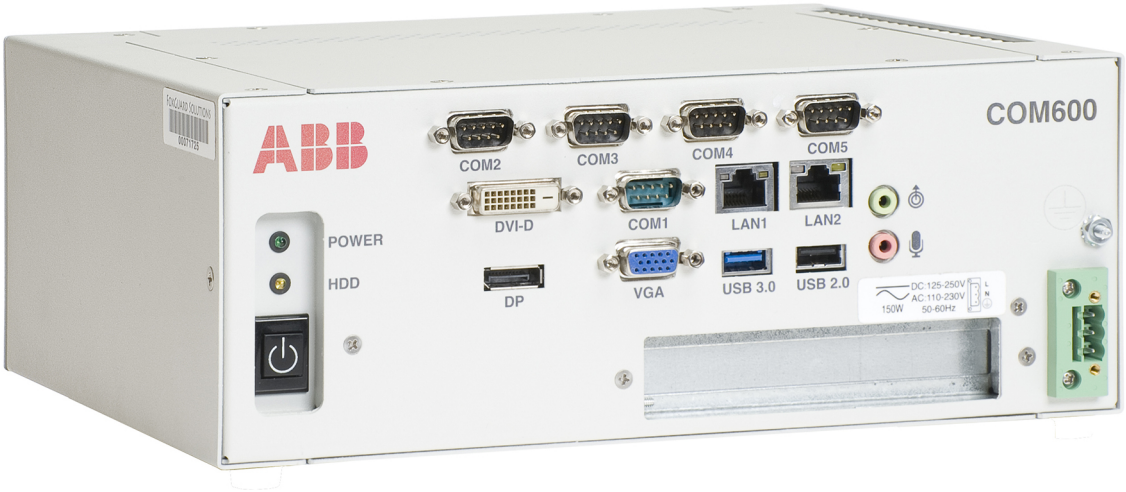
COM600 series 5.1

Cyber Security Deployment Guideline



Contents:

1. About this manual

1.1. Copyright

Warranty

Please inquire about the terms of warranty from your nearest ABB representative.

http://www.abb.com/substationautomation

1.2. Disclaimer

The data, examples and diagrams in this manual are included solely for the concept or product description and are not to be deemed as a statement of guaranteed properties. All persons responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including that any applicable safety or other operational requirements are complied with. In particular, any risks in applications where a system failure and/ or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

This product is designed to be connected and to communicate information and data via a network interface, which should be connected to a secure network. It is sole responsibility of person or entity responsible for network administration to ensure a secure connection to the network and to establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti virus programs, etc) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB is not liable for damages and/or losses related to such security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

This document has been carefully checked by ABB but deviations cannot be completely ruled out. In case any errors are detected, the reader is kindly requested to notify the manufacturer. Other than under explicit contractual commitments, in no event shall ABB

be responsible or liable for any loss or damage resulting from the use of this manual or the application of the equipment.

1.3. Conformity

This product complies with the directive of the Council of the European Communities on the approximation of the laws of the Member States relating to electromagnetic compatibility (EMC Directive 2004/108/EC) and concerning electrical equipment for use within specified voltage limits (Low-voltage directive 2006/95/EC). This conformity is the result of tests conducted by ABB in accordance with the product standards EN 50263 and EN 60255-26 for the EMC directive, and with the product standards EN 60255-1 and EN 60255-27 for the low voltage directive. The product is designed in accordance with the international standards of the IEC 60255 series.

1.4. Trademarks

ABB is a registered trademark of ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

1.5. Document conventions

The following conventions are used for the presentation of material:

- The words in names of screen elements (for example, the title in the title bar of a window, the label for a field of a dialog box) are initially capitalized.
- Capital letters are used for the name of a keyboard key if it is labeled on the keyboard. For example, press the ENTER key.
- Lowercase letters are used for the name of a keyboard key that is not labeled on the keyboard. For example, the space bar, comma key, and so on.
- Press CTRL+C indicates that you must hold down the CTRL key while pressing the C key (to copy a selected object in this case).
- Press ESC E C indicates that you press and release each key in sequence (to copy a selected object in this case).
- The names of push and toggle buttons are boldfaced. For example, click **OK**.
- The names of menus and menu items are boldfaced. For example, the **File** menu.
  - The following convention is used for menu operations: **MenuName > MenuItem > CascadedMenuItem**. For example: select **File > New > Type**.
  - The **Start** menu name always refers to the **Start** menu on the Windows taskbar.
- System prompts/messages and user responses/input are shown in the Courier font. For example, if you enter a value out of range, the following message is displayed:

```
Entered value is not valid. The value must be 0 - 30  .
```

