AN OFFERING IN THE BLUE CYBER SERIES:

“Hardening MS Windows for NIST SP 800-171 Compliance” by the California NIST Manufacturing Extension Partnership (MEP) www.cmtc.com

Version 28 Sep 2021

#13 in the Blue Cyber Education Series

Pragmatic Security

Microsoft Windows Security for DFARS provisions & clauses

Ernie Edmonds CISSP SSCP CAP MCSE MCSA FSCA CEH CSEPS
Senior Managing Consultant | CMTC

CMTC is affiliated with the National Institute of Standards and Technology (NIST) and is part of the Hollings Manufacturing Extension Partnership (MEP) Program.

CMTC is not affiliated with the CMMC-AB, and is not a CMMC-AB authorized registered practitioner organization.

CASCADE

The California Advanced Supply Chain Analysis and Diversification Effort (CASCADE) is an initiative funded by the U.S. Department of Defense (DoD) to bolster California's defense supply chain cybersecurity resilience. CASCADE ties into OPR's High Road Economic Development work by providing technical assistance programs and helping grow and sustain California's cybersecurity and smart technology workforce through education curricula, training, and apprenticeship programs. CASCADE includes multiple project components executed by a consortium comprised of community, industry and non-profit partners; state agencies; and educational institutions.

Notice

The views expressed in this presentation are those of the authors
and may not necessarily be endorsed by
the Department of Defense, Defense Acquisition University,
the Department of Homeland Security,
the National Institute of Standards & Technology,
the NIST Manufacturing Extension Partnership,
the Governor's Office, CASCADE
or any other organization.

Notice

Nothing in this presentation is legal advice
(written, spoken, expressed or implied).
You should confer with a qualified lawyer for legal matters.

Nothing in this presentation is should be construed as an endorsement (written, spoken, expressed or implied) of any solution, product, service, or methodology.

Pragmatic Security

Agenda:

- Presentation ~55 Minutes
- Q/A ~15 Minutes
- Caution- Heavy Technical Ahead!

Why This Session?

- Controlled Unclassified Information (CUI) shall be protected from compromised confidentiality per the DFARS 252.204-7012. The CUI designation is replacing several legacy designations within the US Federal Government.
- Microsoft Windows is the most widely used operating system used by the D.O.D. Supply Chain – both Server and Workstation.
- Applications Suites such as Microsoft 365 and the Microsoft Server Family are the most widely used application suites in use by the DOD Supply Chain.
- Out of the Box, Windows and the Microsoft Application Suites do not meet the requirements for the DFARS 252.204-7012 or any level of the forthcoming CMMC (Compelling 10/1/2025 per the DOD Interim Rule published 9/29/2020). This is not synonymous with systems configured for D.O.D. C2 Compliance.
- SMMs often do not understand the complexities of the Windows OS.
- Likewise, the SMM community doesn't understand the tools available to them that are integrated into the Microsoft Windows OS Family.

Publications, Seminars, & Conference Guidelines | Trademarks (microsoft.com)

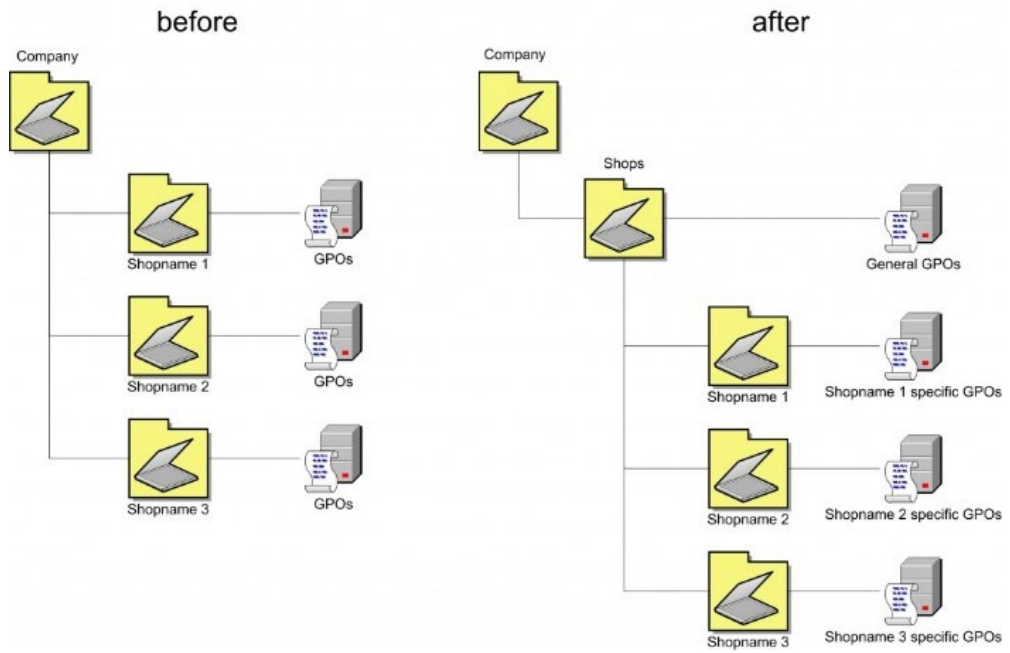
Windows AD - Active Directory

- Modern Microsoft Windows employs a feature called Active Directory which is the Microsoft interpretation of the x.500 Directory Structure and can interact in limited and varying ways with other operating systems such as Unix, Linux, MacOS, Android, and iOS. **This is how Windows organizes sites, services, users, and computers.**
- Active Directory is only available on the server editions of Windows beginning with Windows 2000 and continues into current generation Window Server 2019.
- Windows Workstations gained full Active Directory integration beginning with Windows 2000 Professional and all Professional and higher designated desktop operating systems continue to support Active Directory integration.
- Windows “Home” versions do not support integration within the Active Directory Forest and Domain schemas in any way, they will however participate in a limited fashion with file and print sharing.

Publications, Seminars, & Conference Guidelines | Trademarks (microsoft.com)

AD Organizational Constructs

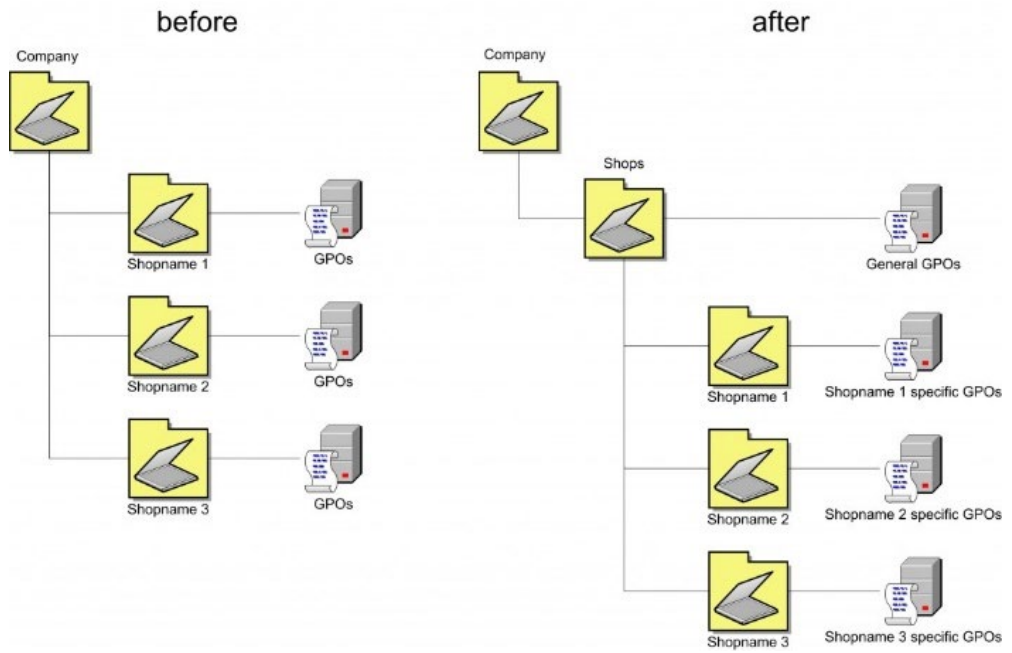
- The x.500 Directory Structure is the most widely used structure in the world.
- The structure consists of Organizational Units and Containers.
- Organizational Units are more flexible than Containers.
- Both OUs and Containers can contain Users and Computers.
- OUs provide more granular provisioning of configuration elements.
- Advise using OUs as your default grouping object.



Publications, Seminars, & Conference Guidelines | Trademarks (microsoft.com)

AD Management Constructs

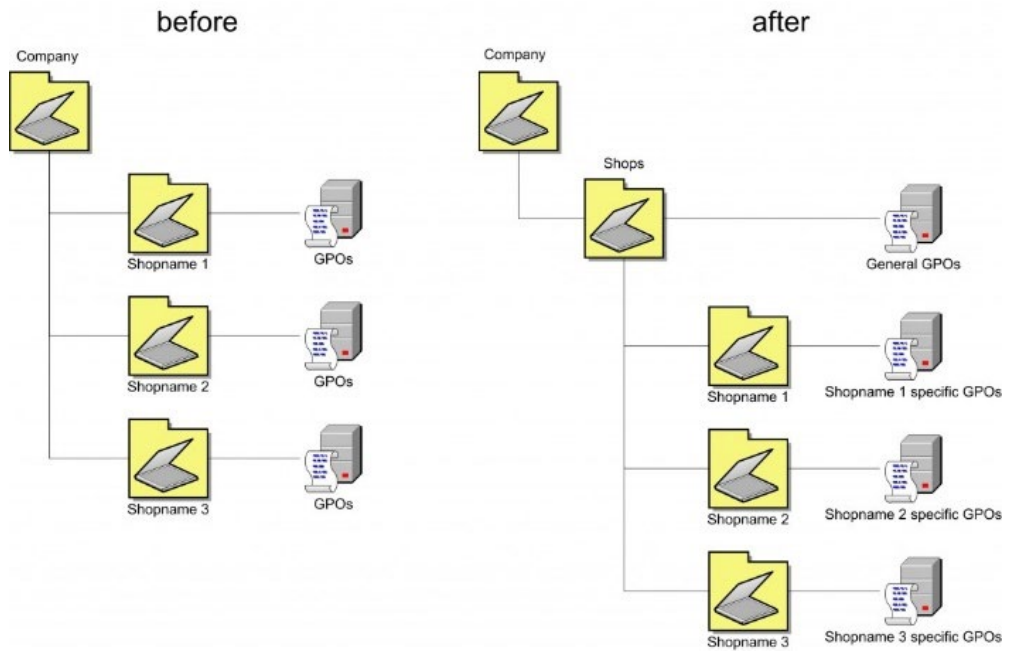
- Global Management of both Users and Devices is most efficiently accomplished in Active Directory by use of Group Policy Objects
- Group Policy Editor edits each policy
- Group Policy Management Console is used for:
  - Management of each GPO
  - Linking each GPO to an Organizational Unit
- Multiple GPOs can be assigned to a single OU
- Inheritance from a higher-level OU can be blocked



Publications, Seminars, & Conference Guidelines | Trademarks (microsoft.com)

GPO Structure

- GPO Computer Configuration
  - Applied globally to the computer that is subject to the GPO.
  - Affects all users logged onto the subject computer.
- GPO User Configuration
  - Applied globally to the computer.
  - Affects the user logged in.
- GPO Combinations
  - More than one GPO may be applied to both the computer and the logged-on user.
  - Combinations are most granular to least granular implementation.
  - Specific enforcement is allowed and will supersede the combination rule above.



