SANGFOR

NGAF

Best Practices for Scenarios_NGAF Correlate to Cyber Command Guide

Version 8.0.17

Change Log

Date	Change Description
Nov 1, 2020	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Basic Configuration

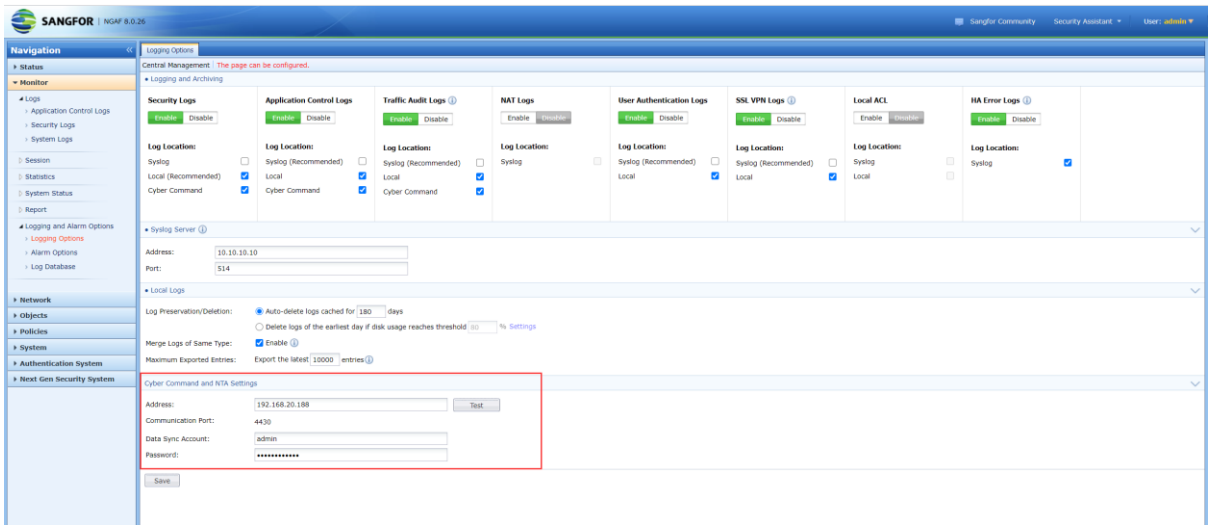
1. The communication ports between NGAF and Cyber Command are as follows:

Cyber Command	NGAF accesses TCP port 4430 of CC CC accesses TCP port 7443 of NGAF	One-way configuration for NGAF (standard) Two-way configuration for NGAF+CC (high security)	NGAF can upload botnets and webshell backdoors. When the hacker link produces a security event to CC, which can correlate with NGAF for threat blocking and application control.

