

The QuickStart FortiNAC Service

Service Overview

Whether deploying new devices into your environment or migrating from another vendor or legacy technology, it's crucial to ensure the right features and functionalities are enabled when you're integrating a new solution. When the technology is deployed correctly the first time, you get the best protection with all the necessary features, meeting your strategic and time-to-value needs.

FortiNAC (network access control) QuickStart is a consulting service that helps you with the deployment of your FortiNAC solution into a new environment. The service aims to assist you in accelerating the time-to-adoption of your FortiNAC solution based on predefined, standardized phases. Having completed thousands of implementations, Fortinet follows a structured process to deploy your solution. Our Professional Service experts assess your requirements and then efficiently deploy your new FortiNAC while facilitating knowledge transfer and assisting in introducing the targeted FortiNAC into your environment.

Business Outcomes

- Day-one threat mitigation
- Expert assistance
- Best-practice deployment
- Faster time-to-value
- Timely product adoption

Service Matrix

The following table describes the predefined deployment options:

Service options	Standard	Advanced
Environment size	Up to 1,000 endpoints and/or single site	Up to 10,000 endpoints and/or multiple sites
Product installation and configuration	1 FortiNAC Control and Application VM or Appliance	1 FortiNAC Control and Application VM or Appliance and 1 FortiNAC Manager VM or Appliance
Network access policy development and enforcement	Up to 5 managed devices	Up to 15 managed devices
Agent installation	Up to 5 users	Up to 5 users
Access and compliance policies	Up to 10 policies	Up to 10 policies
Device profiling rules	Up to 10 rules	Up to 10 rules

Scope and Deliverables

Fortinet will work with you and perform the following tasks:

Review and Plan

Fortinet will review the project scope and milestones and capture all the necessary details of the proposed configuration and determine the timing to accommodate any change window. The final project scope will be reviewed and mutually agreed upon with you before moving to the next stage.

Design and Deploy

The Fortinet team will work on the FortiNAC configuration based on the requirements agreed upon during the planning phase. This includes basic network configuration, certificate installation, high availability setup, and more. Through these steps, FortiNAC enables devices and users access to necessary resources while blocking restricted and potentially malicious access. It also minimizes risks and the spread of malware by ensuring the integrity of devices before they connect to the network. The portal configuration will also help you monitor the network on an ongoing basis, giving you the tools to easily adjust access levels based on network traffic changes.

Test and Validate

Fortinet will perform an initial testing of the new FortiNAC product on the production system—this may include basic health checks, high-availability checks, and functional checks prior to turning the solution live. Fortinet will then provide support during your go-live deployment. Minor revisions or fine-tuning can be made if necessary.

Documentation and Knowledge Transfer

Fortinet will deliver an “as-built” document that describes key implementation elements of the deployed configuration and baseline system check results. Fortinet will then conduct a knowledge transfer session with you so that you’re familiar with your new FortiNAC environment.

Hand-off and Disengage

Fortinet will then hand over all the documentation, get the project sign-off, and close the project.

Please contact your Fortinet partner or your sales representative to order QuickStart Services.