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

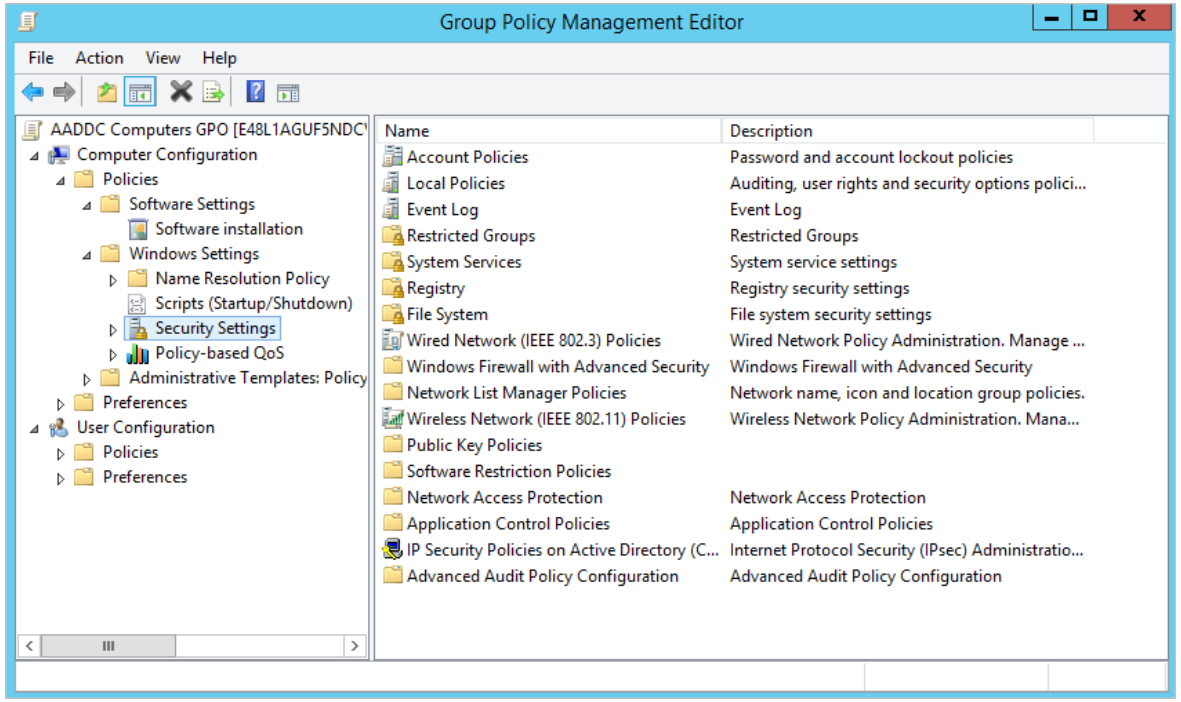
AC.2.005 / 3.1.9

“Provide privacy and security notices consistent with applicable CUI rules.”

Solution (Access Control)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Security Options
      - Interactive logon: Message text for users attempting to log on
        - » DO NOT ATTEMPT UNAUTHORIZED ACCESS! (Required)
        - » THERE IS NO EXPECTATION OF PRIVACY ON THIS SYSTEM! (Required)



There is also a “Title Text” field that may be used but is not a requirement for implementation unless it is used to convey one or both of the required components (Not Typical).

Computer Configuration

CMMC / NIST SP800-171r2 Requirement

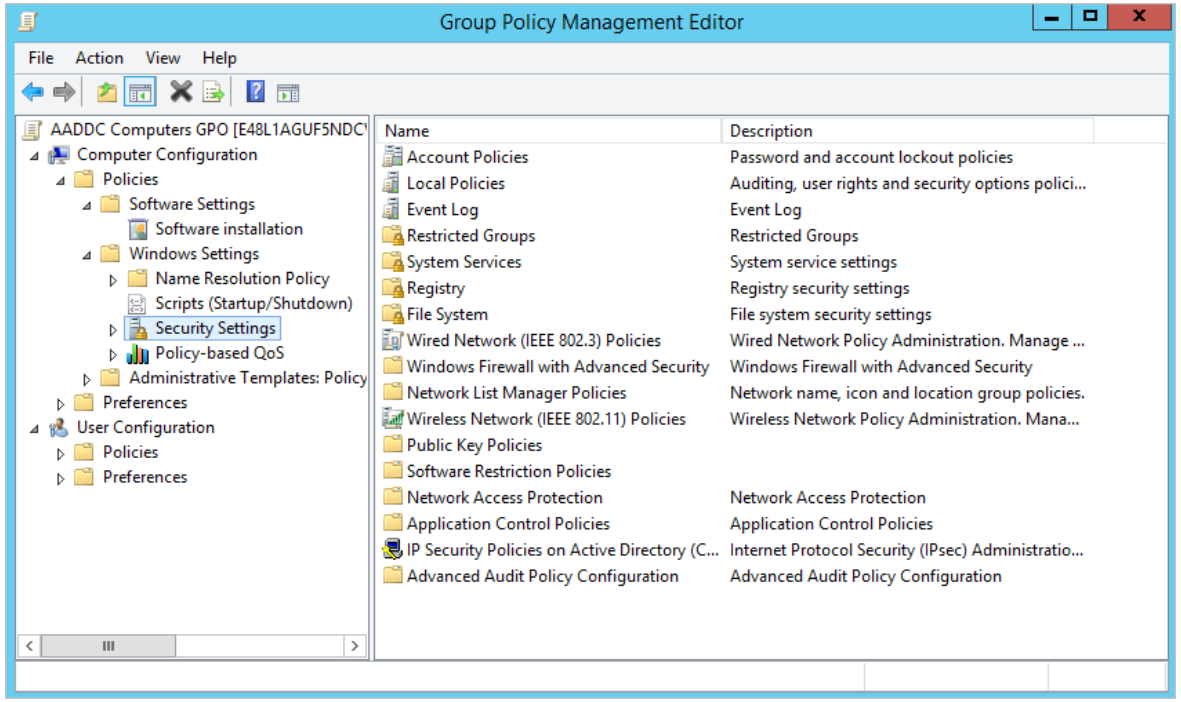
AC.2.009 / 3.1.8

“Limit Unsuccessful Logon Attempts.”

Solution (Access Control) (Account Lockout Step 1 of 3)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Account Policies/Account Lockout Policy
      - Account Lockout Threshold
        - » 5 Invalid Login Attempts



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

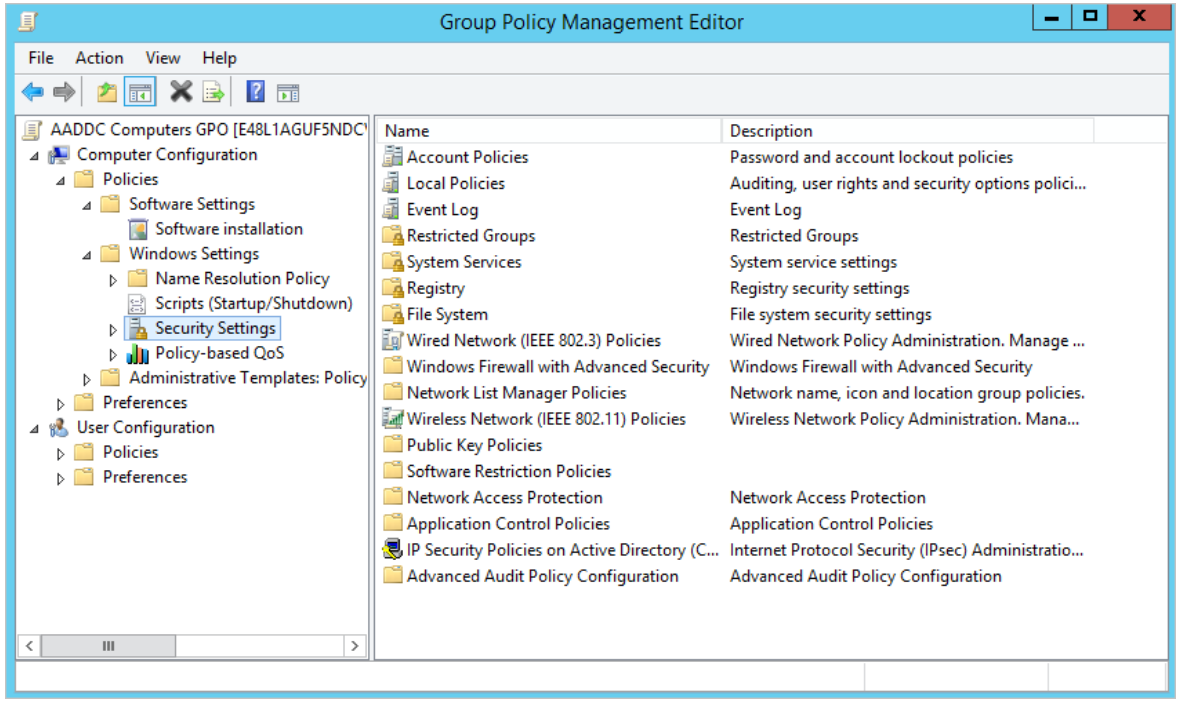
None: Industrywide Accepted Best Practice

Account Lockout Duration

Solution (~Access Control) (Account Lockout Step 2 of 3)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Account Policies/Account Lockout Policy
      - Account Lockout Duration
        - » 30 Minutes



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

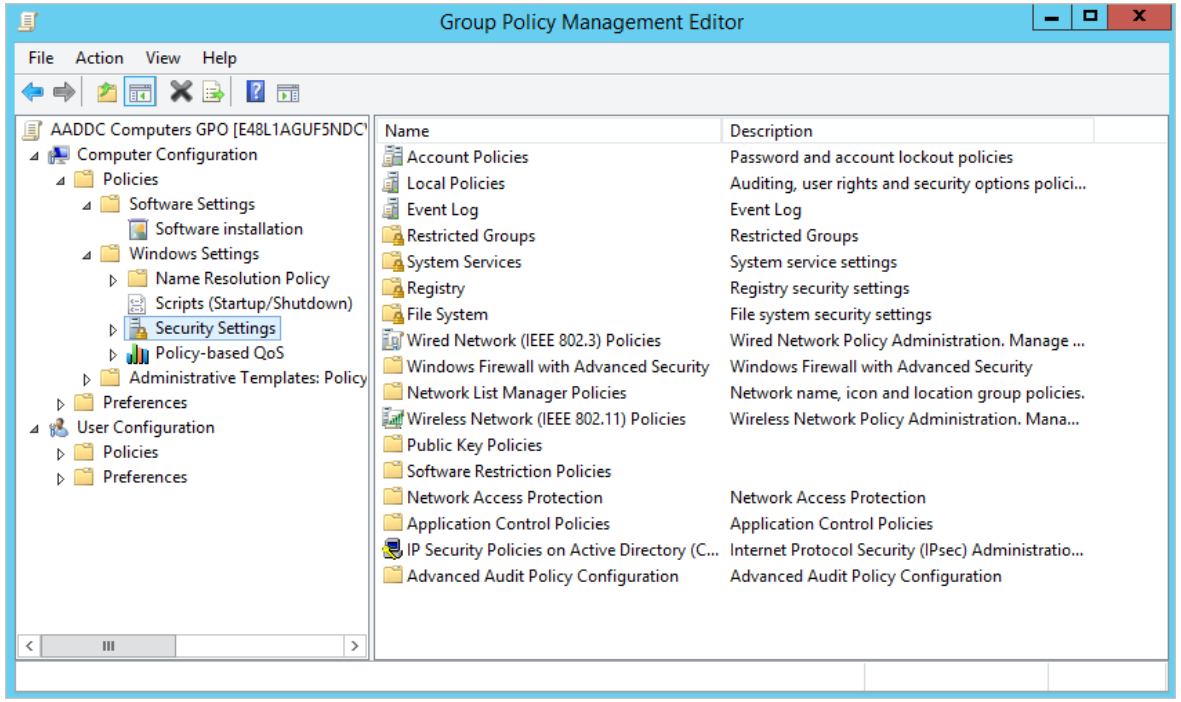
None: Industrywide Accepted Best Practice

Reset account lockout counter after

Solution (~Access Control) (Account Lockout Step 3 of 3)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Account Policies/Account Lockout Policy
      - Reset account lockout counter after
        - » 30 Minutes



