xylem
Let's Solve Water

USER GUIDE
AUG-10023-28

RNI System Security

sensus
a xylem brand

Revision history

Rev No.	Date	Description
01	20-MAY-10	Updated for RNI 2.1.0.
02	02-MAY-11	Updated for RNI 3.1.0.
03	13-FEB-13	Updated for RNI 3.1 SP2.
04	25-JUL-14	Updated for RNI 3.1 SP3.
05	29-MAR-15	Updated with new permission for Trickle functionality. Removed Meter Read Upload permission.
06	31-JUL-15	Added Secure Broker Configuration.
07	04-NOV-15	Updated the Authentication and Authorization section of the Overview; updated Appendix A; removed obsolete appendixes.
08	25-FEB-16	Updated with ClickJacking vulnerability mitigation, Apache FileETag vulnerability, mitigate ActiveMQ Administrator RC4 cipher vulnerability, and replace ActiveMQ Broker Certificate.
09	05-OCT-16	Updated for RNI 4.1.
10	31-JUL 17	Updated for RNI 4.2.
11	26-FEB-18	Updated for RNI 4.3.
12	8-JUN-18	Updated for RNI 4.3.1.
13	28-AUG-18	Updated for RNI 4.4.0.
14	26-OCT-18	Updated for RNI 4.4.1.
15	25-FEB-19	Updated for RNI 4.5.0.
16	29-APR-19	Updated for RNI 4.5.1.
17	27-AUG-19	Updated for RNI 4.6.0.
18	29-OCT-19	Updated for RNI 4.6.1.
19	26-OCT-20	Updated for RNI 4.7.0.
20	30-APR-20	Updated for RNI 4.7.1.
21	28-AUG-20	Updated for RNI 4.8.
22	20-NOV-20	Additional updates for RNI 4.8 (4.8.1).
23	10-JUN-21	Updated for RNI 4.9.1.
24	25-OCT-21	Updated for RNI 4.10.
25	06-JUN-22	Updated for RNI 4.11. Added detailed definitions for some user roles in Appendix D. Also deleted some obsolete roles.
26	02-DEC-22	Updated for RNI 4.12.
27	16-JUN-23	Updated for RNI 4.13.
28	15-NOV-23	Updated for RNI 4.14.

Copyright

Sensus
637 Davis Drive
Morrisville, NC 27560
1-800-638-3748
www.sensus.com

Document: RNI System Security User Guide
Document Number: AUG-10023-28

Contents

Overview

This document describes the following aspects of the FlexNet™ Regional Network Interface (RNI) system security:

- Authentication and authorization
- Encrypted Communications
- Operating system and application hardening

Authentication and authorization

Authentication is the process of evaluating a user's credentials (username and password, or security certificate) as well as multi-factor authentication (MFA) before allowing access to a system. Access to a user interface is normally performed by means of a local instance of OpenLDAP Directory Server, which is accessed by a protocol called LDAP. The RNI can be configured to operate with an alternate external authentication service that is compatible with LDAP. For details on configuring an alternate service, see the *RNI Microsoft® Active Directory Integration Guide*. For setup and configuration of MFA please see the *RNI System Administrator User Guide*.

Upon authenticating a user, the system grants privileges (authorization) to that user based on one or more assigned roles. These roles are a collection of specific permissions that grant access to specific functions or information within the application. For a detailed listing of the current Roles and Permissions, see Appendix D.

Encrypted communications

Sensus uses encryption to protect sensitive information during communication to prevent unauthorized personnel from accessing the information.

User and system interfaces

Sensus provides support for securing both user- and system-level interfaces using Transport Layer Security (TLS) encryption. This secures the communications to and from these interfaces to provide protection for all sensitive information. The user interface is provided through a Web server that users connect to using a browser. In addition, for system-level interfaces, Sensus provides a Web Services gateway that uses Simple Object Access Protocol (SOAP) messaging for communications. The following diagram depicts the security architecture of the RNI Web Server where these interfaces reside.

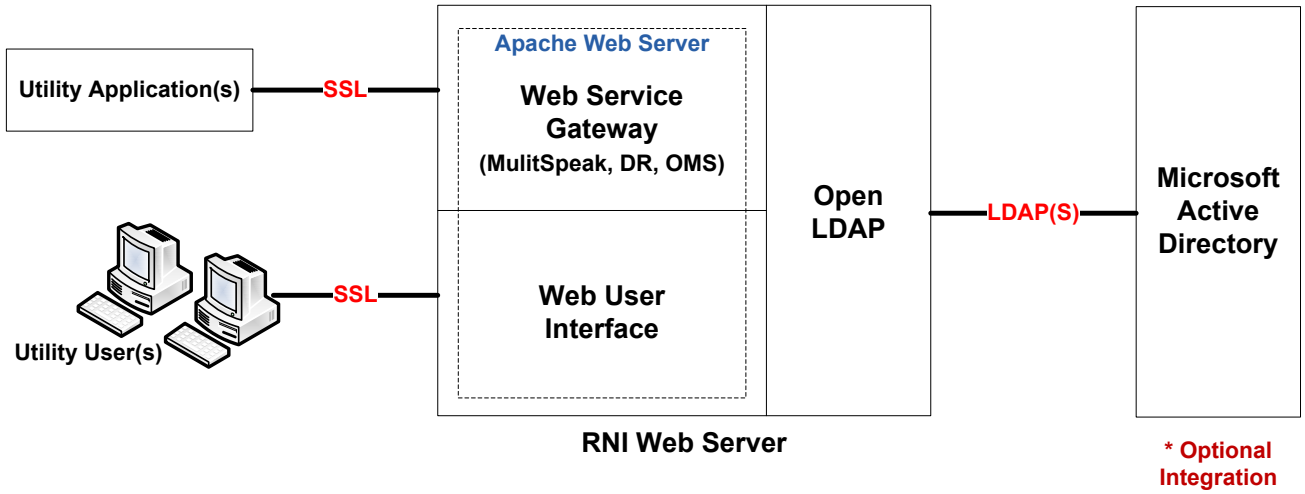


Figure 1: Interface security architecture

Transport Layer Security (TLS) overview

RNI systems employ Transport Layer Security (TLS) to encrypt all communication with the system as well as communication among the subcomponents within the system. This ensures the integrity of the data and the security of the users authorized to access the system.

All public-facing interfaces of an RNI system employ TLS 1.2 or higher with only strong-encryption algorithms enabled when encrypted communication is desired.

TLS is the successor of SSL (Secure Socket Layer). Due to the deep impact of SSL in computer and information security, the terms SSL and TLS are sometimes used interchangeably, e.g., SSL certificates.

TLS/SSL certificates are digital certificates which facilitate the encrypted connection between two entities. Certificates are also used to prove the identity of the servers, such as the RNI web server.

Certificates are linked together to create a chain of trust. At the top of the chain is the Root Certificate which identifies a root Certificate Authority (CA) such as VeriSign, DigiCert, and so on. The Root Certificates can be used to sign other certificates, which can be trusted and are part of the chain. Another type of certificate is a self-signed certificate, which is signed by an unapproved entity, not part of the chain of trust.

Sensus recommends that certificates issued by a well-trusted Certificate Authority are installed on RNI systems.

Web user interface – TLS

The Sensus application provides encryption to secure communications. This support is available on several of the RNI components. By default, TLS communication is enabled on the web server. As part of the installation, a self-signed digital certificate is generated on the web server for TLS communications. This certificate is generally used for the initial installation testing and system acceptance testing. Customers may choose to install a digital certificate from a public certificate authority (such as VeriSign, Entrust, or Go Daddy). The digital certificates and private keys are located in `/opt/flexnet/security/certs` and `/opt/flexnet/security/private` for commercial CA replacements.

Web service gateways

Note*:* If gateway components are installed on the web server, these are also TLS-enabled.

Sensus provides system-level interfaces for a variety of areas (MultiSpeak, Demand Response, Home Area Networking, and so on). These interfaces are protected using TLS encryption in the same manner as the web user interface. Because some of the web services support asynchronous notifications or callbacks, two-way TLS is recommended for protecting both directions of information flow. This requires setting up digital certificates and installing them in the appropriate key store (on the server host) and trust store (on the client host).

FlexNet communications

Information confidentiality is a key concern for Sensus and our customers. Because Sensus communications are encrypted, they are protected from end to end through the FlexNet network. Sensus has implemented encrypted communications across the FlexNet network using standards-based encryption algorithms, which provides confidentiality of the bi-directional communications between the endpoints and the head end system. Communications are encrypted at the endpoint/RNI using the AES algorithm with a 256-bit key. The communications remain encrypted across the network to the RNI/endpoint where it is decrypted. This provides protection for the information transmitted across the IP and RF networks.

In addition to confidentiality, end-to-end integrity of data and communication within the system is a key component of the Sensus security model. For communication across the FlexNet network, integrity of the communications to and from the endpoint is achieved through the use of authenticated messages. These messages are validated using the unique cryptographic key for the endpoint and also using the AES-CCM algorithm. This ensures that only communications originating from the RNI are processed by the endpoint. In addition, communications with the meter include a time-based quantum as a defense against replay attacks, or retransmission of communications.

In addition, FlexNet v2 mode supports asymmetric encryption using ECC p-256 curves. Support for ECDHA, ECDSA have been added to provide key derivation (of the AES-256 key), and digital signatures for Critical commands and firmware downloads.

By default, encryption is not enabled on the equipment when Sensus ships it to the customer. The customer can enable encryption, either by manual or automatic means, as desired upon installation of the device and receipt of the required cryptographic key material.

FlexNet endpoints

Sensus supports encrypted communications across all of its endpoint products. The encryption implementation is fundamentally the same across all device types. However, there are some differences between our electric-based devices (Electric and Distribution Automation) and battery-operated devices (Water and Gas). The main difference is in the setup of encrypted communications. Electric-based device radios are always on and can receive the commands to encrypt or rotate keys immediately, while battery-operated devices are in a Listen After Talk (LAT) mode for their radio communications. This limits the available timeframe for receiving commands and cryptographic keys. As a result, battery-operated endpoints take longer to enable encryption and rotate keys due to the limited communications timeframe. Customers are encouraged to consider the business and technology impacts when considering enabling encryption, such as field visits to endpoints with encrypted communications enabled.

RNI component security

As part of the software installation process, all RNI servers are hardened by default.

Security hardening for the Sensus RNI components is based on the Center for Internet Security Benchmarks: https://benchmarks.cisecurity.org.