- You can be asked to enter the string MIF349 in a field. The string is shown as follows in the procedure:

  MIF349
- Variables are shown using lowercase letters:

  sequence name

1.6. Use of symbols

This publication includes warning, caution, and information icons that point out safety-related conditions or other important information. It also includes tip icons to point out useful information to the reader. The corresponding icons should be interpreted as follows.

The electrical warning icon indicates the presence of a hazard which could result in electrical shock.

The warning icon indicates the presence of a hazard which could result in personal injury.

The caution icon indicates important information or warning related to the concept discussed in the text. It may indicate the presence of a hazard which could result in corruption of software or damage to equipment or property.

The information icon alerts the reader to relevant facts and conditions.

The tip icon indicates advice on, for example, how to design your project or how to use a certain function.

1.7. Terminology

The following is a list of terms associated with that you should be familiar with. The list contains terms that are unique to ABB or have a usage or definition that is different from standard industry usage.

Term	Description
Alarm	An abnormal state of a condition.

Term	Description
Alarms and Events; AE	An OPC service for providing information about alarms and events to OPC clients.
Device	A physical device that behaves as its own communication node in the network, for example, protection relay.
Event	Change of process data or an OPC internal value. Normally, an event consists of value, quality, and timestamp.
Intelligent Electronic Device	A physical IEC 61850 device that behaves as its own communication node in the IEC 61850 protocol.
OPC	Series of standards specifications aiming at open connectivity in industrial automation and the enterprise systems that support industry.
Property	Named data item.

1.8. Abbreviations

The following is a list of abbreviations associated with COM600 that you should be familiar with. See also 1.7, Terminology.

Abbreviation	Description
DCOM	Distributed Component Object Model
DEP	Data Execution Prevention
GAT	GOOSE Analyzer Tool
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
MMS	Manufacturing Message Specification
NCC	Network Control Center
OS	Operating System
RCC	Regional Control Centre
SEV	Security Event
SNTP	Simple Network Time Protocol
WSUS	Windows Server Update Services

1.9. Related documents

Name of the manual	MRS number
CAL and SEV OPC Server User’s Manual	1MRS201326
COM600 Operator’s Manual	1MRS756705
SNTP OPC Server User’s Manual	1MRS757277

1.10. Document revisions

Document version/date	Product revision	History
A/13.3.2015	4.1	Document created
B/24.5.2017	5.0	Document revised
C/16.4.2018	5.1	Document revised

2. Introduction

2.1. General information about the COM600 series

The COM600 product series are versatile Substation Management Units that help realize smart substation and grid automation solutions in industrial and utility distribution networks.

They get deployed together with protection and control IEDs, substation devices such as RTUs, meters and PLCs in dedicated cabinets and switchgear.

The COM600 product is an all-in-one unit that functions as:
- Communication gateway
- Web Human Machine Interface (WebHMI)
- Automation controller
- Real-time and historical data management unit

The COM600 product series use process information and device data, acquired over Ethernet or serial communication protocol interfaces to execute specific substation functions and applications. Thus, they are critical building blocks to realize substation secondary system solutions and in the process solving diverse customer needs.

2.2. COM600 product series variants and rationale

To facilitate substation and grid automation solutions in IEC and ANSI market areas, a variant-based system similar to Relion® 615 and 620 series is being followed from COM600 5.0 release.

The main reasons for such an approach are the following:

- To ensure all COM600 product series features are advantageously used in end-customer projects in the medium voltage substation automation domain.
- To ensure an optimum feature set to be bundled together to realize specific applications required in IEC and ANSI market areas.
- To ensure a future-proof product approach.

