FORESCOUT


# Using Forescout for Security and IT Operations During COVID-19

The COVID-19 (novel coronavirus) pandemic has created serious IT and security challenges for Federal civilian government departments and agencies which must continue to meet their mission while reducing the on-premise workforce to limit health risk. The situation has also created an opportunity to adapt existing and new cyber defense technologies that the agencies have invested in previously such as those under the Continuous Diagnostics and Mitigation (CDM) program. As increasing numbers of employees work from home during the COVID-19 pandemic, new obstacles arise such as scaling and securing Virtual Private Networks (VPN) and remote access. For example, many agencies had previously not established or required mature security practices for VPN networks and remote workers at such a large scale and this situation is changing rapidly.

## Meeting the Challenge with Forescout

Forescout is uniquely positioned to help agencies secure this suddenly increasing remote workforce. Agencies' network administrators need to extend the same level of insight and control to remote endpoints when they connect to corporate networks by VPN as they would for on-campus devices. These methods include compliance assessment and policy-based endpoint and network controls which can help secure users while remotely connecting corporate or personal devices to corporate networks. Additional methods include security and policy compliance monitoring and the ability to quickly act on threats.

Forescout customers also have the option to have remote employees install a SecureConnector (SC) client on their personal Windows/Mac/Linux PC or laptops, enabling network administrators to understand the security posture of these devices and manage them accordingly based on a risk assessment for each scenario. Utilizing these methods, Forescout customers can ensure both government-owned managed devices and personally-owned unmanaged devices connecting through VPN are secure prior to accessing agency resources as well as continuously, while the devices remain connected to the agency's network.

Network administrators must now see and identify these remote devices the moment they connect to the corporate network, just like on-campus devices in the past. This extended visibility helps to minimize risk in the new work-from-home environment. Next, they need to ensure those devices are, and remain compliant, regardless of the specific location from which they connect. The Forescout platform identifies and secures devices connecting by VPN, with or without agents, thereby helping to ensure security hygiene, device compliance and a reduced attack surface.

Forescout allows customers to identify VPN clients and enforce policies on:

- Managed Windows Devices
- Managed Mac Devices
- Managed Linux Devices
- BYOD/Unmanaged Devices

Managed devices connecting via VPN are subject to the same Pre-connect and Post-connect security policies that are applied to on-premises connecting devices. The Forescout platform can also help address Bring Your Own Device (BYOD)/unmanaged devices connecting through the VPN. Such devices are immediately flagged by Forescout as non-corporate and placed in the "Unmanaged Devices Connecting Through VPN" category. This grouping together of BYOD/unmanaged connected devices allows system administrators to easily monitor them for certain undesirable characteristics or behaviors. Agency system administrators can then rapidly make informed decisions about denying or limiting access to network resources. In this scenario, Forescout customers can deploy the optional lightweight SC client on to the BYOD/unmanaged device. Combining the Forescout VPN Concentrator Plugin with the SC client allows administrators to enforce greater host and network controls over unknown VPN connected devices, thereby ensuring policy-defined security requirements are met before accessing corporate network resources. As an example, the VPN Concentrator Plugin can disconnect users and prevent them from reconnecting, if necessary, through the network's authentication server, such as Radius or active directory (AD).

Forescout can provide a standard policy template that identifies the VPN segment first to determine what endpoints are managed and unmanaged by the agency. This expedites the process of grouping devices into their appropriate category and applying access controls. The screenshot in Figure 1 shows this policy in the Forescout Policy Manager console.

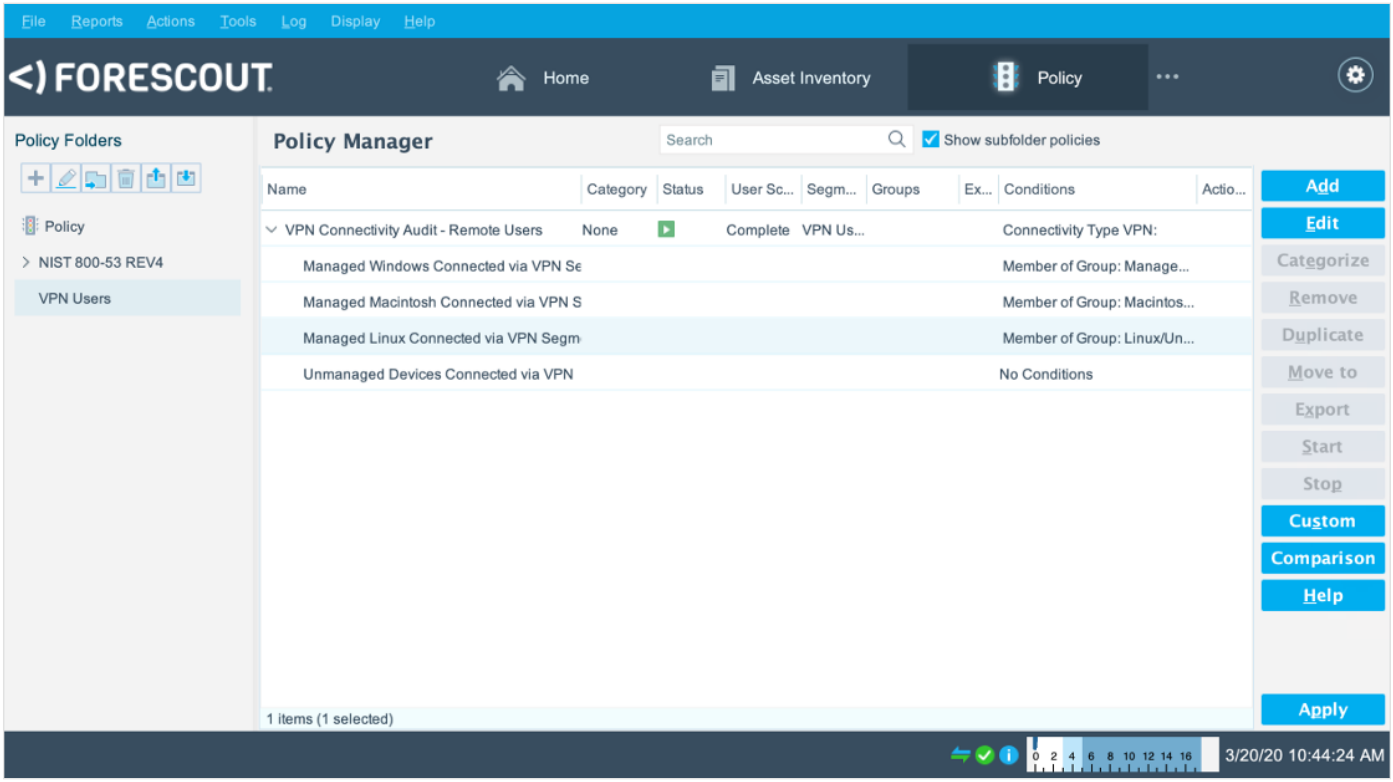


*Figure 1 – Forescout policy to identify managed and unmanaged devices connecting via VPN.*

If there are questions on how to configure Forescout to achieve the outcomes listed above please consult the *Forescout's VPN Integration Primer: Device Visibility, Compliance and Control for Remote Teleworkers* and contact your Account Manager and Engineer for additional assistance.


FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591


Learn more at Forescout.com