Database server

The database server runs on Microsoft Windows Server 2019. Use the following steps to secure the database server:

1. Change default passwords for local accounts:
    - At a minimum, the Administrator account password should be changed to a complex password consisting of at least 8 characters with 1 alpha, 1 numeric, 1 uppercase alpha, 1 lowercase alpha, and 1 special character. An example of this would be *kH9v2&wB.*
    - Any other locally created accounts should have complex passwords matching the same criteria.
2. Change default passwords on the SQL Server:
    - The Sensus installation program sets all of the SQL database accounts to a default password for initial operation. Sensus recommends changing these accounts to unique complex passwords prior to any production release of our system. Details on how to perform these changes, and subsequent configurations across other components in the system are detailed in Appendix B: MS SQL database password change.

Third-party security controls

Sensus supports the installation of various third-party security applications for our products that run on general-purpose operating systems, such as Linux or Windows. Some examples of these security products are host-based firewalls, Anti-Virus/Anti-Spyware, Intrusion Detection/Prevention, and Host Integrity software. The Sensus components that support these types of security software are as follows:

- RNI Network Controller
- RNI Web Server
- FlexNet Database Server

Sensus does not certify all possible third-party security products in our environment because of the large number of solutions in the security marketplace. However, Sensus does provide information and configuration details to assist the customer in support of these products in their individual environments. Sensus will perform systems acceptance testing of all installed components and third-party security products to validate the installed functionality prior to final sign-off by the customer and Sensus. This provides the customer with a secure, reliable environment that supports industry standards.

The customer should weigh the risks versus rewards when considering third-party security solutions. In any case, it is suggested that all third-party applications and servers being considered are tested in a non-production environment and be approved for use in a production environment.

Firewall

Sensus supports the installation of host-based firewall applications on our products that run on general-purpose operating systems (Linux, Windows). In addition to any communication ports specific to the platform, Sensus has specific requirements for communication ports required for normal operations of the

product. These ports and protocols are detailed in the document *Sensus FlexNet RNI Server Port Settings* included on the installation media. In addition, the details for the Base Station firewall configuration are included in the *FlexNet® RNI Base Station Security Guide.*

Anti-virus and anti-spyware

Sensus supports the installation of anti-virus and anti-spyware software on our products that run on general-purpose operating systems (Linux, Windows). There are no specific configuration requirements for the normal operation of the product; the customer can configure the software based on their security requirements and policies.

Sensus does recommend for performance considerations to exclude certain directories and files for real-time scanning. Because of the constant access requirements for database files, Sensus recommends excluding these files. Specific details on the locations of these files are in the Microsoft SQL Server or Oracle Database documentation.

Intrusion detection and prevention

Sensus supports the installation of Intrusion Detection/Prevention applications on our products that run on general-purpose operating systems (Linux, Windows). There are no specific configuration requirements for the normal operation of the product; the customer can configure the software based on their security requirements and policies.

Host integrity software

Sensus supports the installation of Host Integrity Software products on our products that run on general-purpose operating systems (Linux, Windows). There are no specific configuration requirements for the normal operation of the product; the customer can configure the software based on their security requirements and policies.

Hardware Security Module

Sensus supports integration with SafeNet LunaSA Hardware Security Module (HSM) to provide hardware cryptographic key storage. In addition, the HSM provides cryptographic functions for encryption and decryption of application data. SafeNet LunaSA provides a FIPS 140-2 Level 3 device for secure key generation and storage. Additional information and integration can be found in the *FlexNet® RNI Hardware Security Module Installation Guide*.

Appendix A: Red Hat Enterprise Linux 8 CIS benchmark compliance v2.0

Reference ID	Description	Compliant	Notes
1.1.1.1	Ensure mounting of cramfs filesystems is disabled (Automated)	Yes	
1.1.1.2	Ensure mounting of squashfs filesystems is disabled (Automated)	Yes	
1.1.1.3	Ensure mounting of udf filesystems is disabled (Automated)	Yes	
1.1.2.1	Ensure /tmp is a separate partition (Automated)	Yes	
1.1.2.2	Ensure nodev option set on /tmp partition (Automated)	No	Customer optional configuration item
1.1.2.3	Ensure noexec option set on /tmp partition (Automated)	No	Customer optional configuration item
1.1.2.4	Ensure nosuid option set on /tmp partition (Automated)	No	Customer optional configuration item
1.1.3.1	Ensure separate partition exists for /var (Automated)	Yes	
1.1.3.2	Ensure nodev option set on /var partition (Automated)	No	Customer optional configuration item
1.1.3.3	Ensure noexec option set on /var partition (Automated)	No	Customer optional configuration item
1.1.3.4	Ensure nosuid option set on /var partition (Automated)	No	Customer optional configuration item
1.1.4.1	Ensure separate partition exists for /var/tmp (Automated)	Yes	
1.1.4.2	Ensure noexec option set on /var/tmp partition (Automated)	No	Customer optional configuration item
1.1.4.3	Ensure nosuid option set on /var/tmp partition (Automated)	No	Customer optional configuration item
1.1.4.4	Ensure nodev option set on /var/tmp partition (Automated)	No	Customer optional configuration item
1.1.5.1	Ensure separate partition exists for /var/log (Automated)	Yes	
1.1.5.2	Ensure nodev option set on /var/log partition (Automated)	No	Customer optional configuration item
1.1.5.3	Ensure noexec option set on /var/log partition (Automated)	No	Customer optional configuration item
1.1.5.4	Ensure nosuid option set on /var/log partition (Automated)	No	Customer optional configuration item

Reference ID	Description	Compliant	Notes
1.1.6.1	Ensure separate partition exists for /var/log/audit (Automated)	Yes	
1.1.6.2	Ensure noexec option set on /var/log/audit partition (Automated)	No	Customer optional configuration item
1.1.6.3	Ensure nodev option set on /var/log/audit partition (Automated)	No	Customer optional configuration item
1.1.6.4	Ensure nosuid option set on /var/log/audit partition (Automated)	No	Customer optional configuration item
1.1.7.1	Ensure separate partition exists for /home (Automated)	Yes	
1.1.7.2	Ensure nodev option set on /home partition (Automated)	No	Customer optional configuration item
1.1.7.3	Ensure nosuid option set on /home partition (Automated)	No	Customer optional configuration item
1.1.7.4	Ensure usrquota option set on /home partition (Automated)	No	Customer optional configuration item
1.1.7.5	Ensure grpquota option set on /home partition (Automated)	No	Customer optional configuration item
1.1.8.1	Ensure nodev option set on /dev/shm partition (Automated)	Yes	
1.1.8.2	Ensure noexec option set on /dev/shm partition (Automated)	No	Needed for Oracle RNIs
1.1.8.3	Ensure nosuid option set on /dev/shm partition (Automated)	Yes	
1.1.9	Disable Automounting (Automated)	Yes	
1.1.10	Disable USB Storage (Automated)	Yes	
1.2.1	Ensure Red Hat Subscription Manager connection is configured (Manual)	Yes	
1.2.2	Ensure GPG keys are configured (Manual)	Yes	
1.2.3	Ensure gpgcheck is globally activated (Automated)	Yes	
1.2.4	Ensure package manager repositories are configured (Manual)	Yes	
1.3.1	Ensure AIDE is installed (Automated)	Yes	

Reference ID	Description	Compliant	Notes
1.3.2	Ensure filesystem integrity is regularly checked (Automated)	No	Customer optional configuration item
1.4.1	Ensure bootloader password is set (Automated)	No	Customer optional configuration item
1.4.2	Ensure permissions on bootloader config are configured (Automated)	Yes	
1.4.3	Ensure authentication is required when booting into rescue mode (Automated)	Yes	
1.5.1	Ensure core dump storage is disabled (Automated)	Yes	
1.5.2	Ensure core dump backtraces are disabled (Automated)	Yes	
1.5.3	Ensure address space layout randomization (ASLR) is enabled (Automated)	Yes	
1.6.1.1	Ensure SELinux is installed (Automated)	Yes	
1.6.1.2	Ensure SELinux is not disabled in bootloader configuration (Automated)	Yes	
1.6.1.3	Ensure SELinux policy is configured (Automated)	Yes	
1.6.1.4	Ensure the SELinux mode is not disabled (Automated)	No	Customer optional configuration item
1.6.1.5	Ensure the SELinux mode is enforcing (Automated)	No	Customer optional configuration item
1.6.1.6	Ensure no unconfined services exist (Automated)	Yes	
1.6.1.7	Ensure SETroubleshoot is not installed (Automated)	Yes	
1.6.1.8	Ensure the MCS Translation Service (mcstrans) is not installed (Automated)	Yes	
1.7.1	Ensure message of the day is configured properly (Automated)	Yes	
1.7.2	Ensure local login warning banner is configured properly (Automated)	Yes	
1.7.3	Ensure remote login warning banner is configured properly (Automated)	Yes	

Reference ID	Description	Compliant	Notes
1.7.4	Ensure permissions on /etc/motd are configured (Automated)	Yes	
1.7.5	Ensure permissions on /etc/issue are configured (Automated)	Yes	
1.7.6	Ensure permissions on /etc/issue.net are configured (Automated)	Yes	
1.8.1	Ensure GNOME Display Manager is removed (Manual)	Yes	
1.8.2	Ensure GDM login banner is configured (Automated)	Yes	
1.8.3	Ensure last logged in user display is disabled (Automated)	Yes	
1.8.4	Ensure XDMCP is not enabled (Automated)	Yes	
1.8.5	Ensure automatic mounting of removable media is disabled (Automated)	Yes	
1.9	Ensure updates, patches, and additional security software are installed (Manual)	No	Customer must manually update
1.10	Ensure system-wide crypto policy is not legacy (Automated)	Yes	
2.1.1	Ensure time synchronization is in use (Manual)	Yes	
2.1.2	Ensure chrony is configured (Automated)	Yes	
2.2.1	Ensure xinetd is not installed (Automated)	Yes	
2.2.2	Ensure xorg-x11-server-common is not installed (Automated)	Yes	
2.2.3	Ensure Avahi Server is not installed (Automated)	Yes	
2.2.4	Ensure CUPS is not installed (Automated)	Yes	
2.2.5	Ensure DHCP Server is not installed (Automated)	Yes	
2.2.6	Ensure DNS server is not installed (Automated)	Yes	