This release then comprises of two variants, based on the primary intent or application are defined as follows:
- COM600S IEC – COM600 for substation automation, analysis and data management (for IEC markets)
  - COM600S IEC is a substation automation, analyzer and data management unit that integrates devices, facilitates operations, manages communication and runs analysis applications pertinent to equipment or operations in utility or industrial distribution substations.
- COM600F ANSI – COM600 as distribution automation controller (for ANSI markets)

- COM600F is a dedicated distribution automation controller unit that runs distributed grid and feeder applications for ANSI power networks and inherits all core features of the COM600 series.

2.3. Overview

This document outlines key information needed to secure and harden COM600 when commissioned in a substation. This document is intended for system administrators, network security personnel and automation engineers/experts, involved in commissioning a COM600 in a substation or in an industrial environment. The reader is expected to have general familiarity with:

- PCs, servers, and Windows operating system
- networking including TCP/IP and the concepts of ports and services
- Windows Audit policies
- firewalls
- anti-virus
- remote and secure communication
- Windows updates.

The COM600 commissioned within a substation communicates with downstream and upstream devices for its functioning. The downstream devices represent devices that are local to substation typically located along with COM600, and include devices like protection relays, RTUs and Remote I/O units. The upstream devices represent devices that are remote to substation and not physically present in the same location with COM600. The upstream devices include devices like SCADA servers and WSUS servers located at the Network Control Center/ Utility Control Center. Figure 2.3-1 shows a typical network setup when using COM600.

These downstream and upstream devices can be connected to COM600 through two different LANs, allowing a further separation/isolation of resources. COM600 has two Ethernet adapters which are pre-configured, to be identified as Local and Remote Ethernet adapters. Through Local Ethernet adapter in COM600, downstream devices can be connected to it through a Local LAN and through Remote adapter in COM600, upstream devices can be connected to it through a Remote LAN. Also different firewall policy can be enforced for each of the LANs, allowing more stringent connection rules to entities outside of the substation.

Windows Server Update Services (WSUS) is an infrastructure that allows software updates from Microsoft to be distributed to COM600. These updates include OS related critical/security patches for COM600. Typical WSUS would include at a minimum one Windows 2012 server machine capable of connecting to Microsoft Update Server through Internet. It is important to isolate the WSUS server from other network resources through multiple LANs and firewall rules. The WSUS server should be managed by a System administrator who approves/rejects, available updates for installation. After approval, the update installation process in COM600 can be configured to proceed automatically.

