

Following these changes, with an administrator level account, you need to navigate in the Cognito Detect UI to **Settings, Services, Remote Support**. This page will display the status of the Remote Support VPN. By default, this will be disabled.

To enable click on Edit and toggle the setting to on.

Once enabled the user interface will report “**Remote Support is enabled"**.



Remote Support	Remote Support is enabled View info

VPN may also be enabled with the “vectra” user from the SSH or console CLI.

To enable the Remote Support VPN:

```
set vpn enable on
```

To disable the Remote Support VPN:

```
set vpn enable off
```