Reference ID	Description	Compliant	Notes
2.2.7	Ensure FTP Server is not installed (Automated)	Yes	
2.2.8	Ensure VSFTP Server is not installed (Automated)	Yes	
2.2.9	Ensure TFTP Server is not installed (Automated)	Yes	
2.2.10	Ensure a web server is not installed (Automated)	No	Needed for RNI operation
2.2.11	Ensure IMAP and POP3 server is not installed (Automated)	Yes	
2.2.12	Ensure Samba is not installed (Automated)	Yes	
2.2.13	Ensure HTTP Proxy Server is not installed (Automated)	Yes	
2.2.14	Ensure net-snmp is not installed (Automated)	Yes	
2.2.15	Ensure NIS server is not installed (Automated)	Yes	
2.2.16	Ensure telnet-server is not installed (Automated)	Yes	
2.2.17	Ensure mail transfer agent is configured for local-only mode (Automated)	Yes	
2.2.18	Ensure nfs-utils is not installed or the nfs-server service is masked (Automated)	Yes	
2.2.19	Ensure rpcbind is not installed or the rpcbind services are masked (Automated)	No	Needed for RNI installation
2.2.20	Ensure rsync is not installed or the rsyncd service is masked (Automated)	Yes	
2.3.1	Ensure NIS Client is not installed (Automated)	Yes	
2.3.2	Ensure rsh client is not installed (Automated)	Yes	
2.3.3	Ensure talk client is not installed (Automated)	Yes	
2.3.4	Ensure telnet client is not installed (Automated)	Yes	

Reference ID	Description	Compliant	Notes
2.3.5	Ensure LDAP client is not installed (Automated)	No	Needed for RNI operation
2.3.6	Ensure TFTP client is not installed (Automated)	Yes	
2.4	Ensure nonessential services are removed or masked (Manual)	Yes	
3.1.1	Verify if IPv6 is enabled on the system (Manual)	No	Customer optional configuration item
3.1.2	Ensure SCTP is disabled (Automated)	Yes	
3.1.3	Ensure DCCP is disabled (Automated)	Yes	
3.1.4	Ensure wireless interfaces are disabled (Automated)	No	No wireless controllers installed
3.2.1	Ensure IP forwarding is disabled (Automated)	No	Customer optional configuration item
3.2.2	Ensure packet redirect sending is disabled (Automated)	Yes	
3.3.1	Ensure source routed packets are not accepted (Automated)	Yes	
3.3.2	Ensure ICMP redirects are not accepted (Automated)	Yes	
3.3.3	Ensure secure ICMP redirects are not accepted (Automated)	Yes	
3.3.4	Ensure suspicious packets are logged (Automated)	Yes	
3.3.5	Ensure broadcast ICMP requests are ignored (Automated)	Yes	
3.3.6	Ensure bogus ICMP responses are ignored (Automated)	Yes	
3.3.7	Ensure Reverse Path Filtering is enabled (Automated)	Yes	
3.3.8	Ensure TCP SYN Cookies is enabled (Automated)	Yes	
3.3.9	Ensure IPv6 router advertisements are not accepted (Automated)	Yes	
3.4.1.1	Ensure firewalld is installed (Automated)	Yes	

Reference ID	Description	Compliant	Notes
3.4.1.2	Ensure iptables-services is not installed with firewalld (Automated)	Yes	
3.4.1.3	Ensure nftables either not installed or masked with firewalld (Automated)	Yes	
3.4.1.4	Ensure firewalld service enabled and running (Automated)	Yes	
3.4.1.5	Ensure firewalld default zone is set (Automated)	Yes	
3.4.1.6	Ensure network interfaces are assigned to appropriate zone (Manual)	Yes	
3.4.1.7	Ensure firewalld drops unnecessary services and ports (Manual)	Yes	
3.4.2.1	Ensure nftables is installed (Automated)	Yes	
3.4.2.2	Ensure firewalld is either not installed or masked with nftables (Automated)	Yes	
3.4.2.3	Ensure iptables-services not installed with nftables (Automated)	Yes	
3.4.2.4	Ensure iptables are flushed with nftables (Manual)	Yes	
3.4.2.5	Ensure a nftables table exists (Automated)	Yes	
3.4.2.6	Ensure nftables base chains exist (Automated)	Yes	
3.4.2.7	Ensure nftables loopback traffic is configured (Automated)	Yes	
3.4.2.8	Ensure nftables outbound and established connections are configured (Manual)	Yes	
3.4.2.9	Ensure nftables default deny firewall policy (Automated)	Yes	
3.4.2.10	Ensure nftables service is enabled (Automated)	Yes	
3.4.2.11	Ensure nftables rules are permanent (Automated)	Yes	
3.4.3.1.1	Ensure iptables packages are installed (Automated)	Yes	

Reference ID	Description	Compliant	Notes
3.4.3.1.2	Ensure nftables is not installed with iptables (Automated)	Yes	
3.4.3.1.3	Ensure firewalld is either not installed or masked with iptables (Automated)	No	RNI uses firewalld
3.4.3.2.1	Ensure iptables loopback traffic is configured (Automated)	Yes	
3.4.3.2.2	Ensure iptables outbound and established connections are configured (Manual)	Yes	
3.4.3.2.3	Ensure iptables rules exist for all open ports (Automated)	Yes	
3.4.3.2.4	Ensure iptables default deny firewall policy (Automated)	Yes	
3.4.3.2.5	Ensure iptables rules are saved (Automated)	Yes	
3.4.3.2.6	Ensure iptables is enabled and running (Automated)	Yes	
3.4.3.3.1	Ensure ip6tables loopback traffic is configured (Automated)	No	Customer optional configuration item
3.4.3.3.2	Ensure ip6tables outbound and established connections are configured (Manual)	No	Customer optional configuration item
3.4.3.3.3	Ensure ip6tables firewall rules exist for all open ports (Automated)	No	Customer optional configuration item
3.4.3.3.4	Ensure ip6tables default deny firewall policy (Automated)	No	Customer optional configuration item
3.4.3.3.5	Ensure ip6tables rules are saved (Automated)	No	Customer optional configuration item
3.4.3.3.6	Ensure ip6tables is enabled and active (Automated)	No	Customer optional configuration item
4.1.1.1	Ensure auditd is installed (Automated)	Yes	
4.1.1.2	Ensure auditd service is enabled (Automated)	Yes	
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled (Automated)	Yes	
4.1.1.4	Ensure audit_backlog_limit is sufficient (Automated)	Yes	

Reference ID	Description	Compliant	Notes
4.1.2.1	Ensure audit log storage size is configured (Automated)	Yes	
4.1.2.2	Ensure audit logs are not automatically deleted (Automated)	No	Customer optional configuration item
4.1.2.3	Ensure system is disabled when audit logs are full (Automated)	No	Customer optional configuration item
4.1.3.1	Ensure changes to system administration scope (sudoers) is collected (Automated)	Yes	
4.1.3.2	Ensure actions as another user are always logged (Automated)	No	Customer optional configuration item
4.1.3.3	Ensure events that modify the sudo log file are collected (Automated)	No	Customer optional configuration item
4.1.3.4	Ensure events that modify date and time information are collected (Automated)	Yes	
4.1.3.5	Ensure events that modify the system's network environment are collected (Automated)	Yes	
4.1.3.6	Ensure use of privileged commands are collected (Automated)	No	Customer optional configuration item
4.1.3.7	Ensure unsuccessful file access attempts are collected (Automated)	Yes	
4.1.3.8	Ensure events that modify user/group information are collected (Automated)	Yes	
4.1.3.9	Ensure discretionary access control permission modification events are collected (Automated)	Yes	
4.1.3.10	Ensure successful file system mounts are collected (Automated)	Yes	
4.1.3.11	Ensure session initiation information is collected (Automated)	Yes	
4.1.3.12	Ensure login and logout events are collected (Automated)	Yes	
4.1.3.13	Ensure file deletion events by users are collected (Automated)	Yes	
4.1.3.14	Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	Yes	
4.1.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)	No	Customer optional configuration item

Reference ID	Description	Compliant	Notes
4.1.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)	No	Customer optional configuration item
4.1.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)	No	Customer optional configuration item
4.1.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)	No	Customer optional configuration item
4.1.3.19 (Level 2)	Ensure kernel module loading unloading and modification is collected (Automated)	No	Customer optional configuration item
4.1.3.20	Ensure the audit configuration is immutable (Automated)	No	Customer optional configuration item
4.1.3.21	Ensure the running and on disk configuration is the same (Manual)	Yes	
4.2.1.1	Ensure rsyslog is installed (Automated)	Yes	
4.2.1.2	Ensure rsyslog service is enabled (Automated)	Yes	
4.2.1.3	Ensure journald is configured to send logs to rsyslog (Manual)	No	Customer optional configuration item
4.2.1.4	Ensure rsyslog default file permissions are configured (Automated)	Yes	
4.2.1.5	Ensure logging is configured (Manual)	No	Customer optional configuration item
4.2.1.6	Ensure rsyslog is configured to send logs to a remote log host (Manual)	No	Customer optional configuration item
4.2.1.7	Ensure rsyslog is not configured to recieve logs from a remote client (Automated)	Yes	
4.2.2.1.1	Ensure systemd-journal-remote is installed (Manual)	No	Customer optional configuration item
4.2.2.1.2	Ensure systemd-journal-remote is configured (Manual)	No	Customer optional configuration item
4.2.2.1.3	Ensure systemd-journal-remote is enabled (Manual)	No	Customer optional configuration item
4.2.2.1.4	Ensure journald is not configured to recieve logs from a remote client (Automated)	No	Customer optional configuration item
4.2.2.2	Ensure journald service is enabled (Automated)	Yes	

Reference ID	Description	Compliant	Notes
4.2.2.3	Ensure journald is configured to compress large log files (Automated)	Yes	
4.2.2.4	Ensure journald is configured to write logfiles to persistent disk (Automated)	Yes	
4.2.2.5	Ensure journald is not configured to send logs to rsyslog (Manual)	Yes	
4.2.2.6	Ensure journald log rotation is configured per site policy (Manual)	No	Customer optional configuration item
4.2.2.7	Ensure journald default file permissions configured (Manual)	No	Customer optional configuration item
4.2.3	Ensure permissions on all logfiles are configured (Automated)	No	Customer optional configuration item
4.3	Ensure logrotate is configured (Manual)	No	Customer optional configuration item
5.1.1	Ensure cron daemon is enabled (Automated)	Yes	
5.1.2	Ensure permissions on /etc/crontab are configured (Automated)	Yes	
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Automated)	Yes	
5.1.4	Ensure permissions on /etc/cron.daily are configured (Automated)	Yes	
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Automated)	Yes	
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Automated)	Yes	
5.1.7	Ensure permissions on /etc/cron.d are configured (Automated)	Yes	
5.1.8	Ensure cron is restricted to authorized users (Automated)	Yes	
5.1.9	Ensure at is restricted to authorized users (Automated)	Yes	
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	Yes	
5.2.2	Ensure permissions on SSH private host key files are configured (Automated)	Yes	