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

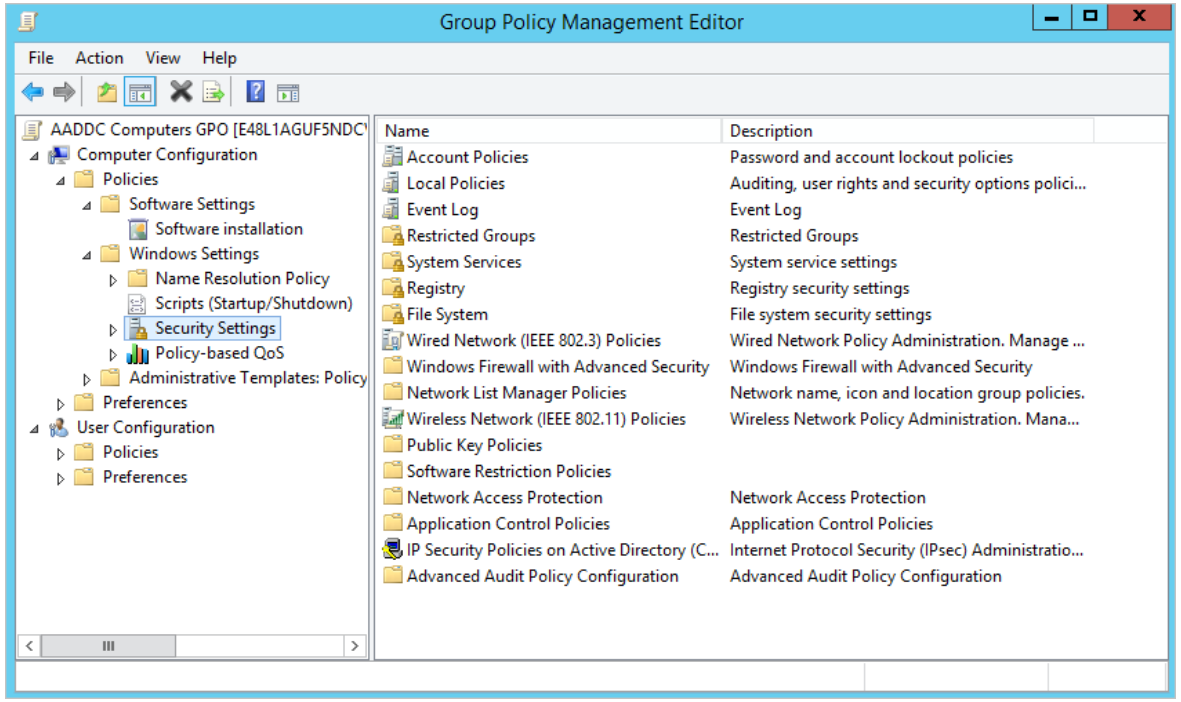
None: Industrywide Accepted Best Practice

Minimum Password Age

Solution (~Access Control) (Password Management Step 1 of 5)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Account Policies/Password Policy
      - Minimum Password Age
        - » 30 Days



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

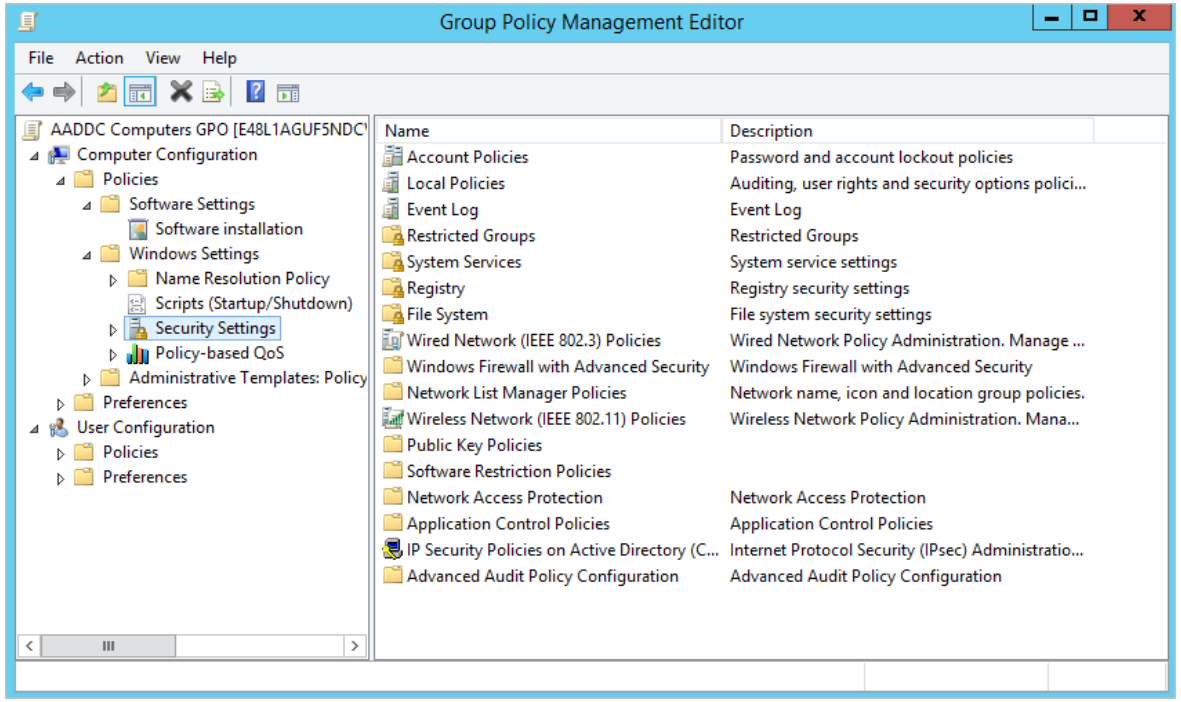
None: Industrywide Accepted Best Practice

Maximum Password Age

Solution (~Access Control) (Password Management Step 2 of 5)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Account Policies/Password Policy
      - Maximum Password Age
        - » 90 Days



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

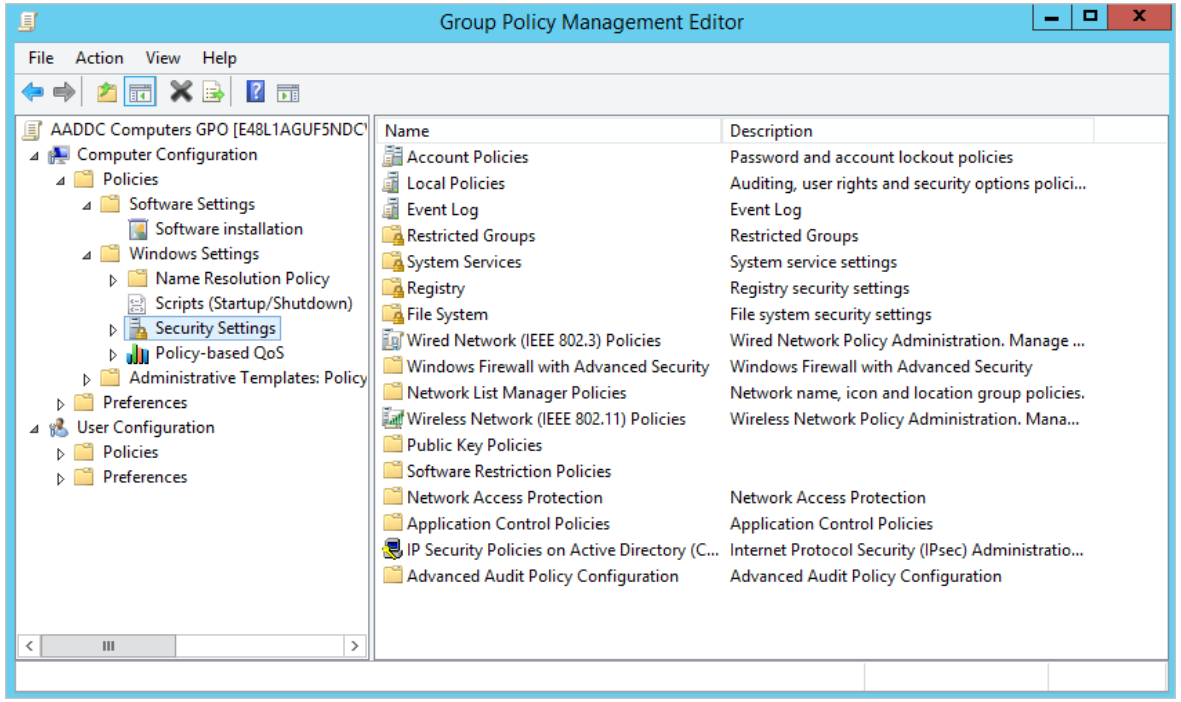
IA.2.079 / 3.5.8

Prohibit password reuse for a specified number of generations.

Solution (Identification and Authentication) (Password Management Step 3 of 5)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Account Policies/Password Policy
      - Enforce Password History
        - » 12 Passwords Remembered



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

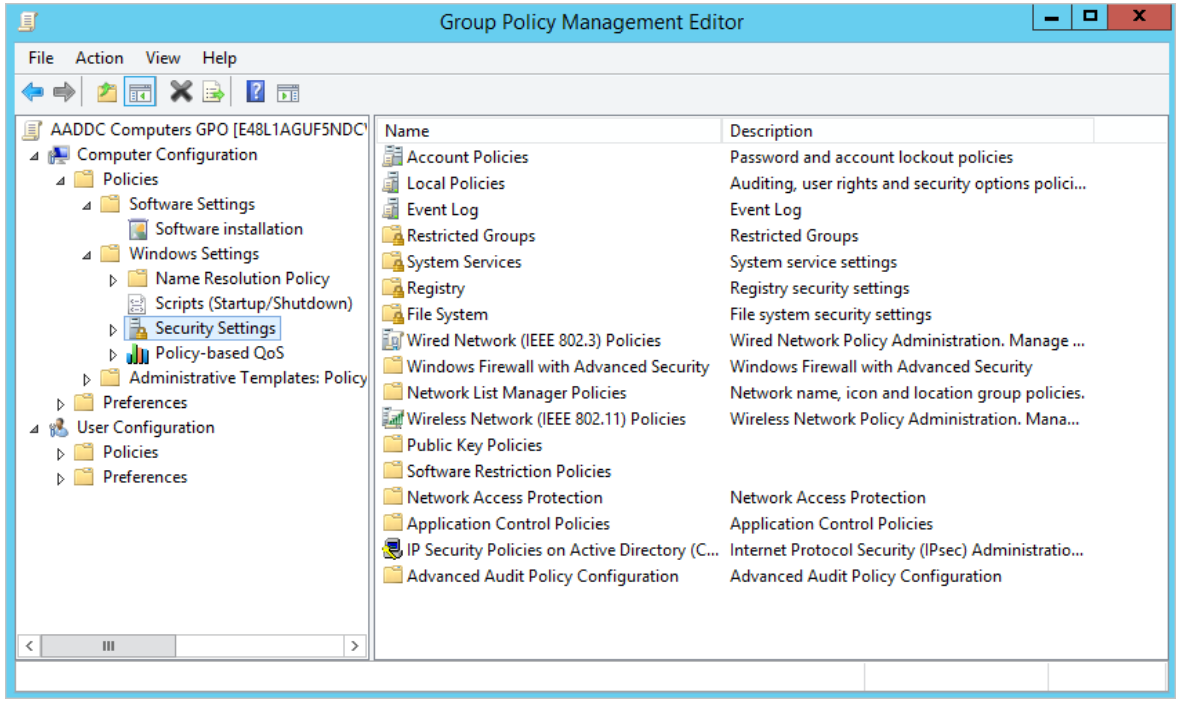
IA.2.078 / 3.5.7

Enforce a minimum password complexity and change of characters when new passwords are created.