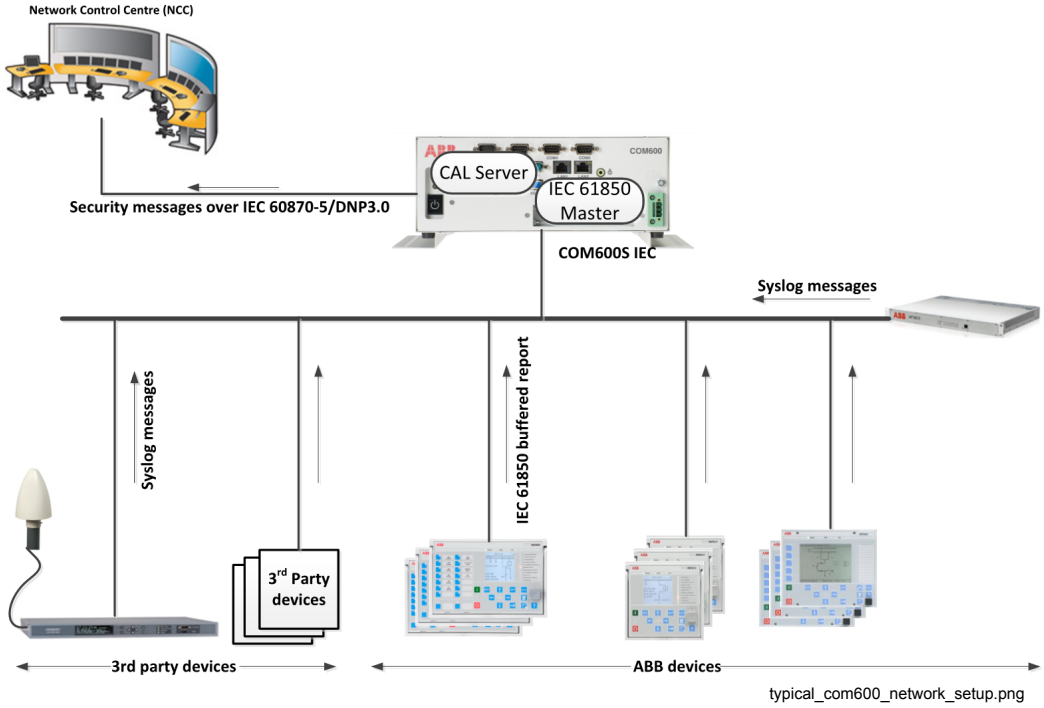


Figure 2.3-1 Typical COM600 network setup

3. Security Guidelines

3.1. Access Control

3.1.1. Access Control

This section describes system hardening measures that can be taken to limit access to various components in COM600 only for users with predefined permissions/access rights.

3.1.2. BIOS access

The BIOS in COM600 loads the operating system during boot time from hard drive and initializes various primary hardware units connected to COM600, such as keyboards, monitors and network adapters. The configuration in BIOS should be limited to users with administrative rights and should be protected from any unauthorized changes through passwords.

By default COM600 has no passwords that restrict changes to settings in BIOS. Therefore it is important to configure Administrator password in BIOS against any unauthorized access.

To assign a password for administrative use in COM600 BIOS:
1. Attach a keyboard/mouse to the blue USB adapter on COM600.
2. Power on COM600.
3. Press **DEL** key in keyboard to enter BIOS immediately.
4. Browse to Security tab in BIOS.
5. Go to **Administrator password** to create a new password.

Using a user password implies a power on password behavior where a valid user/administrator password should be entered manually each time on boot, before BIOS can load the operating system and COM600 applications. Therefore, it is recommended not to assign a aser password, since it may affect the availability of COM600 during restart, requiring a manual intervention.

3.1.3. User Accounts

COM600 user account

Many of the COM600 functionality specific software applications are set up to execute with COM600 user account credentials. This user account has administrative privileges and its password should be changed from default value before use. Aways use **Change Password** option available from Gateway Management Tool in SAB600 when changing

a password for COM600 user account. See Appendix 1 for details on how to launch Gateway Management Tool.

Administrator user account

The default Administrator user account available from Windows operating system is disabled in COM600 device. This account is not required for COM600 functioning and can be left disabled. If this account is enabled for other reasons, it is recommended to assign a password that meets all complexity requirements as defined by the password security policy.

3.1.4. User groups

COM600 user accounts can be classified into four user groups based on the actions that they can be allowed to perform. These four user groups include **COM600-Viewer**, **COM600-Operator**, **COM600-Engineer** and **COM600-Administrator**. These user groups are available in COM600 by default. When creating a new user account in COM600, assign it to any of these COM600 user groups.

Based on the user group assigned for a particular user account, a customized user interface is provided by COM600 WebHMI that limits/allows a specific function/operation.

The user accounts can be grouped and managed either using COM600 WebHMI or using typical Windows User Account Management.

Refer to User Management section in COM600 Operator's Manual for detailed information on access permissions to various COM600 interfaces available for these user groups. The table below shows a summary of access permissions for these user groups.

User Group name	Access permission summary
COM600-Viewer	Only allowed to view.
COM600-Operator	Authorized to make control operations.
COM600-Engineer	Authorized to make parameter setting changes, but limited from control operations.
COM600-Administrator	Full access.

3.1.5. Local security policy

Security related settings in Windows operating system can be managed through security policies. These operating system wide security policies provide a comprehensive set of configuration that can be performed to allow/disallow a particular behavior by a specific user/user group. Security policies defined within COM600 can be viewed/edited through Local Security Policy Editor.

