Mandiant

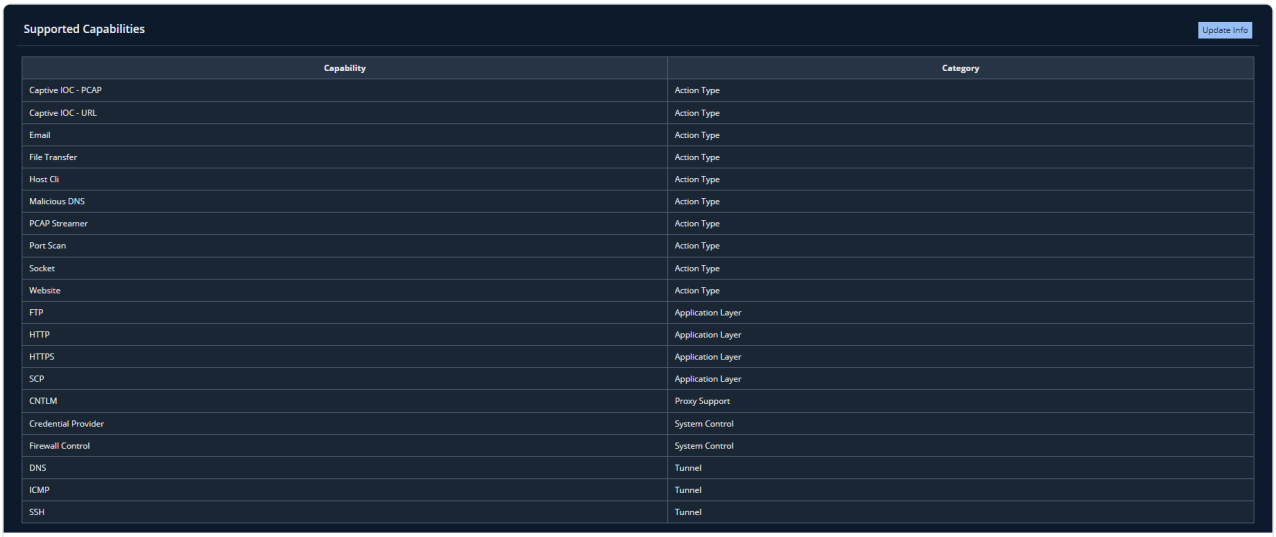
SUPPORTED ACTION TYPES FOR ACTORS

The Actor platform determines specific Actions that can be run. Refer to this table to see which Actions are supported on which Actor platforms.

Actor Platforms→ Action Type ↓	Windows Endpoint	macOS Endpoint	Linux Network (CentOS/RHEL/Rocky Linux & Amazon Linux 2)	Linux Endpoint (Ubuntu)
PCAP (Hex)	✔	✔	✔	✔
Captive IOC (PCAP)			✔	
Captive IOC (URL)			✔	✔
Host CLI	✔	✔	✔	✔
Website	✔	✔	✔	✔
Socket	✔	✔	✔	✔
File Transfer	✔	✔	✔	✔
Port Scan	✔	✔	✔	✔
Email		✔[1]	✔	✔
DNS	✔	✔	✔	✔
Cloud			✔	✔

[1] MacOS Actors support only legacy protocols (IMAP/POP/SMTP) and Gmail.

In addition, you can see supported capabilities for specific Actors that are registered to your Director by selecting **Edit** from an Actor's Action menu. This screen contains a **Supported Capabilities** table that shows you what that particular Actor supports.



Supported Capabilities

Update Info

Capability	Category
Captive IOC - PCAP	Action Type
Captive IOC - URL	Action Type
Email	Action Type
File Transfer	Action Type
Host Cli	Action Type
Malicious DNS	Action Type
PCAP Streamer	Action Type
Port Scan	Action Type
Socket	Action Type
Website	Action Type
FTP	Application Layer
HTTP	Application Layer
HTTPS	Application Layer
SCP	Application Layer
CNTLM	Proxy Support
Credential Provider	System Control
Firewall Control	System Control
DNS	Tunnel
ICMP	Tunnel
SSH	Tunnel

Supported Capabilities Table for an Actor

- The **Application Layer** and **Tunnel** categories relate to File Transfer Actions. Based on the specific type of Action, one of the capabilities is required for an Actor to be able to run the Action.
- **CNTLM** is an external piece of software that can optionally be installed during the Actor installation process. If you choose not to install this component, then the Actor won't have the associated capability.
- **Credential Provider** relates to running Host CLI actions interactively on Windows Actors (protected and non-protected).
- The Credential Provider is dependent on selecting the installation option for it during the Windows installation, as well as these three Windows settings being setup properly:
  - Secure Signin: Disabled
  - Legal Caption: Empty
  - Legal Notice: Empty
- **Firewall Control** is an install-time option on Linux Actors, so users can opt out of having the actor modify firewall rules, if appropriate.
- The **DNS** and **ICMP** capabilities are dependent on selecting the TAP driver as part of the Windows installation (all other OSes are not impacted by this).