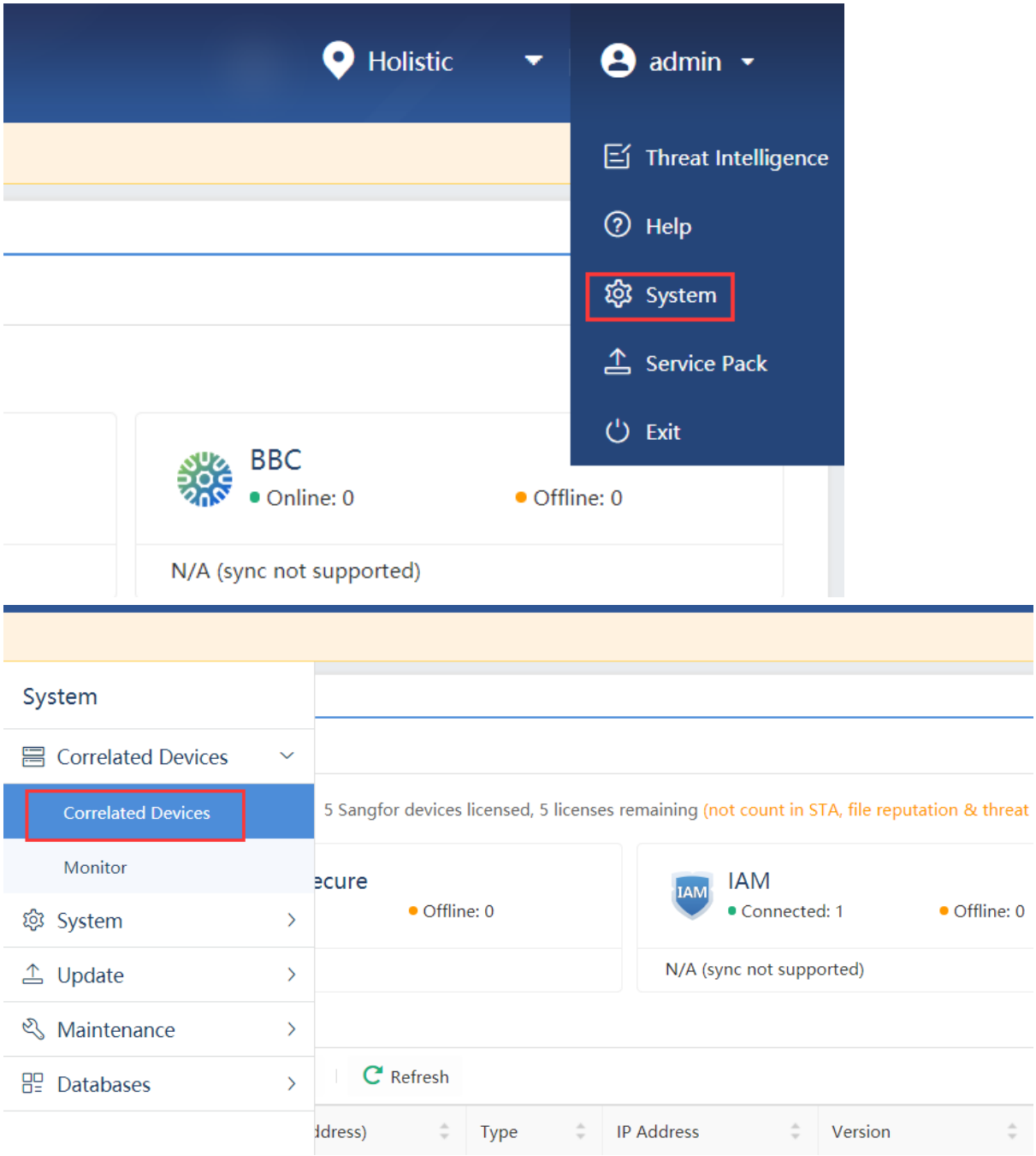
Chapter 2 Configuration

The configuration steps are as follows (need to ensure network connectivity between Cyber Command and NGAF):

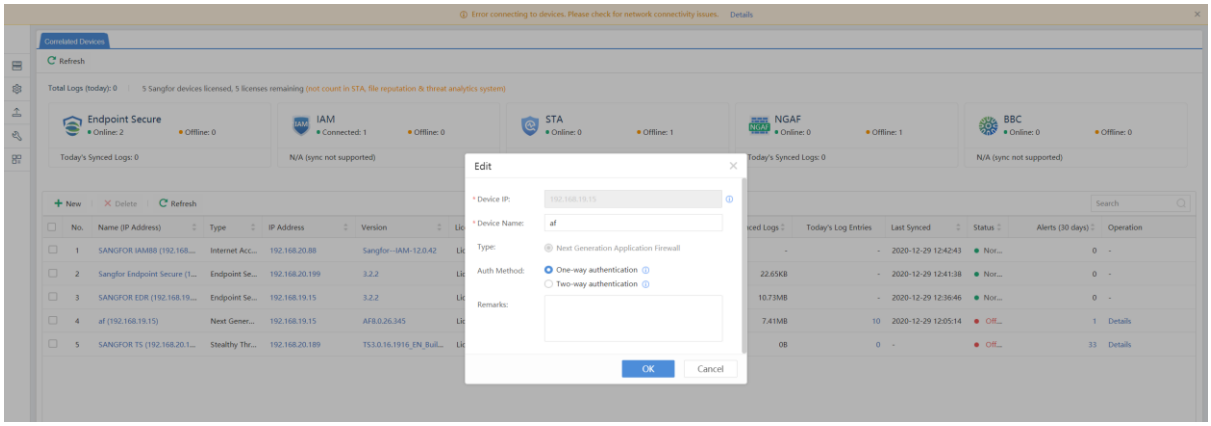
1. First configure Cyber Command information on NGAF and save it.



2. After NGAF synchronizes the information Cyber Command, the Correlated Devices page on Cyber Command will automatically add this Cyber Command. At this time, the authentication method on the Cyber Command side is one-way authentication by default.



3. If the authentication account password is configured on the NGAF side, after NGAF synchronizes the authentication information to Cyber Command, the default one-way authentication on Cyber Command will not affect the use of the function.



4. If you need to strengthen the security mechanism, you can edit the authentication method of the NGAF device on the Cyber Command side as: two-way authentication. And ensure that the authentication account passwords on both sides are configured to be consistent.