Solution (Identification and Authentication) (Password Management Step 4 of 5)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Account Policies/Password Policy
      - Password must meet complexity requirements
        - » Enabled



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

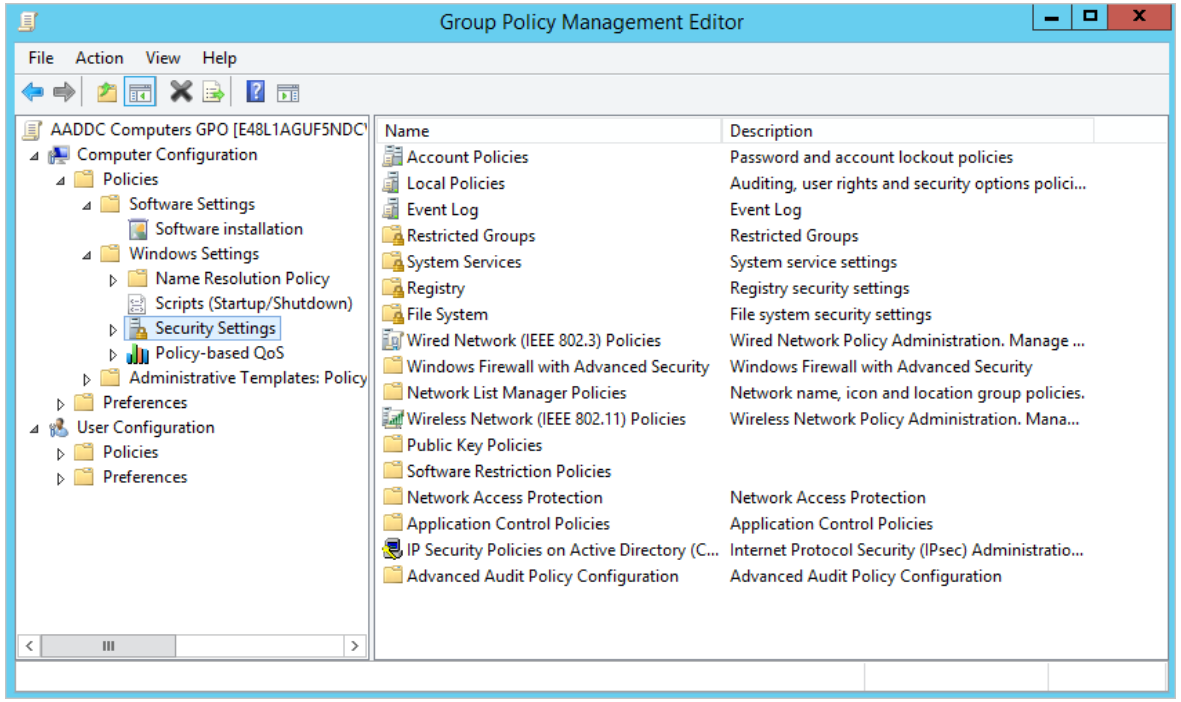
None: Industrywide Accepted Best Practice

Minimum password length

Solution (~Access Control) (Password Management Step 5 of 5)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Account Policies/Password Policy
      - Enforce Password History
        - » 8 Characters



Use Configuration

CMMC / NIST SP800-171r2 Requirement

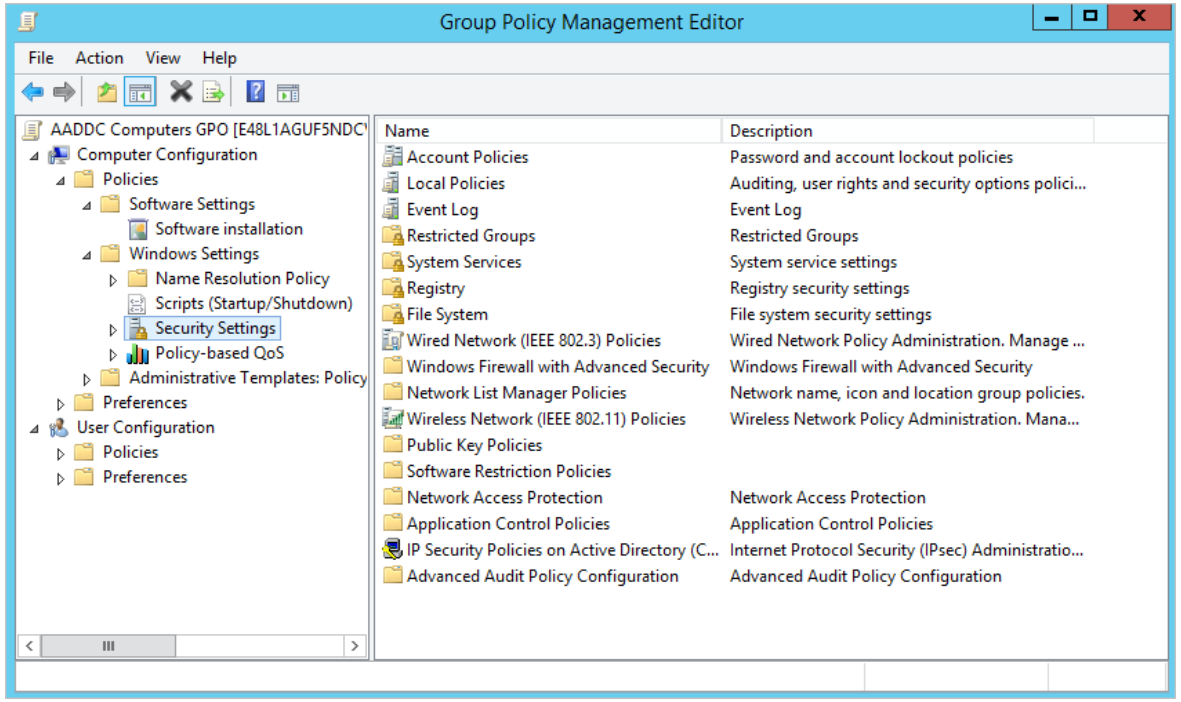
AC.2.010 / 3.1.10

Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

Solution (Access Control) (Session Lock Step 1 of 3)

Group Policy Object Setting:

- User Configuration
  - Policies, Administrative Templates
    - Control Panel/Personalization
      - Enable screen saver
      - Enabled



Use Configuration

CMMC / NIST SP800-171r2 Requirement

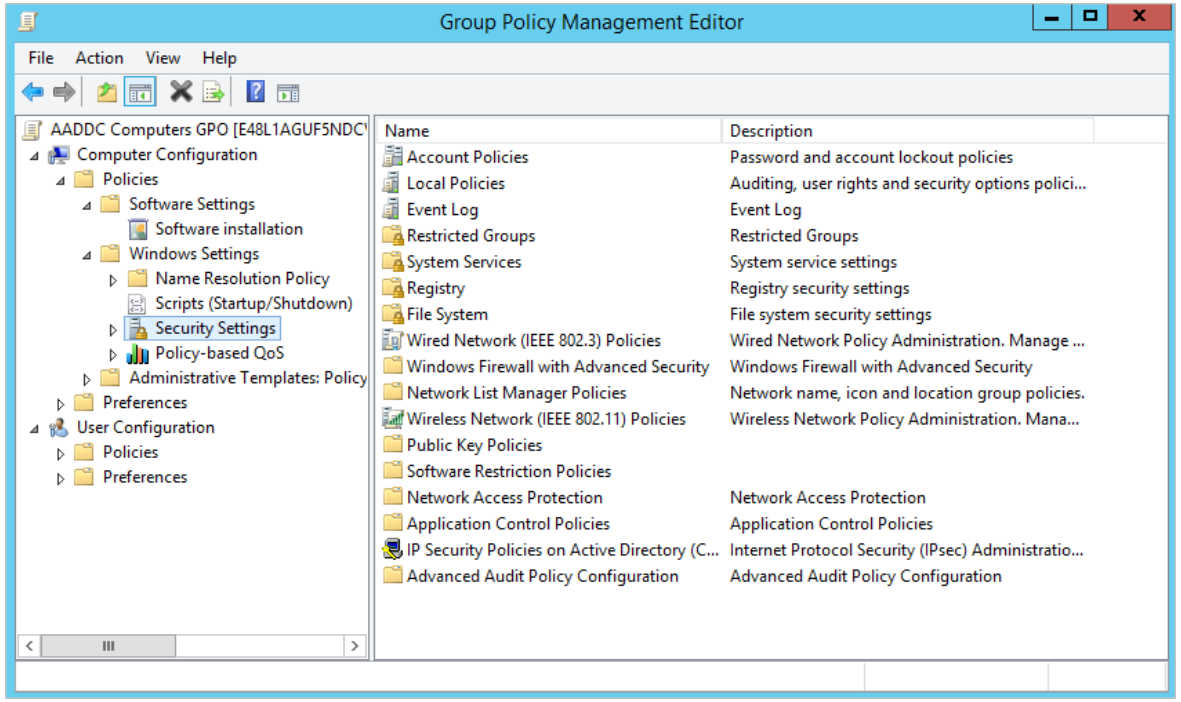
AC.2.010 / 3.1.10

Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

Solution (Access Control) (Session Lock Step 2 of 3)

Group Policy Object Setting:

- User Configuration
  - Policies, Administrative Templates
    - Control Panel/Personalization
      - Password protect the screen saver
      - Enabled



Use Configuration

CMMC / NIST SP800-171r2 Requirement

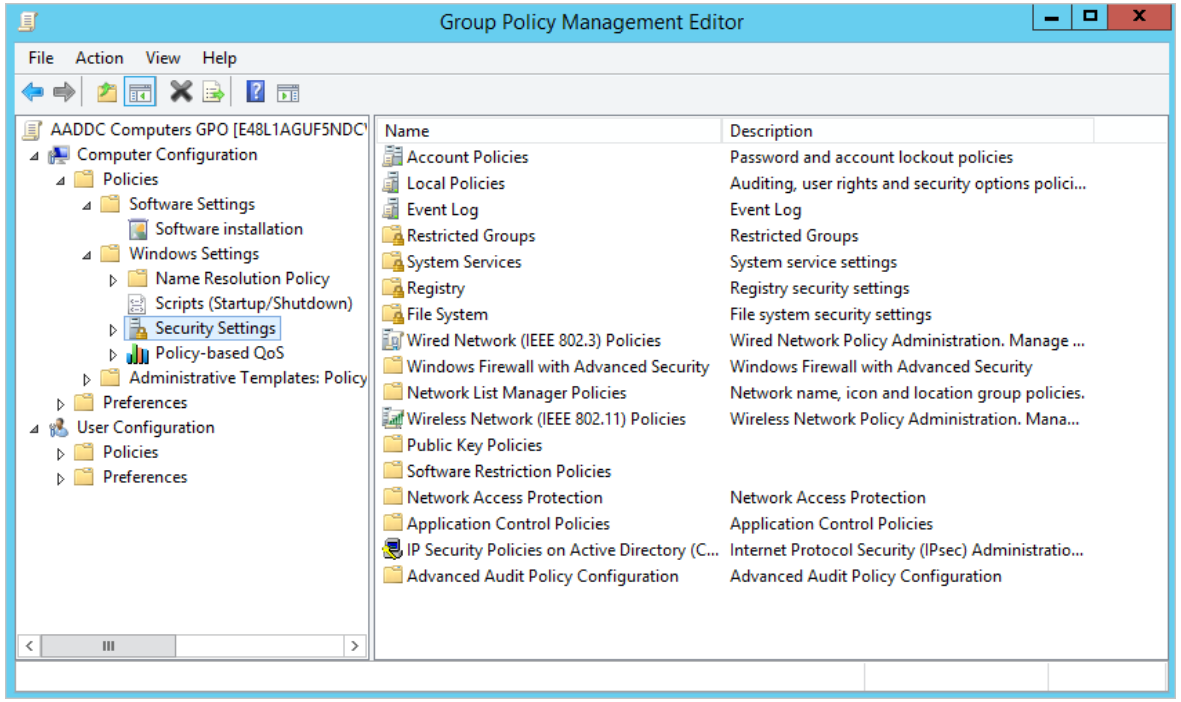
AC.2.010 / 3.1.10

Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

Solution (Access Control) (Session Lock Step 3 of 3)

Group Policy Object Setting:

- User Configuration
  - Policies, Administrative Templates
    - Control Panel/Personalization
      - Screen saver timeout
      - 900 Seconds (15 Minutes)



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AC.3.019, SC.3.186 / 3.1.11, 3.13.9