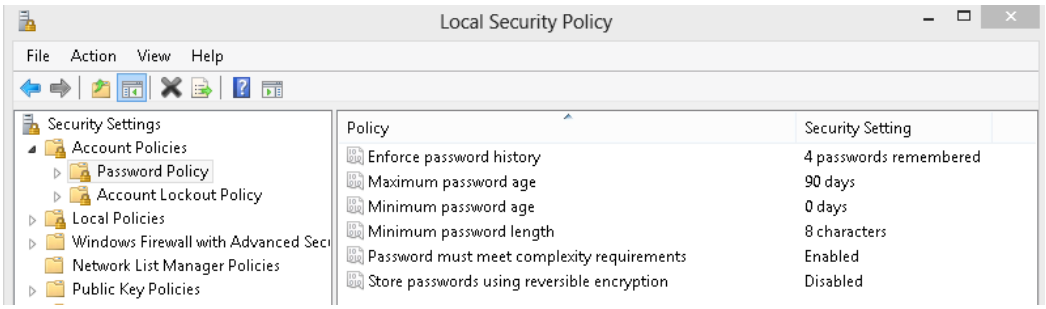
To launch Local security policy editor:
1. Login to COM600 as administrator.
2. Go to **Control Panel**.
3. Click **Administrative tools**.
4. Click **Local Security Policy**. Local security policy editor opens.
5. Browse through each of the policies and make appropriate settings to align with the desired security behavior.

In addition to local security policies, there are domain security policies which become applicable when COM600 is added to a domain. Domain level security policies reflect the same set of local security policies, except that they are defined for a common group of devices managed centrally through a domain controller. Domain security policies are typically managed by a domain level system administrator. It is important to note that whenever COM600 is added to a domain, the settings made for security policies at domain level always override the settings made to local security policies.

Security policies related to passwords and account lockout behavior are configured by default and only reflect the minimum configuration that can be done at factory. It is recommended to configure all applicable security policies, which may better align with specific security needs for the environment in which COM600 is commissioned.

Password policy

Figure 3.1.5-1 shows the default settings for Password security policy.

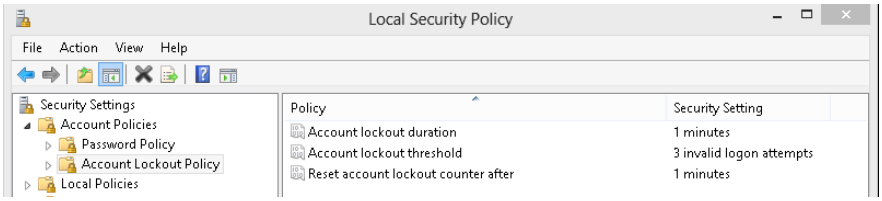


preconfigured_password_policy.png

Figure 3.1.5-1 Preconfigured password policy

Account Lockout policy

Figure 3.1.5-2 shows the default setting for Account Lockout security policy.



preconfigured_account_lockout_policy.png

Figure 3.1.5-2 Preconfigured account lockout policy

3.2. Ports and services

3.2.1. Ports and services

COM600 has two built-in Network Interface Cards (NIC) and an additional extension LAN card (with two more NICs) which can be added through an order code when ordering. The two built-in NICs are referred to as LOCAL and REMOTE adapters in Windows network adapter configuration. These two NICs allow network connections to two different networks.

The Internet Protocol (IP) communications in COM600 rely on two parameters: IP Address and Ports. An NIC in COM600 represents a physical end point to the network (LAN/WAN), to which it is connected. Typically during commissioning, a network administrator assigns an IP address to each of the NICs associated with COM600.

By default, the LOCAL NIC is assigned an IP address of 192.168.2.11 and the REMOTE NIC is assigned an IP address of 10.0.0.11. The NICs in additional extension LAN card are not configured. During commissioning we recommend to change these IP addresses.

3.2.2. Ports

Ports are used in IP communications along with IP address. Ports represent a logical end point within an NIC through which data flows from a source to the destination machine. Ports are identified by numbers ranging from 0 to 65535. This range of ports is typically categorized into:

- Well Known Ports: Ports 0 to 1023
- Registered Ports: Ports 1024 to 49151
- Dynamic or Private Ports: Ports 49152 to 65535

Software processes within COM600 communicate on the network through a combination of IP Address, Port and a communication protocol. A communication protocol, such as DNP, MMS or Modbus HTTS, signifies a set of rules to be used when sending/receiving data over the network.

The table below list the ports used by various software processes in COM600 accomplishing a specific functionality.