Reference ID	Description	Compliant	Notes
5.2.3	Ensure permissions on SSH public host key files are configured (Automated)	Yes	
5.2.4	Ensure SSH access is limited (Automated)	No	Customer optional configuration item
5.2.5	Ensure SSH LogLevel is appropriate (Automated)	Yes	
5.2.6	Ensure SSH PAM is enabled (Automated)	Yes	
5.2.7	Ensure SSH root login is disabled (Automated)	No	Needed for RNI installation
5.2.8	Ensure SSH HostbasedAuthentication is disabled (Automated)	Yes	
5.2.9	Ensure SSH PermitEmptyPasswords is disabled (Automated)	Yes	
5.2.10	Ensure SSH PermitUserEnvironment is disabled (Automated)	Yes	
5.2.11	Ensure SSH IgnoreRhosts is enabled (Automated)	Yes	
5.2.12	Ensure SSH X11 forwarding is disabled (Automated)	Yes	
5.2.13	Ensure SSH AllowTcpForwarding is disabled (Automated)	Yes	
5.2.14	Ensure system-wide crypto policy is not over-ridden (Automated)	Yes	
5.2.15	Ensure SSH warning banner is configured (Automated)	Yes	
5.2.16	Ensure SSH MaxAuthTries is set to 4 or less (Automated)	Yes	
5.2.17	Ensure SSH MaxStartups is configured (Automated)	Yes	
5.2.18	Ensure SSH MaxSessions is set to 10 or less (Automated)	Yes	
5.2.19	Ensure SSH LoginGraceTime is set to one minute or less (Automated)	No	Customer optional configuration item
5.2.20	Ensure SSH Idle Timeout Interval is configured (Automated)	Yes	

Reference ID	Description	Compliant	Notes
5.3.1	Ensure sudo is installed (Automated)	Yes	
5.3.2	Ensure sudo commands use pty (Automated)	Yes	
5.3.3	Ensure sudo log file exists (Automated)	Yes	
5.3.4	Ensure users must provide password for escalation (Automated)	Yes	
5.3.5	Ensure re-authentication for privilege escalation is not disabled globally (Automated)	Yes	
5.3.6	Ensure sudo authentication timeout is configured correctly (Automated)	Yes	
5.3.7	Ensure access to the su command is restricted (Automated)	No	Customer optional configuration item
5.4.1	Ensure custom authselect profile is used (Manual)	No	Customer optional configuration item
5.4.2	Ensure authselect includes with-faillock (Automated)	No	Customer optional configuration item
5.5.1	Ensure password creation requirements are configured (Automated)	No	Need for RNI installation
5.5.2	Ensure lockout for failed password attempts is configured (Automated)	No	Customer optional configuration item
5.5.3	Ensure password reuse is limited (Automated)	No	Customer optional configuration item
5.5.4	Ensure password hashing algorithm is SHA-512 (Automated)	Yes	
5.6.1.1	Ensure password expiration is 365 days or less (Automated)	Yes	
5.6.1.2	Ensure minimum days between password changes is 7 or more (Automated)	No	Customer optional configuration item
5.6.1.3	Ensure password expiration warning days is 7 or more (Automated)	Yes	
5.6.1.4	Ensure inactive password lock is 30 days or less (Automated)	No	Customer optional configuration item
5.6.1.5	Ensure all users last password change date is in the past (Automated)	Yes	

Reference ID	Description	Compliant	Notes
5.6.2	Ensure system accounts are secured (Automated)	Yes	
5.6.3	Ensure default user shell timeout is 900 seconds or less (Automated)	No	Customer optional configuration item
5.6.4	Ensure default group for the root account is GID 0 (Automated)	Yes	
5.6.5	Ensure default user umask is 027 or more restrictive (Automated)	No	Too restrictive for normal RNI operation
6.1.1	Audit system file permissions (Manual)	No	Customer optional configuration item
6.1.2	Ensure sticky bit is set on all world-writable directories (Automated)	Yes	
6.1.3	Ensure permissions on /etc/passwd are configured (Automated)	Yes	
6.1.4	Ensure permissions on /etc/shadow are configured (Automated)	Yes	
6.1.5	Ensure permissions on /etc/group are configured (Automated)	Yes	
6.1.6	Ensure permissions on /etc/gshadow are configured (Automated)	Yes	
6.1.7	Ensure permissions on /etc/passwd- are configured (Automated)	Yes	
6.1.8	Ensure permissions on /etc/shadow- are configured (Automated)	Yes	
6.1.9	Ensure permissions on /etc/group- are configured (Automated)	Yes	
6.1.10	Ensure permissions on /etc/gshadow- are configured (Automated)	Yes	
6.1.11	Ensure no world writable files exist (Automated)	Yes	
6.1.12	Ensure no unowned files or directories exist (Automated)	Yes	
6.1.13	Ensure no ungrouped files or directories exist (Automated)	Yes	
6.1.14	Audit SUID executables (Manual)	Yes	

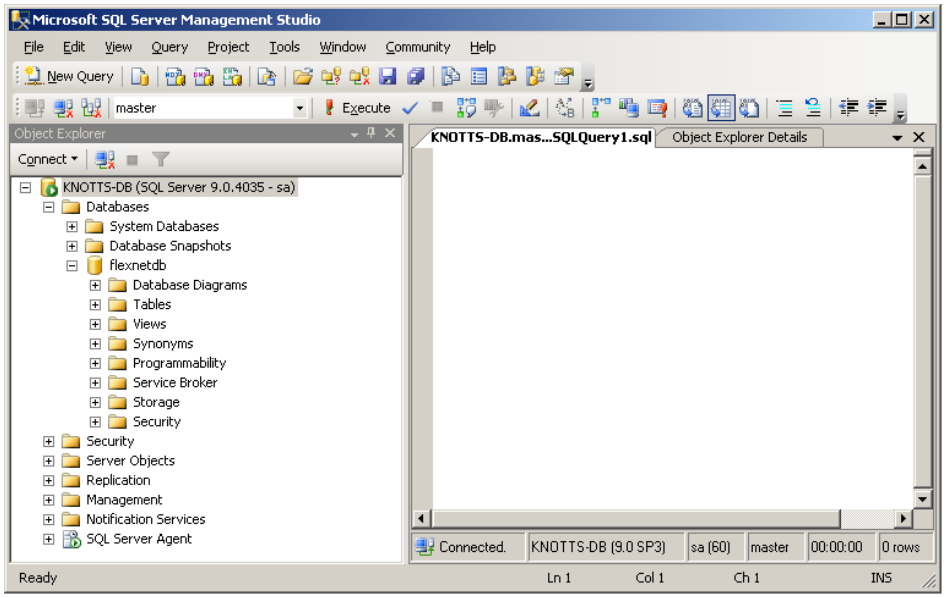
Reference ID	Description	Compliant	Notes
6.1.15	Audit SGID executables (Manual)	Yes	
6.2.1	Ensure password fields are not empty (Automated)	Yes	
6.2.2	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	Yes	
6.2.3	Ensure no duplicate UIDs exist (Automated)	Yes	
6.2.4	Ensure no duplicate GIDs exist (Automated)	Yes	
6.2.5	Ensure no duplicate user names exist (Automated)	Yes	
6.2.6	Ensure no duplicate group names exist (Automated)	Yes	
6.2.7	Ensure root PATH Integrity (Automated)	Yes	
6.2.8	Ensure root is the only UID 0 account (Automated)	Yes	
6.2.9	Ensure all users' home directories exist (Automated)	Yes	
6.2.10	Ensure users own their home directories (Automated)	Yes	
6.2.11	Ensure users' home directories permissions are 750 or more restrictive (Automated)	Yes	
6.2.12	Ensure users' dot files are not group or world writable (Automated)	Yes	
6.2.13	Ensure users' .netrc Files are not group or world accessible (Automated)	Yes	
6.2.14	Ensure no users have .forward files (Automated)	Yes	
6.2.15	Ensure no users have .netrc files (Automated)	Yes	
6.2.16	Ensure no users have .rhosts files (Automated)	Yes	

Appendix B: MS SQL database password change

Because your DBA likely changes passwords periodically as a routine security measure, this section describes how to modify a database user's password, and how to make the necessary changes in other parts of the RNI when the password is changed.

Changing a DB user password

1. Launch SQL Server Management Studio.
2. Log in using a valid login/password (see the FlexNet RNI Pre-Installation Form).
3. Select **New Query**.



4. Enter the ALTER command into the new query window:

   ALTER LOGIN login WITH PASSWORD = 'password';

5. Click **Execute**.

For example, the following query will change the password of login "sa" to a new strong password:

ALTER LOGIN sa WITH PASSWORD = '<enterStrongPasswordHere>';

***IMPORTANT**: Be sure to record this password change in the FlexNet RNI Pre-Installation Form.*

Database *sa* user considerations

The *sa* account is not used in the Sensus application, and it can be disabled on the database using the following SQL command:

```
ALTER LOGIN sa DISABLE;
ALTER LOGIN sa WITH NAME = [sys-admin];
```

Changing passwords that affect other RNI components

Some of the built-in users of the MS SQL Server database are remote from the database and have their passwords defined elsewhere, as well as in the database itself. These users include:

- maps_<database_name>
- mdmif_<database_name>
- parsers_<database_name>
- scheduler_<database_name>
- simsetup_<database_name>
- reports_<database_name>
- stats_<database_name>
- twoway_<database_name>
- web_<database_name>

If you change the password of any of these DB users via MS SQL Studio, you must be sure to update their corresponding definitions throughout the RNI.

The following table lists the database users and the files in which their passwords are configured. When you change a password in MS SQL Studio, you must also access the files shown in the **Where Else Defined** column and duplicate the password change. (Note the user names stated in Table 1 are the default names, having the FlexNetDB database-name appendage.) As you locate each file, open it in the editor of your choice, identify and change the appropriate values, and then save and close the file.