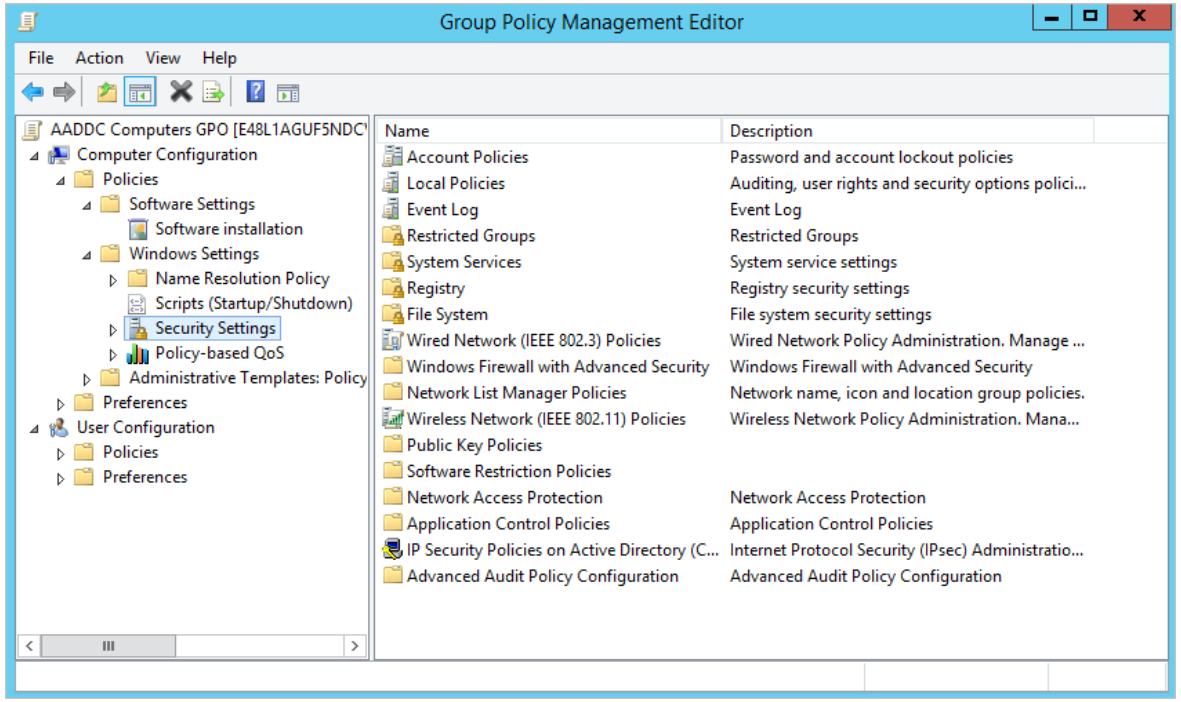
“Terminate (automatically) a user session after a defined condition.”

“Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.”

Solution (Access Control) (Systems and Communications Protection)
(Session Termination Step 1 of 4)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Administrative Templates
      - Windows Components/Remote Desktop Services/Remote Desktop Session Host/Session Time Limits
        - » End session when time limits are reached
          - Enabled



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AC.3.019, SC.3.186 / 3.1.11, 3.13.9

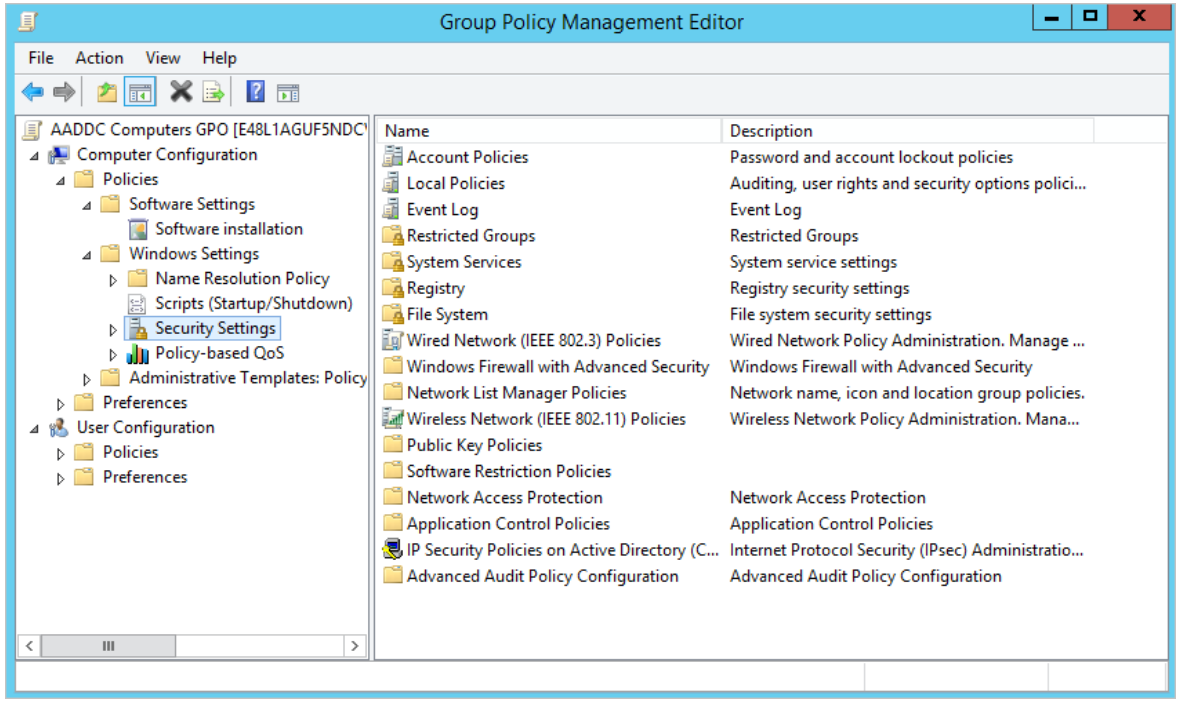
“Terminate (automatically) a user session after a defined condition.”

“Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.”

Solution (Access Control) (Systems and Communications Protection)
(Session Termination Step 2 of 4)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Administrative Templates
      - Windows Components/Remote Desktop Services/Remote Desktop Session Host/Session Time Limits
        - » Set time limit for active but idle Remote Desktop Services sessions
          - Enabled
          - 15 Minutes



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AC.3.019, SC.3.186 / 3.1.11, 3.13.9

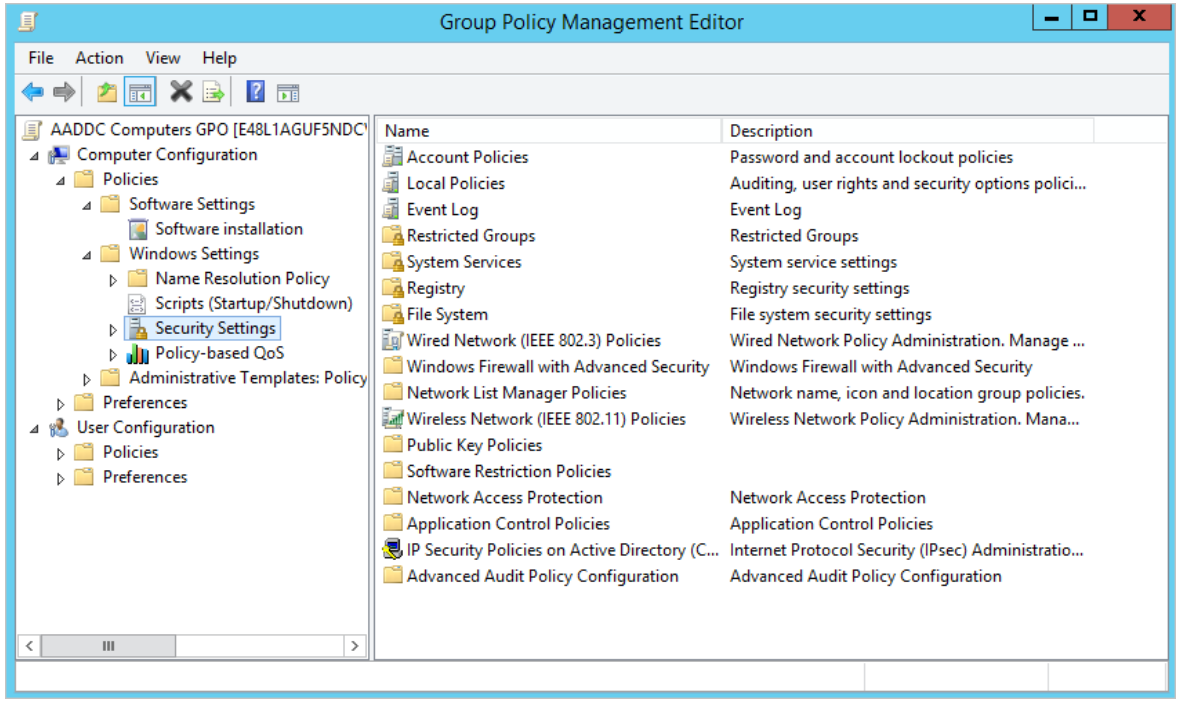
“Terminate (automatically) a user session after a defined condition.”

“Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.”

Solution (Access Control)
(Systems and Communications Protection)
(Session Termination Step 3 of 4)

Group Policy Object Setting:

- Computer Configuration, Policies, Administrative Templates
  - Windows Components/Remote Desktop Services/Remote Desktop Session Host/Session Time Limits
    - Set time limit for disconnected sessions
      - Enabled
      - 2 Hours



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AC.3.019, SC.3.186 / 3.1.11, 3.13.9

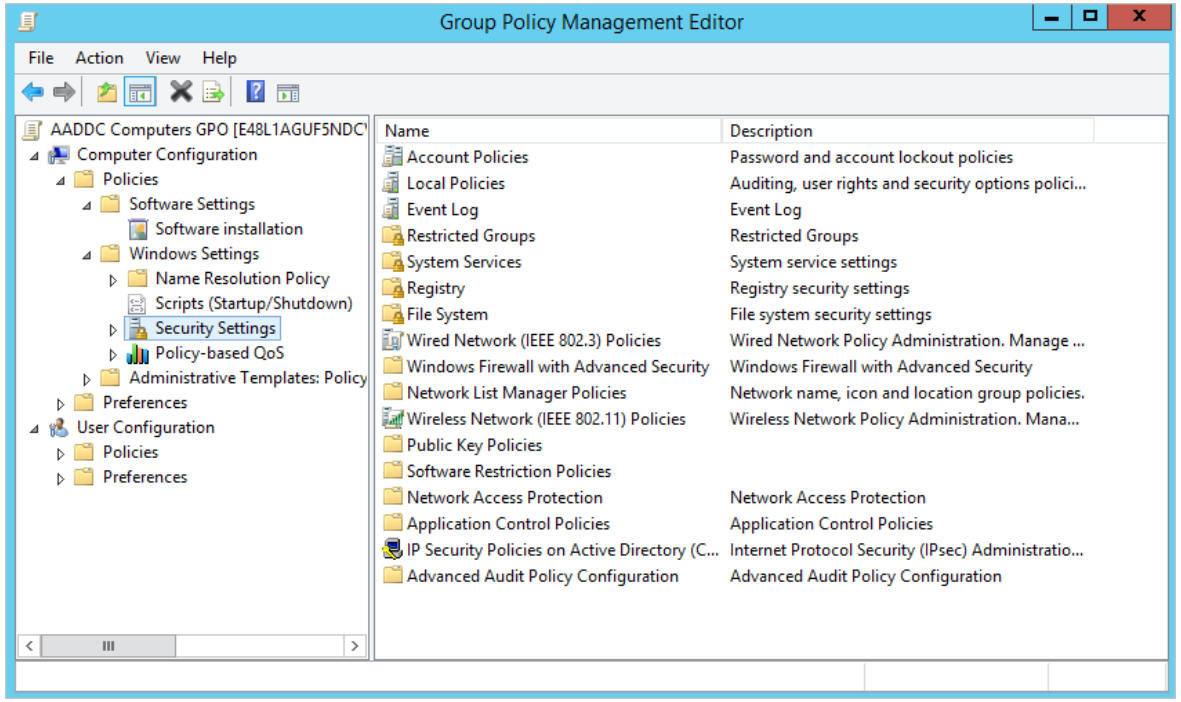
“Terminate (automatically) a user session after a defined condition.”

“Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.”

Solution (Access Control)
(Systems and Communications Protection)
(Session Termination Step 4 of 4)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Security Options
      - Network Security: Force logoff when logon hours expire
        - » Enabled



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AC.3.022, SC.3.185, SC.3.177 / 3.1.19, 3.13.8, 3.13.11

“Encrypt CUI on mobile devices and mobile computing platforms.”

