RayVentory

Smarter Software and Hardware Inventory

Quick Guide RayVentory - Disable FIPS

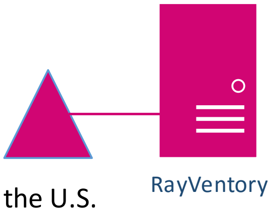
Date: 24.08.2015

Firma	**Raynet GmbH**
Straße	Technologiepark 20
PLZ Ort	33100 Paderborn

RayVentory is part of RaySuite.

Quick Guide RayVentory - FIPS

This guide is designed to configure your RayVentory server in a FIPS Environment.



Original Microsoft Summary
The United States Federal Information Processing Standard (FIPS) defines security and interoperability requirements for computer systems that are used by the U.S. federal government. The FIPS 140 standard defines approved cryptographic algorithms. The FIPS 140 standard also sets forth requirements for key generation and for key management. The National Institute of Standards and Technology (NIST) uses the Cryptographic Module Validation Program (CMVP) to determine whether a particular implementation of a cryptographic algorithm is compliant with the FIPS 140 standard. An implementation of a cryptographic algorithm is considered FIPS 140-compliant only if it has been submitted for and has passed NIST validation. An algorithm that has not been submitted cannot be considered FIPS-compliant even if the implementation produces identical data as a validated implementation of the same algorithm.
Source: https://support.microsoft.com/en-us/kb/811833

The Administration Server will not work correctly as long FIPS is enabled . Nevertheless FIPS is not recommend anymore.
Source: http://blogs.technet.com/b/secguide/archive/2014/04/07/why-we-re-not-recommending-fips-mode-anymore.aspx

Before you proceed

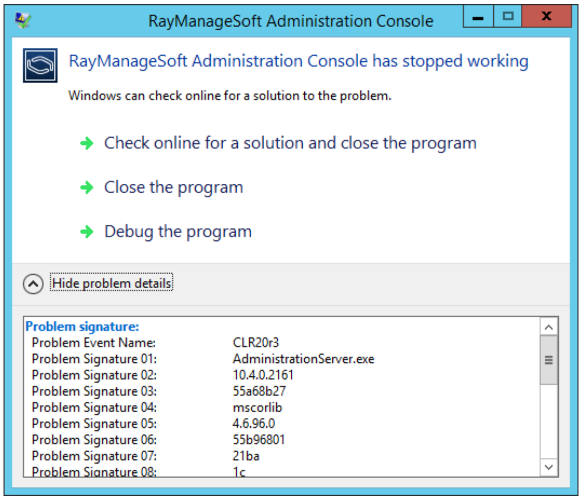
This guide assumes:

- The RayManageSoft Administration Server is already setup and preconfigured.
- You are familiar to the local and/or global security policy management for Microsoft Windows.

The RayVentory release notes and full-size documentation are available in addition to this document.

I. Purpose

As long as FIPS is enabled the RayManageSoft Administration Server Application will not start. The following error occur on start of the console:


RayManageSoft Administration Console

RayManageSoft Administration Console has stopped working

Windows can check online for a solution to the problem.

- Check online for a solution and close the program
- Close the program
- Debug the program

Hide problem details

```
Problem signature:
  Problem Event Name:        CLR20r3
  Problem Signature 01:      AdministrationServer.exe
  Problem Signature 02:      10.4.0.2161
  Problem Signature 03:      55a68b27
  Problem Signature 04:      mscorlib
  Problem Signature 05:      4.6.96.0
  Problem Signature 06:      55b96801
  Problem Signature 07:      21ba
  Problem Signature 08:      1c
```