Table 1: Database users and password change file updates

Database User	Where Else Defined
mdmif_FlexNetDB	The NC server's `flexnet.flexnetdb.mssql.properties` file
parsers_FlexNetDB	The NC server's `flexnet.flexnetdb.mssql.properties` file
scheduler_FlexNetDB	The NC server's `flexnet.flexnetdb.mssql.properties` file
reports_FlexNetDB	The NC server's `flexnet.flexnetdb.mssql.properties` file
twoway_FlexNetDB	The NC server's `flexnet.flexnetdb.mssql.properties` file
web_FlexNetDB	• The NC server's `flexnet.flexnetdb.mssql.properties` file • The Web server's `settings.properties` file

Appendix C: Windows Server (2019) CIS 2.0 benchmark compliance

Reference ID	Description	Compliant	Notes
1.1.1	Ensure 'Enforce password history' is set to '24 or more password(s)	Yes	
1.1.2	Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'	Yes	
1.1.3	Ensure 'Minimum password age' is set to '1 or more day(s)'	Yes	
1.1.4	Ensure 'Minimum password length' is set to '14 or more character(s)'	No	Default user created during install time does not have a long password.
1.1.5	Ensure 'Password must meet complexity requirements' is set to 'Enabled'	Yes	
1.1.6	Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	Yes	
1.2.1	Ensure 'Account lockout duration' is set to '15 or more minute(s)'	Yes	
1.2.2	Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'	Yes	
1.2.3	Ensure 'Allow Administrator account lockout' is set to 'Enabled'	Yes	
1.2.4	Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'	Yes	
2.2.1	Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'	Yes	
2.2.2	Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS'	N/A	Applies to domain controllers only
2.2.3	Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users'	Yes	
2.2.4	Ensure 'Act as part of the operating system' is set to 'No One'	Yes	
2.2.5	Ensure 'Add workstations to domain' is set to 'Administrators'	N/A	Applies to domain controllers only
2.2.6	Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	Yes	
2.2.7	Ensure 'Allow log on locally' is set to 'Administrators'	Yes	
2.2.8	Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators'	N/A	Applies to domain controllers only
2.2.9	Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'	Yes	

Reference ID	Description	Compliant	Notes
2.2.10	Ensure 'Back up files and directories' is set to 'Administrators'	Yes	
2.2.11	Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	Yes	
2.2.12	Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE'	Yes	
2.2.13	Ensure 'Create a pagefile' is set to 'Administrators'	Yes	
2.2.14	Ensure 'Create a token object' is set to 'No One'	Yes	
2.2.15	Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Yes	
2.2.16	Ensure 'Create permanent shared objects' is set to 'No One'	Yes	
2.2.17	Ensure 'Create symbolic links' is set to 'Administrators'	N/A	Applies to domain controllers only
2.2.18	Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines'	Yes	
2.2.19	Ensure 'Debug programs' is set to 'Administrators'	Yes	
2.2.20	Ensure 'Deny access to this computer from the network' to include 'Guests'	N/A	Applies to domain controllers only
2.2.21	Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group'	No	Remote admin done via RDP using local Admin user
2.2.22	Ensure 'Deny log on as a batch job' to include 'Guests'	Yes	
2.2.23	Ensure 'Deny log on as a service' to include 'Guests'	Yes	
2.2.24	Ensure 'Deny log on locally' to include 'Guests'	Yes	
2.2.25	Ensure 'Deny log on through Remote Desktop Services' to include 'Guests'	N/A	Applies to domain controllers only
2.2.26	Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account'	No	Remote admin done via RDP using local Admin user
2.2.27	Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators'	N/A	Applies to domain controllers only
2.2.28	Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One'	Yes	
2.2.29	Ensure 'Force shutdown from a remote system' is set to 'Administrators'	Yes	
2.2.30	Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	Yes	
2.2.31	Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	N/A	Applies to domain controllers only

Reference ID	Description	Compliant	Notes
2.2.32	Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' and (when the Web Server (IIS) Role with Web Services Role Service is installed) 'IIS_IUSRS'	Yes	
2.2.33	Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'	Yes	
2.2.34	Ensure 'Load and unload device drivers' is set to 'Administrators'	Yes	
2.2.35	Ensure 'Lock pages in memory' is set to 'No One'	Yes	
2.2.36	Ensure 'Log on as a batch job' is set to 'Administrators'	N/A	Applies to domain controllers only
2.2.37	Ensure 'Manage auditing and security log' is set to 'Administrators` and (when Exchange is running in the environment) `Exchange Servers'	N/A	Applies to domain controllers only
2.2.38	Ensure 'Manage auditing and security log' is set to 'Administrators'	Yes	
2.2.39	Ensure 'Modify an object label' is set to 'No One'	Yes	
2.2.40	Ensure 'Modify firmware environment values' is set to 'Administrators'	Yes	
2.2.41	Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	Yes	
2.2.42	Ensure 'Profile single process' is set to 'Administrators'	Yes	
2.2.43	Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'	Yes	
2.2.44	Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	Yes	
2.2.45	Ensure 'Restore files and directories' is set to 'Administrators'	Yes	
2.2.46	Ensure 'Shut down the system' is set to 'Administrators'	Yes	
2.2.47	Ensure 'Synchronize directory service data' is set to 'No One'	N/A	Applies to domain controllers only
2.2.48	Ensure 'Take ownership of files or other objects' is set to 'Administrators'	Yes	
2.3.1.1	Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts	Yes	
2.3.1.2	Ensure 'Accounts: Guest account status' is set to 'Disabled'	Yes	
2.3.1.3	Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	Yes	
2.3.1.4	Configure 'Accounts: Rename administrator account'	No	Remote admin done via RDP using local Admin user
2.3.1.5	Configure 'Accounts: Rename guest account'	Yes	

Reference ID	Description	Compliant	Notes
2.3.2.1	Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	Yes	
2.3.2.2	Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'	Yes	
2.3.4.1	Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'	Yes	
2.3.4.2	Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'	Yes	
2.3.5.1 - 2.3.5.3	Domain Controller	N/A	Applies to domain controllers only
2.3.6.1	Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'	Yes	
2.3.6.2	Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled'	Yes	
2.3.6.3	Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled'	Yes	
2.3.6.4	Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'	Yes	
2.3.6.5	Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'	Yes	
2.3.6.6	Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled'	Yes	
2.3.7.1	Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'	Yes	
2.3.7.2	Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'	Yes	
2.3.7.3	Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'	Yes	
2.3.7.4	Configure 'Interactive logon: Message text for users attempting to log on'	Yes	
2.3.7.5	Configure 'Interactive logon: Message title for users attempting to log on'	Yes	
2.3.7.6 (Level 2)	Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)'	Yes	
2.3.7.7	Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'	Yes	
2.3.7.8	Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled'	Yes	
2.3.7.9	Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	Yes	

Reference ID	Description	Compliant	Notes
2.3.8.1	Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	Yes	
2.3.8.2	Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'	Yes	
2.3.8.3	Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'	Yes	
2.3.9.1	Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0'	Yes	
2.3.9.2	Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	Yes	
2.3.9.3	Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	Yes	
2.3.9.4	Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'	Yes	
2.3.9.5	Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher	Yes	
2.3.10.1	Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	Yes	
2.3.10.2	Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'	Yes	
2.3.10.3	Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	Yes	
2.3.10.4 (Level 2)	Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'	Yes	
2.3.10.5	Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'	Yes	
2.3.10.6	Configure 'Network access: Named Pipes that can be accessed anonymously'	N/A	Applies to domain controllers only
2.3.10.7	Configure 'Network access: Named Pipes that can be accessed anonymously'	Yes	
2.3.10.8	Configure 'Network access: Remotely accessible registry paths' is configured	Yes	
2.3.10.9	Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured	Yes	
2.3.10.10	Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'	Yes	
2.3.10.11	Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'	Yes	
2.3.10.12	Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	Yes	

Reference ID	Description	Compliant	Notes
2.3.10.13	Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'	Yes	
2.3.11.1	Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'	Yes	
2.3.11.2	Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	Yes	
2.3.11.3	Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	Yes	
2.3.11.4	Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	Yes	
2.3.11.5	Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'	Yes	
2.3.11.6	Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'	Yes	
2.3.11.7	Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'	Yes	
2.3.11.8	Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher	Yes	
2.3.11.9	Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	Yes	
2.3.11.10	Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	Yes	
2.3.13.1	Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled'	Yes	
2.3.15.1	Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled'	Yes	
2.3.15.2	Ensure 'System objects: Strengthen default permissions of internal system objects (e.g., Symbolic Links)' is set to 'Enabled'	Yes	
2.3.17.1	Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	Yes	
2.3.17.2	Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher	No	Installation scripts require this
2.3.17.3	Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	No	Installation scripts require this
2.3.17.4	Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'	Yes	
2.3.17.5	Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'	Yes	

Reference ID	Description	Compliant	Notes
2.3.17.6	Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'	Yes	
2.3.17.7	Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'	Yes	
2.3.17.8	Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'	Yes	
5.1	Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only)	N/A	Applies to domain controllers only
5.2	Ensure 'Print Spooler (Spooler)' is set to 'Disabled	Yes	
9.1.1	Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On' (recommended)	Yes	
9.1.2	Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	Yes	
9.1.3	Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	Yes	
9.1.4	Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'	Yes	
9.1.5	Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'	Yes	
9.1.6	Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Yes	
9.1.7	Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	Yes	
9.1.8	Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'	Yes	
9.2.1	Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	Yes	
9.2.2	Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	Yes	
9.2.3	Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'	Yes	
9.2.4	Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	Yes	
9.2.5	Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log'	Yes	
9.2.6	Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Yes	
9.2.7	Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	Yes	
9.2.8	Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	Yes	

Reference ID	Description	Compliant	Notes
9.3.1	Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	Yes	
9.3.2	Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	Yes	
9.3.3	Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'	Yes	
9.3.4	Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'	Yes	
9.3.5	Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	Yes	
9.3.6	Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'	Yes	
9.3.7	Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'	Yes	
9.3.8	Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater	Yes	
9.3.9	Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	Yes	
9.3.10	Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	Yes	
17.1.1	Ensure 'Audit Credential Validation' is set to 'Success and Failure'	Yes	
17.1.2	Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only)	N/A	Applies to domain controllers only
17.1.3	Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only)	N/A	Applies to domain controllers only
17.2.1	Ensure 'Audit Application Group Management' is set to 'Success and Failure'	Yes	
17.2.2	Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only)	N/A	Applies to domain controllers only
17.2.3	Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only)	N/A	Applies to domain controllers only
17.2.4	Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only)	N/A	Applies to domain controllers only
17.2.5	Ensure 'Audit Security Group Management' is set to include 'Success'	Yes	
17.2.6	Ensure 'Audit User Account Management' is set to 'Success and Failure'	Yes	
17.3.1	Ensure 'Audit PNP Activity' is set to include 'Success'	Yes	
17.3.2	Ensure 'Audit Process Creation' is set to include 'Success'	Yes	
17.4.1	Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only)	N/A	Applies to domain controllers only