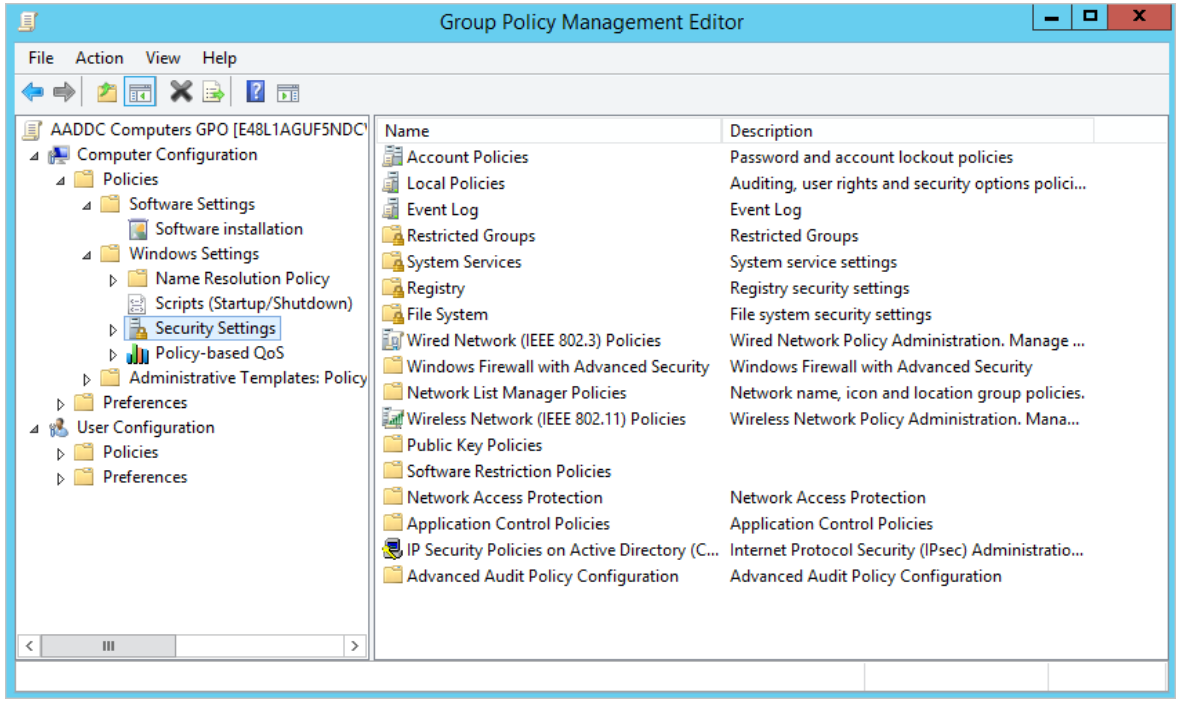
“Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.”

“Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.”

Solution (Access Control) (Systems and Communications Protection)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Security Options
      - System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
        - » Enabled



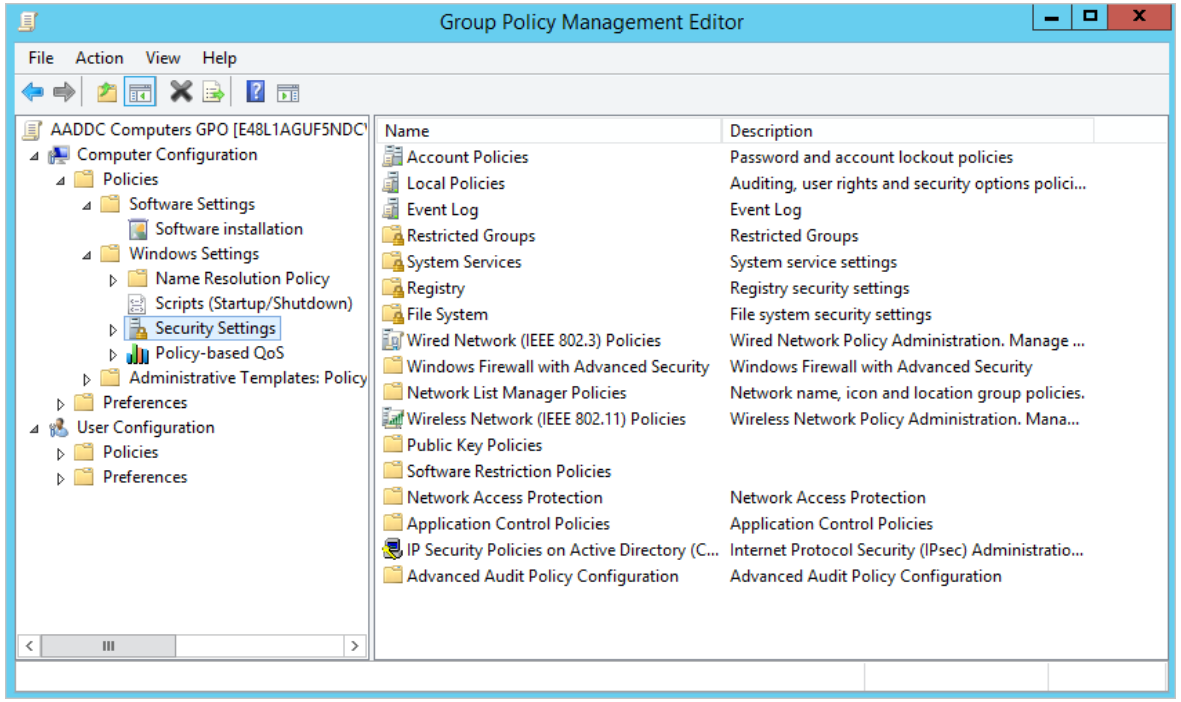
Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AU.2.041 / 3.3.2

"Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions."

Solution (Audit and Accountability) (Individual Accountability Step 1 of 8)



Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Audit Policy
      - Audit account logon events
        - » Success, Failure

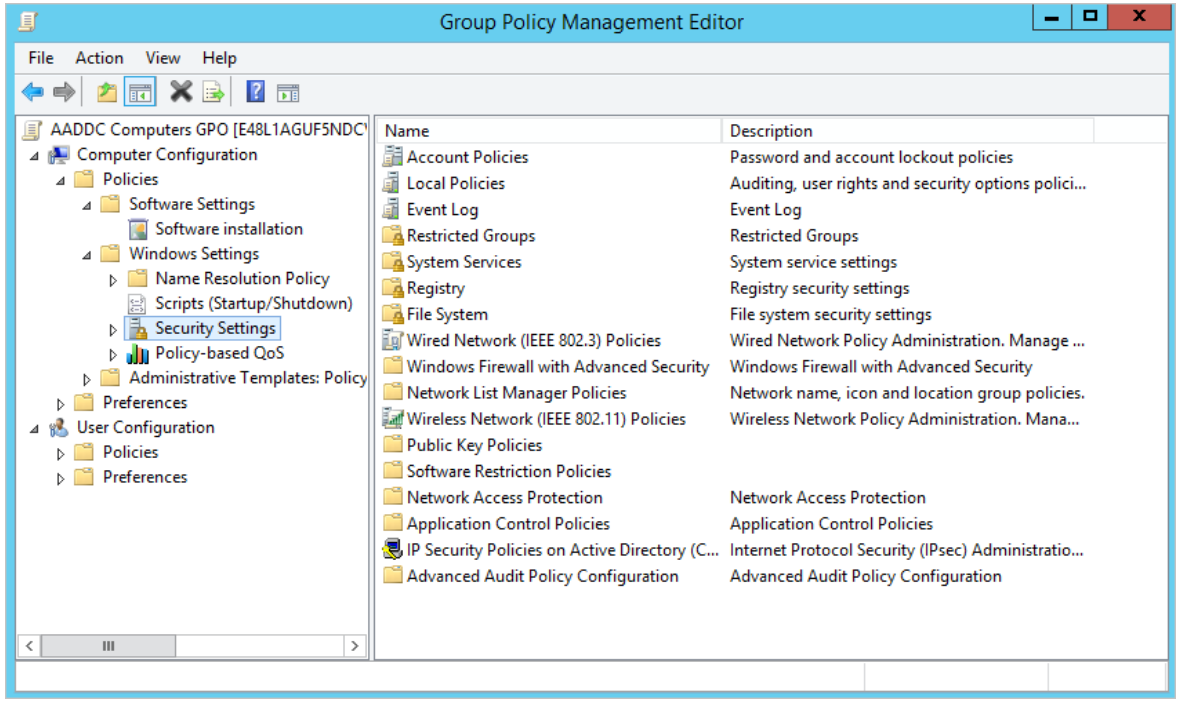
Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AU.2.041 / 3.3.2

"Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions."

Solution (Audit and Accountability) (Individual Accountability Step 2 of 8)



Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Audit Policy
      - Audit login events
        - » Success, Failure

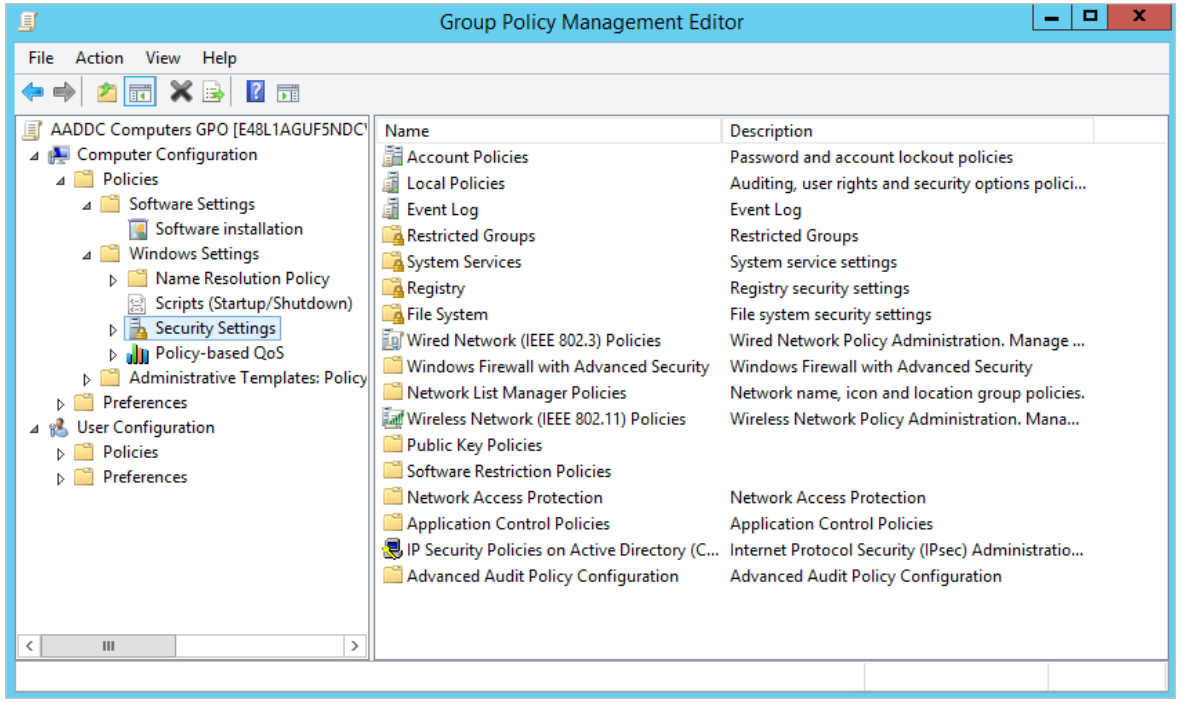
Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AU.2.041 / 3.3.2

Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Solution (Audit and Accountability) (Individual Accountability Step 3 of 8)



Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Audit Policy
      - Audit object access
        - » Success, Failure