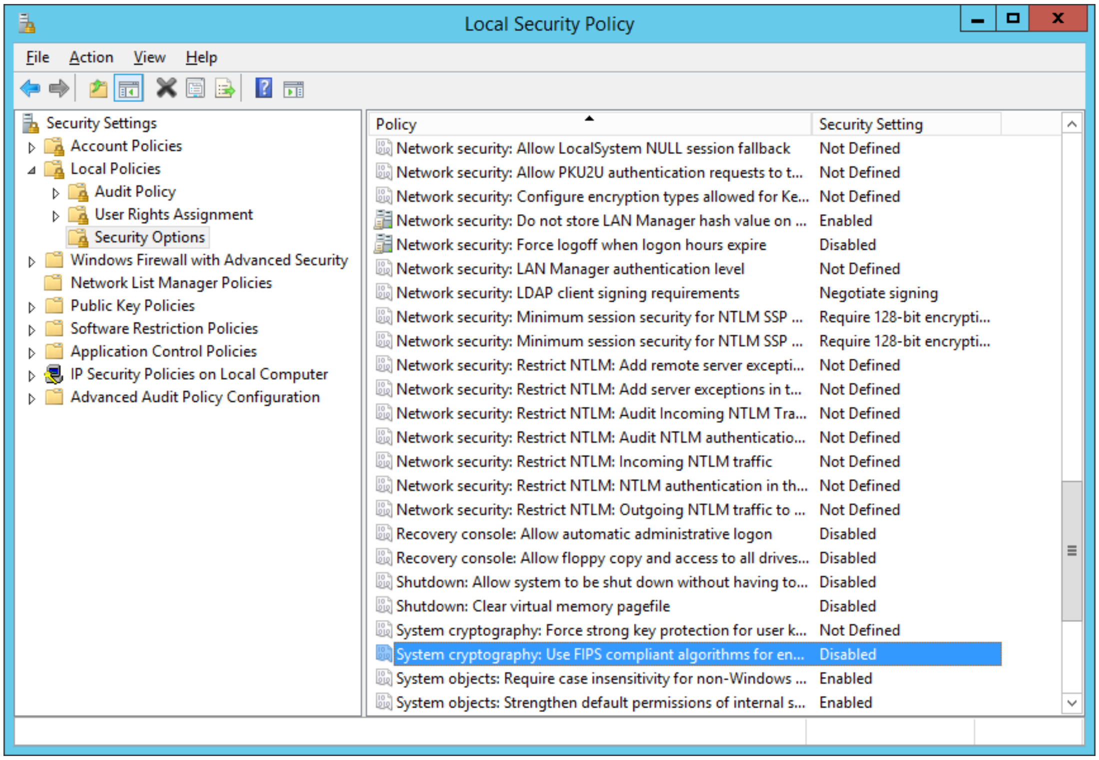
Problem signature:
Problem Event Name: CLR20r3
Problem Signature 01: AdministrationServer.exe
Problem Signature 02: 10.4.0.2161
Problem Signature 03: 55a68b27
Problem Signature 04: mscorlib
Problem Signature 05: 4.6.96.0
Problem Signature 06: 55b96801
Problem Signature 07: 21ba
Problem Signature 08: 1c
Problem Signature 09:
System.InvalidOperationException …

Close the problem message and disable FIPS.

II. Solution (Disable FIPS)

To disable FIPS you need to edit the system security policy. This can either be done global or local; Based on the membership and Policy of an Active Directory.
Global: For modifying a global policy use tools like Group Policy Management Console (GPMC), Group Policy Editor (GPEDIT) and Resultant Set of Policy (RSoP). Consider contacting your Active Directory Administrator.
Local: For modify the local security you can go with the Security Policy Editor (Secpol).

In both way you will edit the same security policy, shown here as an example of a local policy:


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to t...	Not Defined
Network security: Configure encryption types allowed for Ke...	Not Defined
Network security: Do not store LAN Manager hash value on ...	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Tra...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in th...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to ...	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to...	Disabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Disabled
System objects: Require case insensitivity for non-Windows ...	Enabled
System objects: Strengthen default permissions of internal s...	Enabled

Path global: Computer Configuration\Windows Settings\Local Policies\Security Options
Path local: Local Policies\Security Options
Policy: System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing
Setting: Disabled

Close the Policy Editor and start the RayManageSoft Console. In case of an Active Directory Policy consider to enforce an update (e.g. gpupdate /force).