Reference ID	Description	Compliant	Notes
17.4.2	Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only)	N/A	Applies to domain controllers only
17.5.1	Ensure 'Audit Account Lockout' is set to include 'Failure'	Yes	
17.5.2	Ensure 'Audit Group Membership' is set to include 'Success'	Yes	
17.5.3	Ensure 'Audit Logoff' is set to include 'Success'	Yes	
17.5.4	Ensure 'Audit Logon' is set to 'Success and Failure'	Yes	
17.5.5	Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	Yes	
17.5.6	Ensure 'Audit Special Logon' is set to include 'Success'	Yes	
17.6.1	Ensure 'Audit Detailed File Share' is set to include 'Failure'	Yes	
17.6.2	Ensure 'Audit File Share' is set to 'Success and Failure'	Yes	
17.6.3	Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'	Yes	
17.6.4	Ensure 'Audit Removable Storage' is set to 'Success and Failure'	Yes	
17.7.1	Ensure 'Audit Policy Change' is set to include 'Success'	Yes	
17.7.2	Ensure 'Audit Authentication Policy Change' is set to include 'Success'	Yes	
17.7.3	Ensure 'Audit Authorization Policy Change' is set to include 'Success'	Yes	
17.7.4	Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'	Yes	
17.7.5	Ensure 'Audit Other Policy Change Events' is set to include 'Failure'	Yes	
17.8.1	Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	Yes	
17.9.1	Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	Yes	
17.9.2	Ensure 'Audit Other System Events' is set to 'Success and Failure'	Yes	
17.9.3	Ensure 'Audit Security State Change' is set to include 'Success'	Yes	
17.9.4	Ensure 'Audit Security System Extension' is set to include 'Success'	Yes	
17.9.5	Ensure 'Audit System Integrity' is set to 'Success and Failure'	Yes	
18.1.1.1	Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'	Yes	
18.1.1.2	Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'	Yes	
18.1.2.2	Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'	Yes	
18.1.3	Ensure 'Allow Online Tips' is set to 'Disabled'	Yes	

Reference ID	Description	Compliant	Notes
18.3.1	Ensure LAPS AdmPwd GPO Extension / CSE is installed	N/A	Cannot enforce via GPO
18.3.2	Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled'	Yes	
18.3.3	Ensure 'Enable Local Admin Password Management' is set to 'Enabled'	Yes	
18.3.4	Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters'	Yes	
18.3.5	Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more'	Yes	
18.3.6	Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer'	Yes	
18.4.1	Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'	No	Installation scripts require this
18.4.2	Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled'	No	Only available in Windows 10 22H2 and newer
18.4.3	Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver' (recommended)	Yes	
18.4.4	Ensure 'Configure SMB v1 server' is set to 'Disabled'	Yes	
18.4.5	Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'	Yes	
18.4.6	Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node' (recommended)	Yes	
18.4.7	Ensure 'WDigest Authentication' is set to 'Disabled'	Yes	
18.5.1	Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	Yes	
18.5.2	Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	Yes	
18.5.3	Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	Yes	
18.5.4	Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	Yes	
18.5.5 (Level 2)	Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)	Yes	
18.5.6	Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	Yes	

Reference ID	Description	Compliant	Notes
18.5.7 (Level 2)	Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled'	Yes	
18.5.8	Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'	Yes	
18.5.9	Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'	Yes	
18.5.10 (Level 2)	Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'	Yes	
18.5.11 (Level 2)	Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'	Yes	
18.5.12	Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	Yes	
18.6.4.1	Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks'	No	Only available in Windows 11 22H2 insider builds
18.6.4.2	Ensure 'Turn off multicast name resolution' is set to 'Enabled'	Yes	
18.6.5.1 (Level 2)	Ensure 'Enable Font Providers' is set to 'Disabled'	Yes	
18.6.8.1	Ensure 'Enable insecure guest logons' is set to 'Disabled'	Yes	
18.6.9.1 (Level 2)	Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'	Yes	
18.6.9.2 (Level 2)	Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'	Yes	
18.6.10.2 (Level 2)	Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled'	Yes	
18.6.11.2	Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	Yes	
18.6.11.3	Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'	Yes	
18.6.11.4	Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	Yes	
18.6.14.1	Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'	Yes	
18.6.19.2.1 (Level 2)	Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)')	No	Setting not available via GPO
18.6.20.1 (Level 2)	Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'	Yes	
18.6.20.2 (Level 2)	Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'	Yes	

Reference ID	Description	Compliant	Notes
18.6.21.1	Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 3 = Prevent Wi-Fi when on Ethernet'	Yes	
18.6.21.2 (Level 2)	Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled'	Yes	
18.7.1	Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'	Yes	
18.7.2	Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled'	Yes	
18.7.3	Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP'	No	Only available in Windows 11 22H2 and newer
18.7.4	Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default'	No	Only available in Windows 11 22H2 and newer
18.7.5	Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP'	No	Only available in Windows 11 22H2 and newer
18.7.6	Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections:' is set to 'Enabled: Negotiate' or higher	No	Only available in Windows 11 22H2 and newer
18.7.7	Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0'	No	Only available in Windows 11 22H2 and newer
18.7.8	Ensure 'Limits print driver installation to Administrators' is set to 'Enabled'	Yes	
18.7.9	Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles'	No	Only available in Windows 11 22H2 and newer
18.7.10	Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt'	Yes	
18.7.11	Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt'	Yes	
18.8.1.1 (Level 2)	Ensure 'Turn off notifications network usage' is set to 'Enabled'	Yes	
18.9.3.1	Ensure 'Include command line in process creation events' is set to 'Enabled'	Yes	
18.9.4.1	Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'	Yes	
18.9.4.2	Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'	Yes	

Reference ID	Description	Compliant	Notes
18.9.13.1	Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'	Yes	
18.9.19.2	Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	Yes	
18.9.19.3	Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	Yes	
18.9.19.4	Ensure 'Continue experiences on this device' is set to 'Disabled'	Yes	
18.9.19.5	Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'	Yes	
18.9.20.1.1	Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'	Yes	
18.8.20.1.2 (Level 2)	Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled'	Yes	
18.9.20.1.3 (Level 2)	Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled'	Yes	
18.9.20.1.4 (Level 2)	Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled'	Yes	
18.9.20.1.5	Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'	Yes	
18.9.20.1.6 (Level 2)	Ensure 'Turn off printing over HTTP' is set to 'Enabled'	Yes	
18.9.20.1.7 (Level 2)	Ensure 'Turn off Registration if URL connection is referring to Microsoft.com is set to 'Enabled'	Yes	
18.9.20.1.8 (Level 2)	Ensure 'Turn off Search Companion content file updates' is set to 'Enabled'	Yes	
18.9.20.1.9 (Level 2)	Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled'	Yes	
18.9.20.1.10 (Level 2)	Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled'	Yes	
18.9.20.1.11 (Level 2)	Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled'	Yes	
18.9.20.1.12 (Level 2)	Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'	Yes	
18.9.20.1.13 (Level 2)	Ensure 'Turn off Windows Error Reporting' is set to 'Enabled'	Yes	
18.9.23.1 (Level 2)	Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'	Yes	
18.9.24.1	Ensure 'Enumeration policy for external devices incompatible with Kernel DMA Protection' is set to 'Enabled: Block All'	Yes	
18.8.26.1 (Level 2)	Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled'	Yes	

Reference ID	Description	Compliant	Notes
18.8.27.1	Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'	Yes	
18.9.27.2	Ensure 'Do not display network selection UI' is set to 'Enabled'	Yes	
18.9.27.3	Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'	Yes	
18.9.27.4	Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled'	Yes	
18.9.27.5	Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'	Yes	
18.9.27.6	Ensure 'Turn off picture password sign-in' is set to 'Enabled'	Yes	
18.9.27.7	Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'	Yes	
18.9.30.1 (Level 2)	Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled'	Yes	
18.9.30.2 (Level 2)	Ensure 'Allow upload of User Activities' is set to 'Disabled'	Yes	
18.9.32.6.1 (Level 2)	Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'	Yes	
18.9.32.6.2 (Level 2)	Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'	Yes	
18.9.32.6.3	Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'	Yes	
18.9.32.6.4	Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'	Yes	
18.9.34.1	Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	Yes	
18.9.34.2	Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	Yes	
18.9.35.1	Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'	Yes	
18.9.35.2 (Level 2)	Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated'	Yes	
18.9.46.5.1 (Level 2)	Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled'	Yes	
18.9.46.11.1 (Level 2)	Ensure 'Enable/Disable PerfTrack' is set to 'Disabled'	Yes	
18.9.48.1 (Level 2)	Ensure 'Turn off the advertising ID' is set to 'Enabled'	Yes	
18.9.50.1.1 (Level 2)	Ensure 'Enable Windows NTP Client' is set to 'Enabled'	Yes	
18.9.50.1.2 (Level 2)	Ensure 'Enable Windows NTP Server' is set to 'Disabled'	Yes	

Reference ID	Description	Compliant	Notes
18.10.3.1 (Level 2)	Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'	Yes	
18.10.5.1	Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'	Yes	
18.10.7.1	Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	Yes	
18.10.7.2	Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	Yes	
18.10.7.3	Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	Yes	
18.10.8.1.1	Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled'	Yes	
18.10.10.1 (Level 2)	Ensure 'Allow Use of Camera' is set to 'Disabled'	Yes	
18.10.12.1	Ensure 'Turn off cloud consumer account state content' is set to 'Enabled'	No	Only available in Windows 11 22H2 and newer
18.10.12.2	Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'	Yes	
18.10.13.1	Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always'	Yes	
18.10.14.1	Ensure 'Do not display the password reveal button' is set to 'Enabled'	Yes	
18.10.14.2	Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'	Yes	
18.10.15.1	Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'	Yes	
18.10.15.2 (Level 2)	Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage'	Yes	
18.10.15.3	Ensure 'Disable OneSettings Downloads' is set to 'Enabled'	No	Only available in Windows 11 22H2 and newer
18.10.15.4	Ensure 'Do not show feedback notifications' is set to 'Enabled'	Yes	
18.10.15.5	Ensure 'Enable OneSettings Auditing' is set to 'Enabled'	No	Only available in Windows 11 22H2 and newer
18.10.15.6	Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled'	No	Only available in Windows 11 22H2 and newer
18.10.15.7	Ensure 'Limit Dump Collection' is set to 'Enabled'	No	Only available in Windows 11 22H2 and newer
18.10.15.8	Ensure 'Toggle user control over Insider builds' is set to 'Disabled'	Yes	