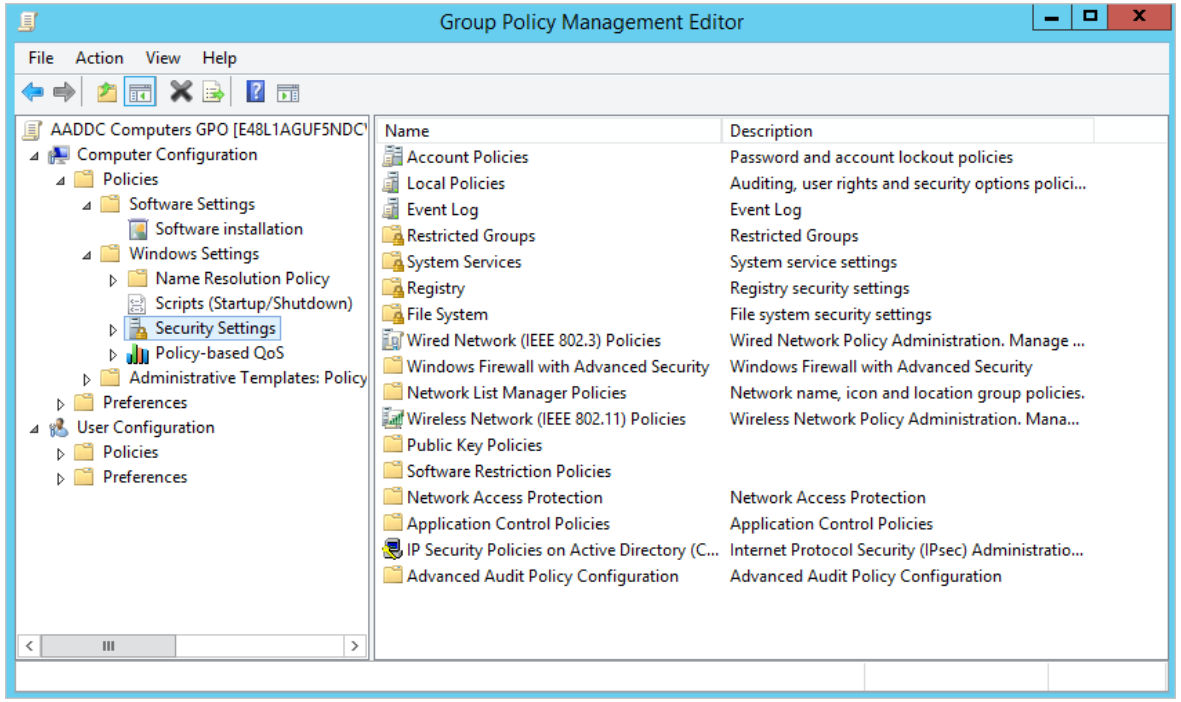
Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AU.2.041 / 3.3.2

“Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.”

Solution (Audit and Accountability) (Individual Accountability Step 4 of 8)



Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Audit Policy
      - Audit privilege use
        - » Success, Failure

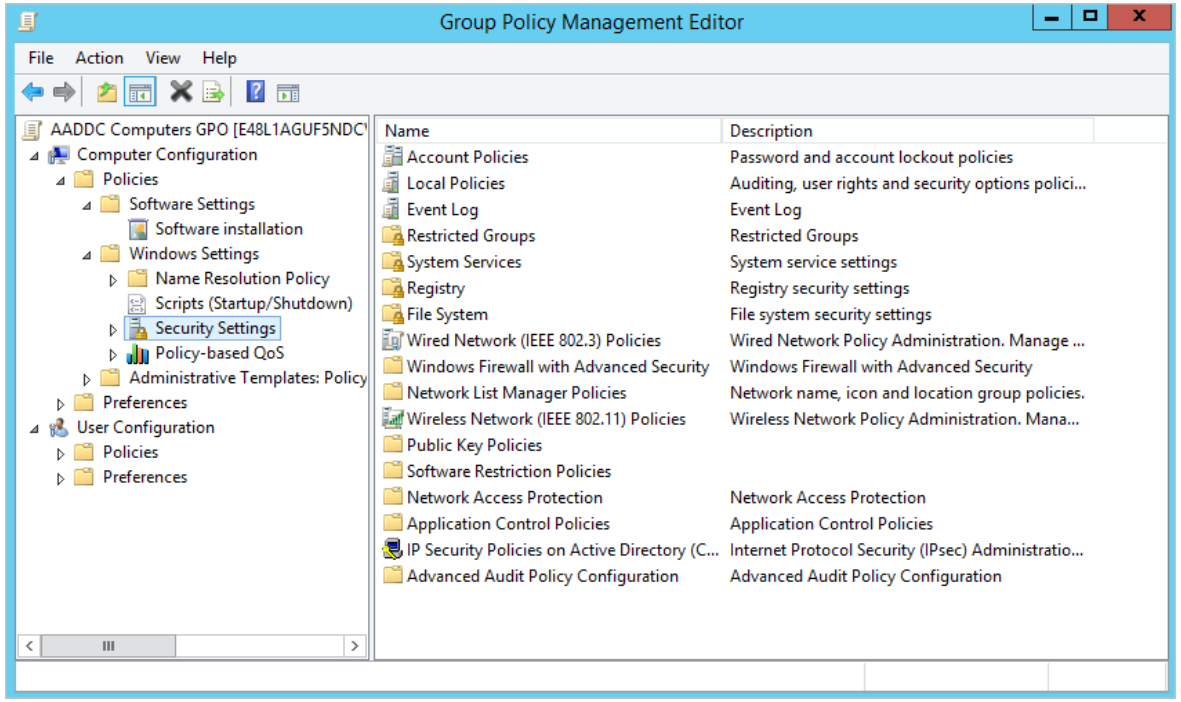
Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AU.2.041 / 3.3.2

"Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions."

Solution (Audit and Accountability) (Individual Accountability Step 5 of 8)



Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Audit Policy
      - Audit policy change
        - » Success, Failure

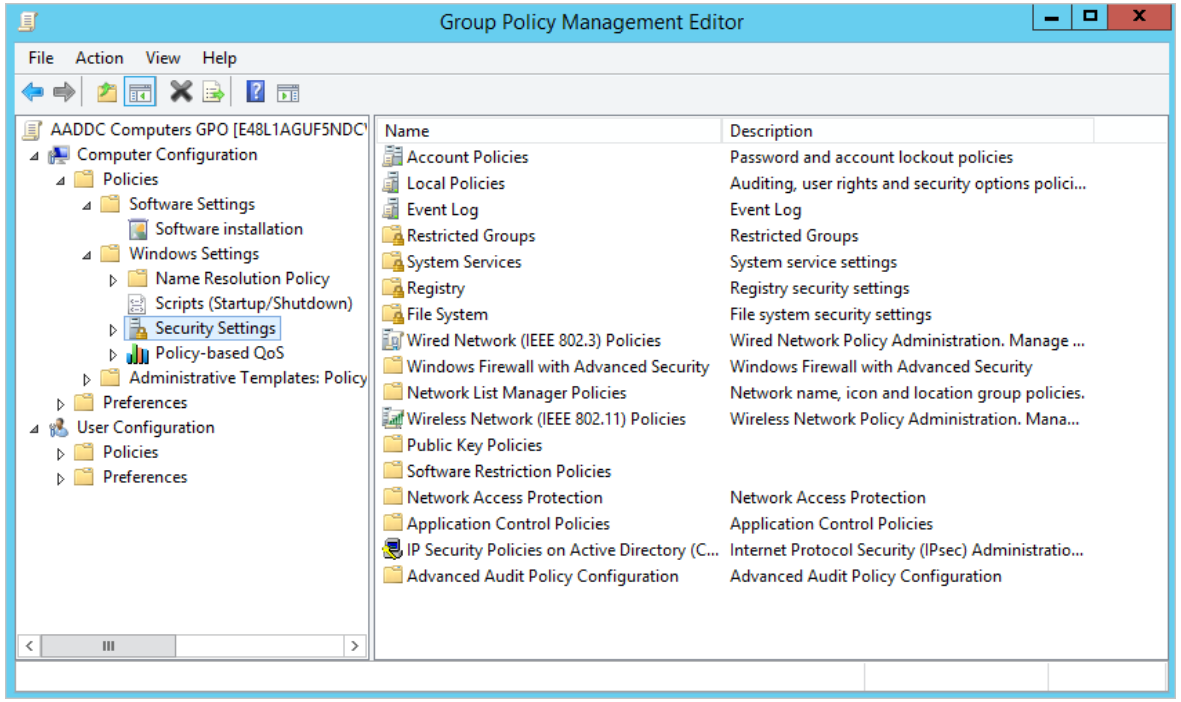
Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AU.2.041 / 3.3.2

"Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions."

Solution (Audit and Accountability) (Individual Accountability Step 6 of 8)



Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Audit Policy
      - Audit account management
        - » Success, Failure

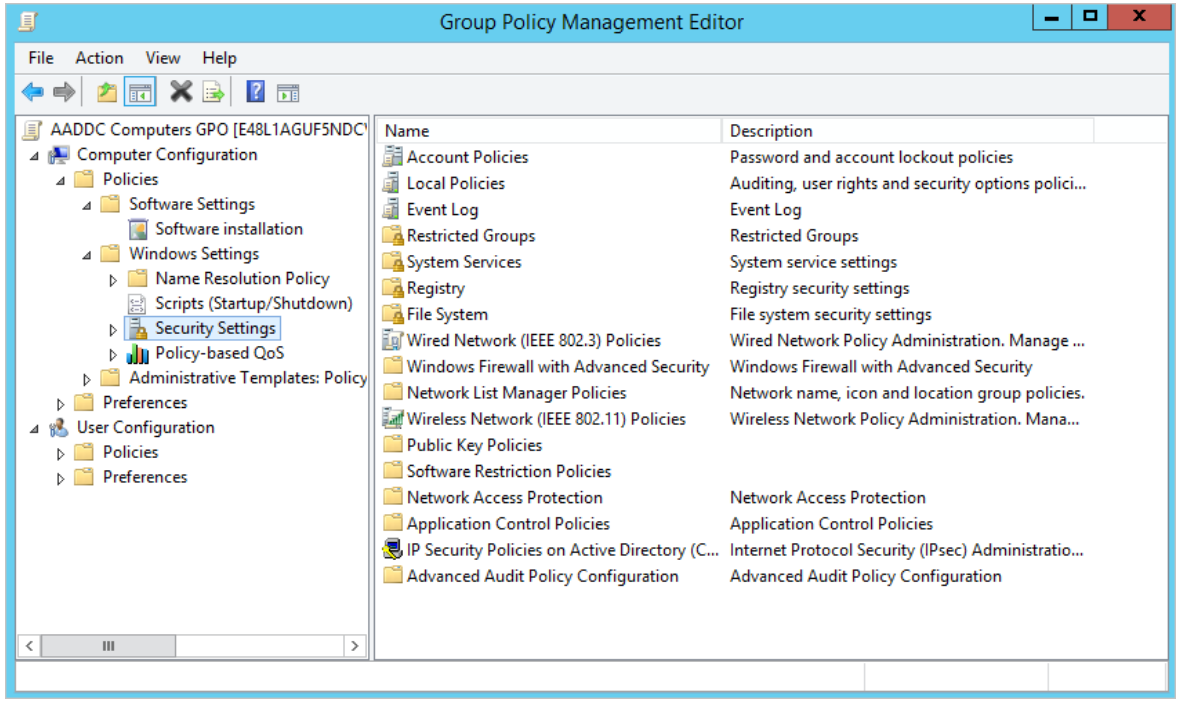
Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AU.2.041 / 3.3.2

“Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.”

Solution (Audit and Accountability) (Individual Accountability Step 7 of 8)



Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Audit Policy
      - Audit system events
        - » Success, Failure

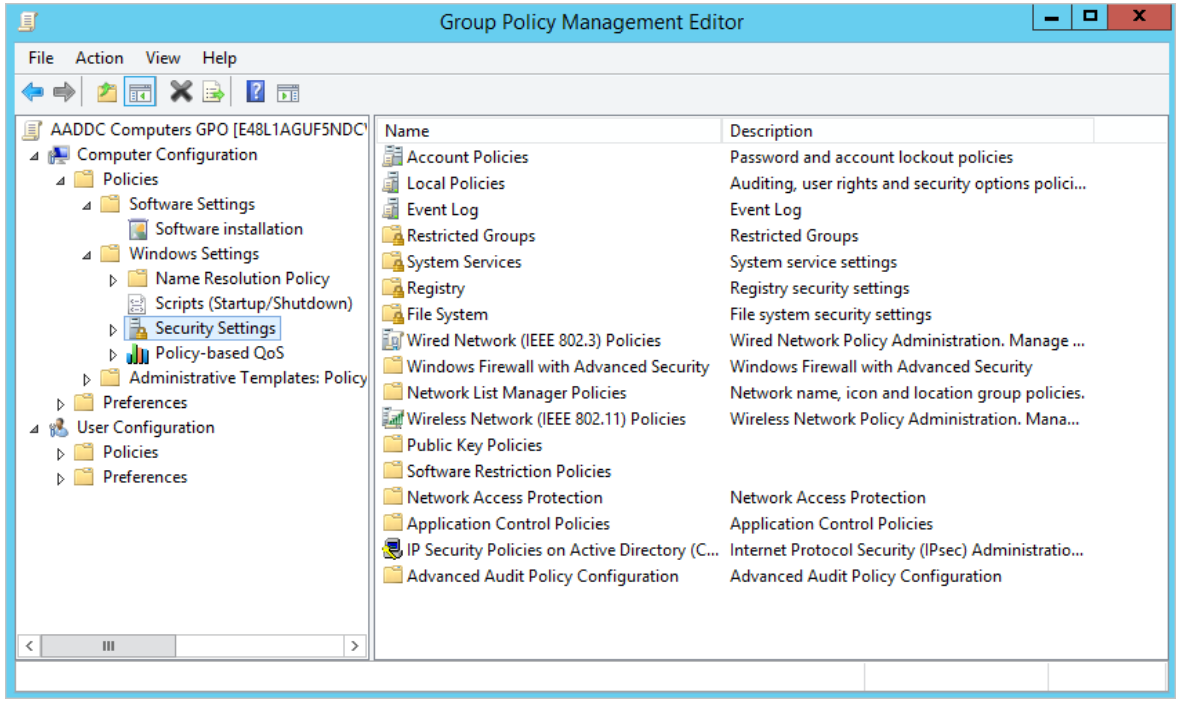
Computer Configuration

CMMC / NIST SP800-171r2 Requirement

AU.2.041 / 3.3.2

"Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions."

Solution (Audit and Accountability) (Individual Accountability Step 8 of 8)



Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Audit Policy
      - Audit process tracking
        - » Success, Failure

Computer Configuration

CMMC / NIST SP800-171r2 Requirement

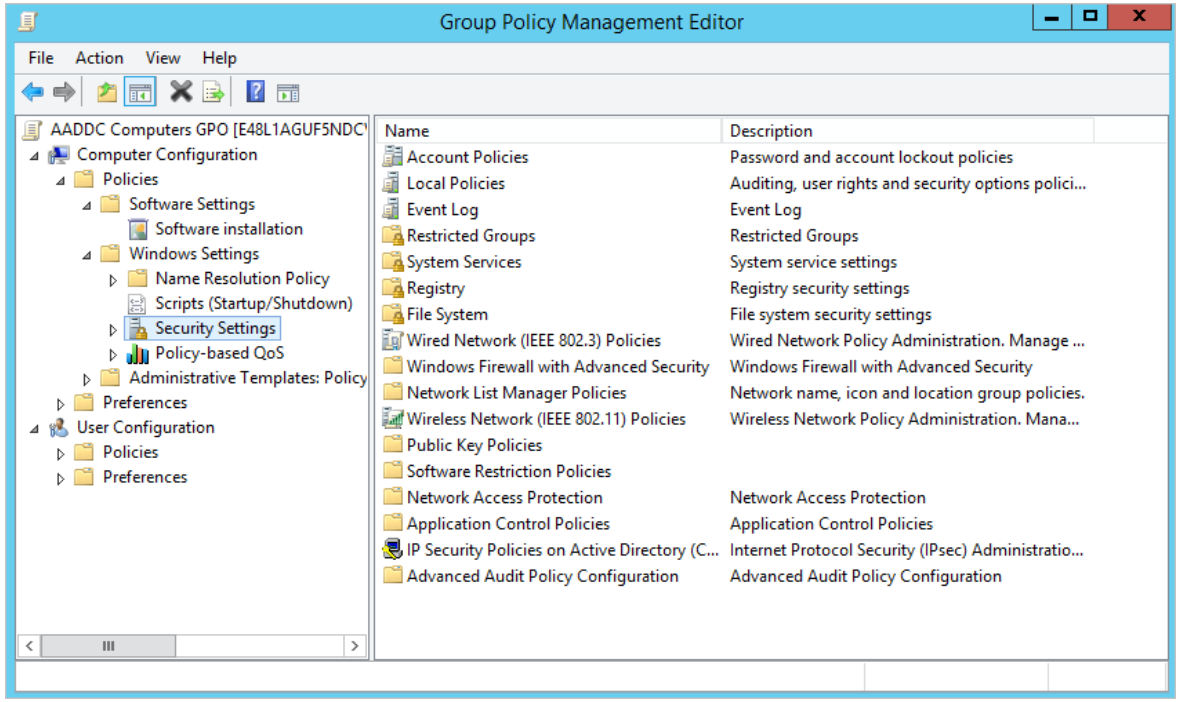
IA.2.081 / 3.5.10

“Store and transmit only cryptographically-protected passwords.”

Solution (Identification and Authentication)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Account Policies/Password Policy
      - Store passwords using reversible encryption
        - » Disabled



Computer Configuration

CMMC / NIST SP800-171r2 Requirement

IA.3.084 / 3.5.4

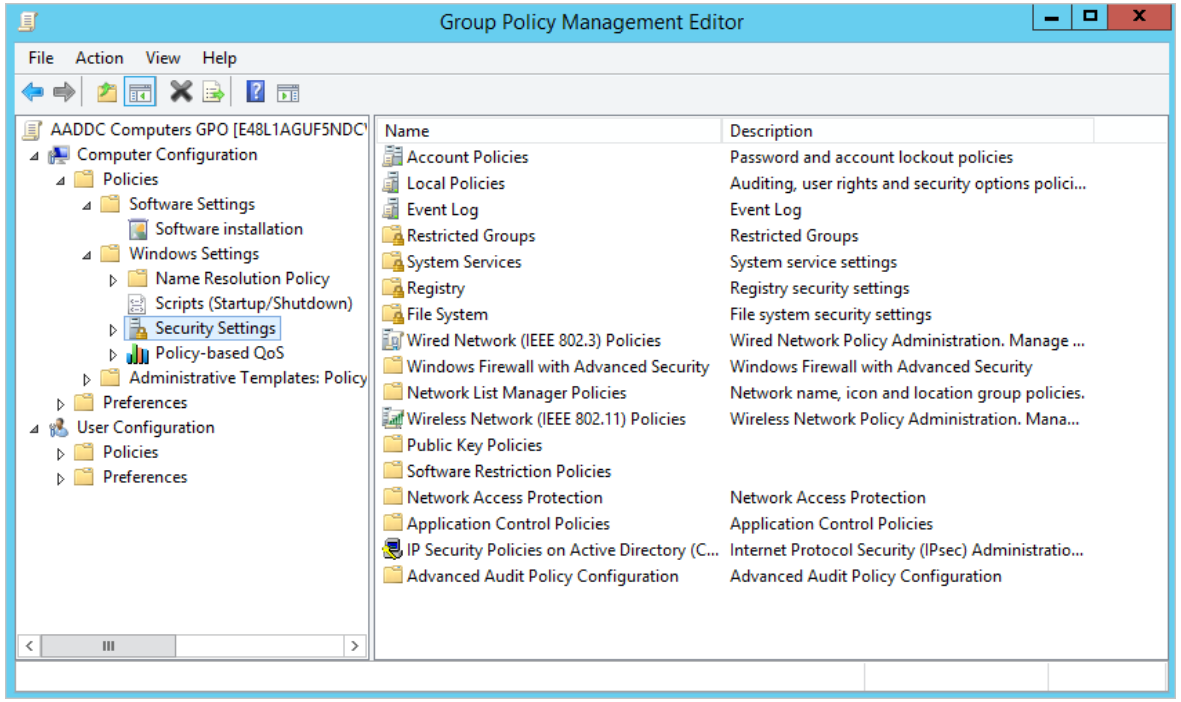
"Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts."

Solution (Replay Resistant Authentication)

Group Policy Object Setting:

- Computer Configuration
  - Policies
    - Local Policies/Security Options
      - Domain Member: Require strong (Windows 2000 or later) session key
        - » Enabled

Multi-factor authentication *can* provide stronger replay resistance that this Windows setting alone when implemented properly.



Additional Configuration

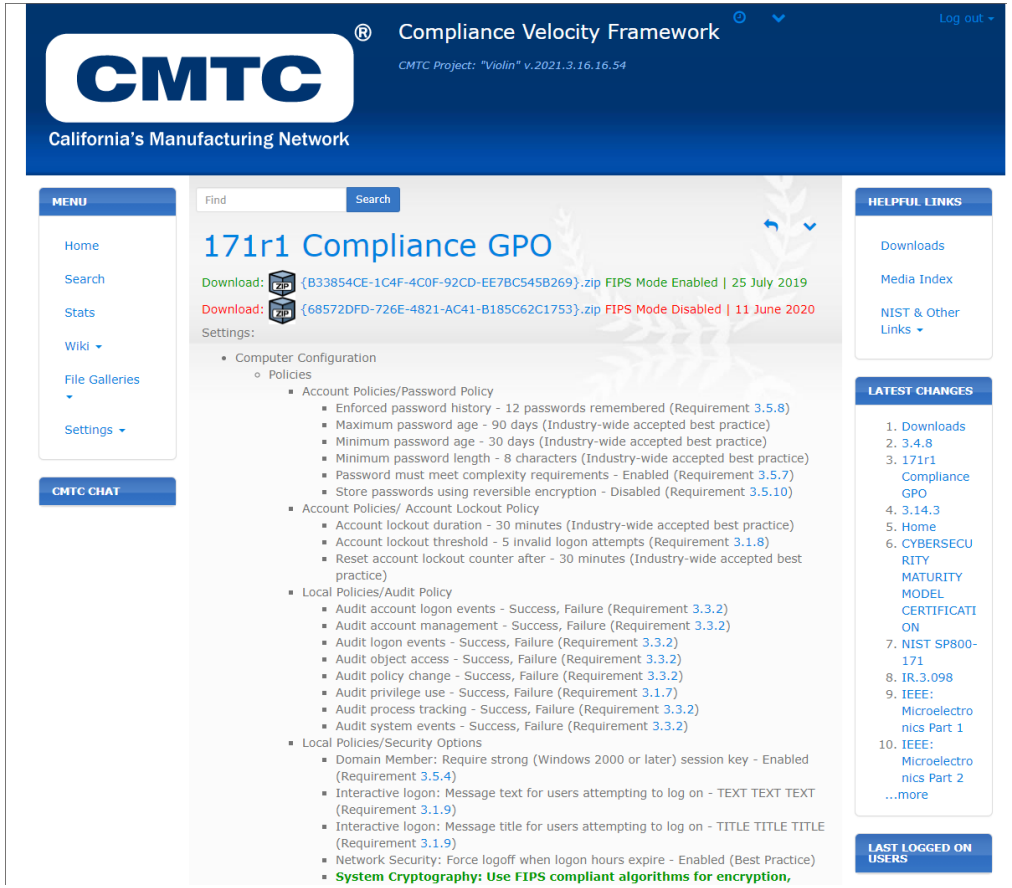
The following MUST be configured in order to be compliant with the CMMC Level 3 and NIST SP800-171 but include variables that must be handled individually for each environment of operation and cannot be responsibly conveyed in a presentation of this nature:

- FIPS-validated full-drive encryption for persistent media such as hard drives and SSDs when used for the storage of CUI at rest.
- FIPS validated portable media encryption for media devices such as thumb drives when used for the storage of CUI at rest and removed from alternative physical safeguards such as secured area of operations or locking container.
- Expressly defined (Whitelisting/Allow-listing) or expressly denied (Blacklisting/Deny-listing) applications. *(Tied for #1 along with Multi-factor Authentication as the highest value in terms of risk-remediation value when successfully implemented)*

Easy Button

Directions:

1. Download the 171r1 GPO from Violin.
2. Create Template GPO and link it in the appropriate place in AD.
3. Right-click the Template GPO and “Import Settings”.
4. Follow the wizard to find the GPO downloaded from Violin…
5. Done! (About 3 seconds)



Microsoft Windows Security for DFARS provisions & clauses

QUESTIONS

For additional questions,

please contact Ernie Edmonds at

info@cmtc.com

Any Questions?

- This briefing is not a substitute for reading the FARs and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions to www.safcn.af.mil/Contact-Us/