Reference ID	Description	Compliant	Notes
18.10.17.1	Ensure 'Enable App Installer' is set to 'Disabled'	No	Only available in Windows 11 22H2 and newer
18.10.17.2	Ensure 'Enable App Installer Experimental Features' is set to 'Disabled'	No	Only available in Windows 11 22H2 and newer
18.10.17.3	Ensure 'Enable App Installer Hash Override' is set to 'Disabled'	No	Only available in Windows 11 22H2 and newer
18.10.17.4	Ensure 'Enable App Installer ms-appinstaller protocol' is set to 'Disabled'	No	Only available in Windows 11 22H2 and newer
18.10.26.1.1	Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	Yes	
18.10.26.1.2	Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	Yes	
18.10.26.2.1	Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	Yes	
18.10.26.2.2	Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	Yes	
18.10.26.3.1	Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	Yes	
18.10.26.3.2	Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	Yes	
18.10.26.4.1	Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	Yes	
18.10.26.4.2	Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	Yes	
18.10.29.2	Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'	Yes	
18.10.29.3	Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	Yes	
18.10.29.4	Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	Yes	
18.10.37.1 (Level 2)	Ensure 'Turn off location' is set to 'Enabled'	Yes	
18.10.41.1 (Level 2)	Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled'	Yes	
18.10.42.1	Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled'	Yes	
18.10.43.5.1	Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled'	Yes	
18.10.43.5.2	Ensure 'Join Microsoft MAPS' is set to 'Disabled'	Yes	

Reference ID	Description	Compliant	Notes
18.10.43.6.1.1	Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'	Yes	
18.10.43.6.1.2	Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured	Yes	
18.10.43.6.3.1	Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'	Yes	
18.10.43.7.1 (Level 2)	Ensure 'Enable file hash computation feature' is set to 'Enabled'	No	Only available in Windows 10 release 2004 and newer
18.10.43.10.1	Ensure 'Scan all downloaded files and attachments' is set to 'Enabled'	Yes	
18.10.43.10.2	Ensure 'Turn off real-time protection' is set to 'Disabled'	Yes	
18.10.43.10.3	Ensure 'Turn on behavior monitoring' is set to 'Enabled'	Yes	
18.10.43.10.4	Ensure 'Turn on script scanning' is set to 'Enabled'	No	Only available in Windows 11 22H2 and newer
18.10.43.12.1	Ensure 'Configure Watson events' is set to 'Disabled'	Yes	
18.10.43.13.1	Ensure 'Scan removable drives' is set to 'Enabled'	Yes	
18.10.43.13.2	Ensure 'Turn on e-mail scanning' is set to 'Enabled'	Yes	
18.10.43.16	Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block'	Yes	
18.10.43.17	Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled'	Yes	
18.10.51.1	Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'	Yes	
18.10.56.1 (Level 2)	Ensure 'Turn off Push To Install service' is set to 'Enabled'	Yes	
18.10.57.2.2	Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	Yes	
18.10.57.3.2.1 (Level 2)	Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled'	Yes	
18.10.57.3.3.1 (Level 2)	Ensure 'Do not allow COM port redirection' is set to 'Enabled'	Yes	
18.10.57.3.3.2	Ensure 'Do not allow drive redirection' is set to 'Enabled'	Yes	
18.10.57.3.3.3 (Level 2)	Ensure 'Do not allow LPT port redirection' is set to 'Enabled'	Yes	
18.10.57.3.3.4 (Level 2)	Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled'	Yes	
18.10.57.3.9.1	Ensure 'Always prompt for password upon connection' is set to 'Enabled'	Yes	
18.10.57.3.9.2	Ensure 'Require secure RPC communication' is set to 'Enabled'	Yes	

Reference ID	Description	Compliant	Notes
18.10.57.3.9.3	Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'	Yes	
18.10.57.3.9.4	Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled'	Yes	
18.10.57.3.9.5	Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'	Yes	
18.10.57.3.10.1 (Level 2)	Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less, but not Never (0)'	No	Needed for installation
18.10.57.3.10.2 (Level 2)	Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'	No	Required in some scenarios
18.10.57.3.11.1	Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	Yes	
18.10.57.3.11.2	Ensure 'Do not use temporary folders per session' is set to 'Disabled'	Yes	
18.10.58.1	Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	Yes	
18.10.59.2 (Level 2)	Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search'	Yes	Set to Disabled
18.10.59.3	Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	Yes	
18.10.59.4	Ensure 'Allow search highlights' is set to 'Disabled'	No	Only available in Windows 10 21H2 and newer
18.10.63.1 (Level 2)	Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled'	Yes	
18.10.76.2.1	Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'	Yes	
18.10.80.1 (Level 2)	Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled'	Yes	
18.10.80.2	Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled'	Yes	
18.10.81.1	Ensure 'Allow user control over installs' is set to 'Disabled'	Yes	
18.10.81.2	Ensure 'Always install with elevated privileges' is set to 'Disabled'	Yes	
18.10.81.3 (Level 2)	Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled'	Yes	
18.10.82.1	Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled'	Yes	
18.10.87.1	Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled'	Yes	
18.10.87.2	Ensure 'Turn on PowerShell Transcription' is set to 'Enabled'	Yes	
18.10.89.1.1	Ensure 'Allow Basic authentication' is set to 'Disabled'	Yes	
18.10.89.1.2	Ensure 'Allow unencrypted traffic' is set to 'Disabled'	Yes	

Reference ID	Description	Compliant	Notes
18.10.89.1.3	Ensure 'Disallow Digest authentication' is set to 'Enabled'	Yes	
18.10.89.2.1	Ensure 'Allow Basic authentication' is set to 'Disabled'	No	Installation scripts require this
18.10.89.2.2 (Level 2)	Ensure 'Allow remote server management through WinRM' is set to 'Disabled'	No	Installation scripts require this
18.10.89.2.3	Ensure 'Allow unencrypted traffic' is set to 'Disabled'	No	Installation scripts require this
18.10.89.2.4	Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'	Yes	
18.10.90.1 (Level 2)	Ensure 'Allow Remote Shell Access' is set to 'Disabled'	No	Installation scripts require this
18.10.92.2.1	Ensure 'Prevent users from modifying settings' is set to 'Enabled'	Yes	
18.10.93.1.1	Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	Yes	
18.10.93.2.1	Ensure 'Configure Automatic Updates' is set to 'Enabled'	No	Unapproved updates may create issues
18.10.93.2.2	Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	No	Unapproved updates may create issues
18.10.93.4.1	Ensure 'Manage preview builds' is set to 'Disabled'	Yes	
18.10.93.4.2	Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days'	Yes	
18.10.93.4.3	Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'	Yes	
19.1.3.1	Ensure 'Enable screen saver' is set to 'Enabled'	Yes	
19.1.3.2	Ensure 'Password protect the screen saver' is set to 'Enabled'	Yes	
19.1.3.3	Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0'	Yes	
19.5.1.1	Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'	Yes	
19.6.6.1.1 (Level 2)	Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled'	Yes	
19.7.4.1	Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'	Yes	
19.7.4.2	Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'	Yes	
19.7.7.1	Ensure 'Configure Windows spotlight on lock screen' is set to Disabled'	Yes	
19.7.7.2	Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'	Yes	

Reference ID	Description	Compliant	Notes
19.7.7.3 (Level 2)	Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled'	Yes	
19.7.7.4 (Level 2)	Ensure 'Turn off all Windows spotlight features' is set to 'Enabled'	Yes	
19.7.7.5	Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled'	No	Only available in Windows 11 22H2 and newer
19.7.25.1	Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'	Yes	
19.7.40.1	Ensure 'Always install with elevated privileges' is set to 'Disabled'	Yes	
19.7.42.2.1 (Level 2)	Ensure 'Prevent Codec Download' is set to 'Enabled'	Yes	

Appendix D: User roles and permissions

Table 1: Service roles

Role	Description
DM_SERVICE_ELECTRIC	This role allows user access to the Manage Electric application. It controls the display of the Manage Electric icon under Device Management on the Launch Pad.
DM_SERVICE_GAS	This role allows user access to the Manage Gas application. It controls the display of the Manage Gas icon under Device Management on the Launch Pad.
DM_SERVICE_WATER	This role allows user access to the Manage Water application. It controls the display of the Manage Water icon under Device Management on the Launch Pad.
SERVICE_BATCH_VIEWER	Enables access to the Batch Job Viewer (available to internal Sensus personnel only).
SERVICE_CATHODIC	This role allows user access to the Cathodic Protection application (SentryPoint). It controls the display of the SentryPoint icon under Solution Applications on the Launch Pad.
SERVICE_CONFIG_DL	This role allows user access to the Configuration Download application. It controls the display of the Configuration Download icon on the Launch Pad.
SERVICE_FWDL	Enables access to the Firmware Download icon on the Launch Pad.
SERVICE_NETWORK_METRICS	This role enables user access to the Network Metrics application. It controls the display of the Network Metrics icon under RF Network Management on the Launch Pad. This role should be coupled with one of the other Network Metrics roles for specific access levels within Network Metrics.

Role	Description
SERVICE_NMS	This role allows user access to the Network Management System application. It controls the display of the Network Management icon under RF Network Management on the Launch Pad.
SERVICE_REPORT_GEN	Enables access to Report Generator. Must be set to access the Report Generator application.
SERVICE_SCHEDULER	This role allows user access to the RNI Scheduler application. It controls the display of the RNI Scheduler icon under RNI Management on the Launch Pad.
SERVICE_SYSTEM_ADMIN	Enables access to the System Administration application under RNI Management on the Launch Pad. This role must be paired with a functional role assignment, such as DM_SERVICE_WATER, which enables the user to view the Manage Water icon on the Launch Pad. This enables an Admin user to have administrative level access to that functional role.
SERVICE_TOU_CONFIG	This role allows user access to the TOU Configurator application. It controls the display of the TOU Configurator icon under Download Configuration on the Launch Pad.

Table 2: Functional roles

Role	Permissions
DM_ADMIN	
	View/export device list and device detail
	View system-wide data: Alerts tab, reports
	View device firmware download job status
	View system-wide settings
	Modify radio configuration over-the-air
	Modify sensor configuration over-the-air
	Initiate demand response events
	Initiate demand reset events
	Initiate service switch operations
	Initiate end point pings
	Initiate device import
	Initiate device firmware download
	Edit system-wide behavior parameters
	Clear alarms, configure smart alarms
	Modify HAN devices and FlexNet LCM relays
	Add/edit/delete Base Station records

Role	Permissions
DM_ADMIN (continued)	Modify device lifecycle state
	Modify device operational mode
	Enable/disable/suspend device encryption
	Create/edit groups and tags
	Manage MultiSpeak dynamic registration
	Create/edit user information within a tenant
	Modify DB attributes of a device
	Manage job execution and lifecycle in scheduler
	Can add a new meter into the RNI
	Can start usage monitoring for a meter
	Can arm a meter for connect
	Be able to do Billing Ping
	Has the ability to clear meter alarms
	Has the ability to configure and cancel load limit
	Can delete a meter from the RNI
	Can stop usage monitoring for a meter
	Has the ability to perform a Demand Reset
	Has the ability to cancel a Demand Reset
	Has the ability to disconnect power for the meter
	Has permission to setup, initiate and cancel Demand Response events
	Has the ability to manage dynamic registration
	Can get a meter record from the RNI
	Can get meter readings from the RNI
	Can get system configurations for the RNI
	Has permission to join, leave and commission HAN devices
	Has permission to create and delete HAN devices
	Has permission to send and cancel display messages to HAN devices
	Has the ability to configure Meters
	Has the ability to change a meter's lifecycle information
	Has the ability to reconnect power for the meter
	Can ping (on-air message) a meter for status
	Has the ability to set remote shutoff valve to trickle

Role	Permissions
	Can update an existing meter in the RNI
	Create/edit group types
	Configure reading units and resolution
	Access experimental features
	Key management, generate encryption files
	Can enable/disable and configure shutoff alarms
	Can shutoff valve
	Can control the display of sub 1hr MSR
	ROLE_AUTH_MANAGE_CB_CLIENT
DM_SYSTEM_OPERATOR	
	View/export device list and device detail
	View system-wide data: Alerts tab, reports
	View device firmware download job status
	View system-wide settings
	Modify radio configuration over-the-air
	Modify sensor configuration over-the-air
	Initiate demand response events
	Initiate demand reset events
	Initiate service switch operations
	Initiate end point pings
	Initiate device import
	Initiate device firmware download
	Clear alarms, configure smart alarms
	Modify HAN devices and FlexNet LCM relays
	Add/edit/delete Base Station records
	Modify device lifecycle state
	Modify device operational mode
	Enable/disable/suspend device encryption
	Create/edit groups and tags
	Manage MultiSpeak dynamic registration
	Create/edit user information within a tenant
	Modify DB attributes of a device

Role	Permissions
DM_SYSTEM_OPERATOR (continued)	Manage job execution and lifecycle in scheduler
	Can add a new meter into the RNI
	Can start usage monitoring for a meter
	Can arm a meter for connect
	Be able to do Billing Ping
	Has the ability to clear meter alarms
	Has the ability to configure and cancel load limit
	Can delete a meter from the RNI
	Can stop usage monitoring for a meter
	Has the ability to perform a Demand Reset
	Has the ability to cancel a Demand Reset
	Has the ability to disconnect power for the meter
	Has permission to setup, initiate and cancel Demand Response events
	Has the ability to manage dynamic registration
	Can get a meter record from the RNI
	Can get meter readings from the RNI
	Can get system configurations for the RNI
	Has permission to join, leave and commission HAN devices
	Has permission to create and delete HAN devices
	Has permission to send and cancel display messages to HAN devices
	Has the ability to configure Meters
	Has the ability to change a meter's lifecycle information
	Has the ability to reconnect power for the meter
	Can ping (on-air message) a meter for status
	Has the ability to set remote shutoff valve to trickle
	Can update an existing meter in the RNI
	Create/ Edit group types
	Can configure Reading Units and Resolution
	Access experimental features
	Key management, generate encryption files
	Can enable/disable and configure shutoff alarms

Role	Permissions
DM_SYSTEM_OPERATOR (continued)	Can shutoff valve
	Can control the display of sub 1hr MSR
DM_CUSTOMER_SUPPORT	
	View/export device list and device detail
	View system-wide data: Alerts tab, reports
	Create/ Edit groups and tags
DM_BILLING_MANAGER	
	View/export device list and device detail
	View system-wide data: Alerts tab, reports
	Create/ Edit groups and tags
FWDL	
	Ability to perform firmware download. This role is used in conjunction with the SERVICE_FWDL role to perform firmware downloads in the Firmware Download (FWDL) application on the Launch Pad. This application manages NA2W FWDL and Electric FWDL.
FWDL_ADMIN	
	View device firmware download job status
	Initiate device firmware download
FWDL_VIEWER	
	View device firmware download job status
SYSTEM_ADMIN	
	Edit system-wide behavior parameters
	Create/edit user information within a tenant
	Create/edit tenants and tenant user admins
	Key management, generate encryption files
	Can manage the maximum number of devices that can be included in an action
	ROLE_AUTH_MANAGE_CB_CLIENT
USER_ADMIN	
	Create/edit user information within a tenant
NMS_ADMIN	
	Access administrative functions within Network Management System

Role	Permissions
NMS_USER	
	Access user only functions within Network Management System
GATEWAY	
	Modify Sensor configuration Over-The-Air
	Modify device operational mode
	Create/ Edit groups and tags
	Modify DB attributes of a device
	Can add a new meter into the RNI
	Can start usage monitoring for a meter
	Can arm a meter for connect
	Be able to do Billing Ping
	Has the ability to clear meter alarms
	Has the ability to configure and cancel load limit
	Can delete a meter from the RNI
	Can stop usage monitoring for a meter
	Has the ability to perform a Demand Reset
	Has the ability to cancel a Demand Reset
	Has the ability to disconnect power for the meter
	Has permission to setup, initiate and cancel Demand Response events
	Has the ability to manage dynamic registration
	Can get a meter record from the RNI
	Can get meter readings from the RNI
	Can get system configurations for the RNI
	Has permission to join, leave and commission HAN devices
	Has permission to create and delete HAN devices
	Has permission to send and cancel display messages to HAN devices
	Has the ability to configure Meters
	Has the ability to change a meter's lifecycle information
	Has the ability to reconnect power for the meter
	Can ping (on-air message) a meter for status
	Has the ability to set remote shutoff valve to trickle
	Can update an existing meter in the RNI
	Can enable/disable and configure shutoff alarms

Role	Permissions
GATEWAY (continued)	Can shutoff valve
	ROLE_AUTH_MANAGE_CB_CLIENT
	Can manage broadcast groups
	Can view broadcast group information
Notif_Subscription_Management	
	Perform subscription notify management. This authenticates the MultiSpeak and RNI API to access the Notifications service (for example, Subscribe, Unsubscribe).
SCHEDULE_VIEWER	
	Enables access to the Scheduler application with view-only permissions. A user can view the scheduled jobs, but not create, update, or delete any scheduled jobs.
SCHEDULE_ADMIN	
	Create, edit, and view Scheduler jobs. Enables access to the Scheduler application. Membership in this role confirms Admin status and conditionally enables actions in the application. Scheduler is an advanced application that enables an Administrator to schedule autonomous actions (for example, Scheduled Reports).
SCS_PROXY_USER	
	Required for any user to access the SCS (Proxy) application
CATHODIC_ADMIN	
	Create/edit group types
CATHODIC_USER	
	Access Cathodic User functions
CATHODIC_VIEWER	
	View-only access for Cathodic Protection application
PERFORM_CONFIG_DL	
	Meter Configuration Download Administrator. Enables the user to perform configuration download.
PERFORM_TOU_CONFIG	
	Access to the TOU (Time of Use) Configurator application for Electric Device Manager
TENANT_ADMIN	
	View/export device list and device detail
	View system-wide data: Alerts tab, reports
	View device firmware download job status

Role	Permissions
TENANT_ADMIN (continued)	View system-wide settings
	Modify radio configuration Over-The-Air
	Modify Sensor configuration Over-The-Air
	Initiate Demand Response events
	Initiate Demand Reset events
	Initiate Service Switch operations
	Initiate endpoint Pings
	Initiate device import
	Initiate device firmware download
	Edit system-wide behavior parameters
	Clear alarms, configure smart alarms
	Modify HAN devices and FlexNet LCM relays
	Add/Edit/Delete Base Station records
	Modify device life cycle state
	Modify device Operational Mode
	Enable/Disable/Suspend Device Encryption
	Create/ Edit groups and tags
	Manage MultiSpeak dynamic registration
	Create/edit user information within a tenant
	Modify DB attributes of a device
	Manage job execution & lifecycle in scheduler
	Can add a new meter into the RNI
	Can start usage monitoring for a meter
	Can arm a meter for connect
	Be able to do Billing Ping
	Has the ability to clear meter alarms
	Has the ability to configure and cancel load limit
	Can delete a meter from the RNI
	Can stop usage monitoring for a meter
	Has the ability to perform a Demand Reset
	Has the ability to cancel a Demand Reset
	Has the ability to disconnect power for the meter

Role	Permissions
TENANT_ADMIN (continued)	Has permission to setup, initiate and cancel Demand Response events
	Has the ability to manage dynamic registration
	Can get a meter record from the RNI
	Can get meter readings from the RNI
	Can get system configurations for the RNI
	Has permission to join, leave and commission HAN devices
	Has permission to create and delete HAN devices
	Has permission to send and cancel display messages to HAN devices
	Has the ability to configure Meters
	Has the ability to change a meter's lifecycle information
	Has the ability to reconnect power for the meter
	Can ping (on-air message) a meter for status
	Has the ability to set remote shutoff valve to trickle
	Can update an existing meter in the RNI
	Create/ Edit group types
	Can configure Reading Units and Resolution
	Access experimental features
	Key management, generate encryption files
	Can enable/disable and configure shutoff alarms
	Can shutoff valve
	Can manage the maximum number of devices that can be included in an action
	Can control the display of sub 1hr MSR
	ROLE_AUTH_MANAGE_CB_CLIENT

Xylem |'zīləm|

1) The tissue in plants that brings water upward from the roots;

2) a leading global water technology company.

We're a global team unified in a common purpose: creating advanced technology solutions to the world's water challenges. Developing new technologies that will improve the way water is used, conserved, and re-used in the future is central to our work. Our products and services move, treat, analyze, monitor and return water to the environment, in public utility, industrial, residential and commercial building services settings. Xylem also provides a leading portfolio of smart metering, network technologies and advanced analytics solutions for water, electric and gas utilities. In more than 150 countries, we have strong, long-standing relationships with customers who know us for our powerful combination of leading product brands and applications expertise with a strong focus on developing comprehensive, sustainable solutions.

For more information on how Xylem can help you, go to www.xylem.com

xylem

Sensus
637 Davis Drive
Morrisville, NC 27560
Tel +1.800.638.3748
www.sensus.com