Application type	Application Name	Port Number	Connection Type
OS	HTTP	80	TCP/UDP
COM600	VTRIN- Net Server	81	TCP
COM600	IEC 61850 Proxy OPC Server, MMS	102	TCP
COM600	SNTP OPC Server	123	UDP
OS	DCOM	135	TCP
OS	NetBIOS Name Service	137	UDP
OS	NetBIOS Datagram Service	138	UDP
OS	NetBIOS Session Service	139	TCP
OS	HTTPS	443	TCP
COM600	VTRIN- Net Server	444	TCP
OS	Microsoft-DS SMB file sharing	445	TCP
OS	ISAKMP/IKE	500	TCP
COM600	Modbus Slave OPC Server	502	TCP
COM600	CAL Server – UDP, Syslog	514	UDP
COM600	CoDeSys GatewayService (Logic Processor)	1217	TCP
COM600	CAL Server – TCP, Syslog	1468	TCP
COM600	SimbaServer	1583	TCP
COM600	IEC104 Slave OPC Server	2404	TCP/UDP
OS	Remote Desktop	3389	TCP
OS	IPSec	4500	TCP
COM600	COM600 Substation Analytics	4934	TCP
COM600	CoDeSys OPC Server (Logic Processor)	4965	TCP
COM600	CoDeSys OPC Server (Logic Processor)	4966	TCP
OS	Link-Local Multicast Name Resolution	5355	TCP

Application type	Application Name	Port Number	Connection Type
COM600	SPA	7001	TCP
COM600	VTRIN- Net Server	7605	TCP
COM600	VTRIN- Net Server	7606	TCP
COM600	Configuration Service, Remoting Server	8080	TCP
COM600	GOOSE Analyzer Tool Server	8089	TCP
COM600	CoDeSys ControlService (Logic Processor)	8088	TCP
COM600	COM600 Service	9932	TCP
COM600	CoDeSys ControlService (Logic Processor)	11740	TCP
COM600	CoDeSys GatewayService (Logic Processor)	11743	TCP
COM600	DNP Slave OPC Server (when using secured version)	19999	TCP
COM600	DNP Slave OPC Server	20000	TCP

Windows System services are using the port range from 49152 to 65535. System services are programs that load automatically as part of an application's startup process or as part of the operating system's startup process. System services support the different tasks that the operating system must perform. These ports are blocked by the COM600 default firewall configuration.

3.2.3. Windows Firewall

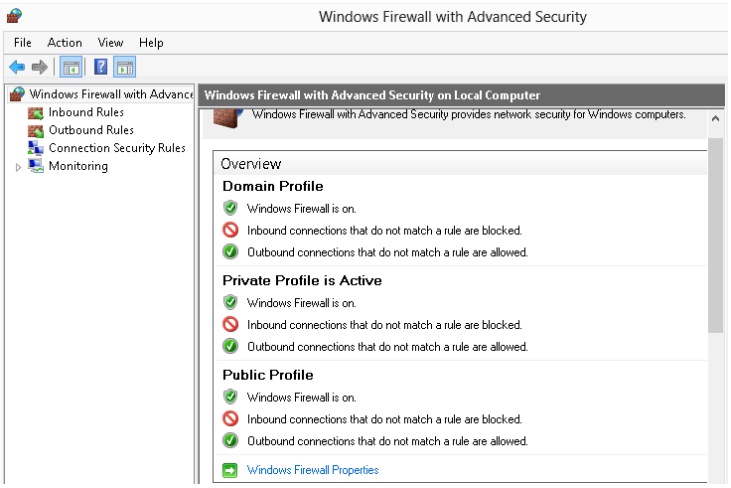
Network security in COM600 can be accomplished by defining a set of rules used by Windows Firewall. Windows Firewall is a software application which allows or blocks any software program executing within COM600 from establishing a connection on the network.

The network connection can be an outgoing connection initiated from COM600 or an incoming connection to COM600. The outgoing connection rules are defined by creating outbound rules and the incoming connection rules are defined by creating inbound rules.

The rules specify whether to allow or block a connection based on some defined criteria. The criteria can include a combination of the factors listed below:

- **Program** – specifies if the rule applies to a single program or to any programs. In case of a single program, further relevant details like name and executing path can be mentioned.

- **Protocol and Port** – specifies if the rule applies to a connection attempt made using a specific network protocol (such as TCP, UDP) and on a specific port. The port mentioned in the rule can cover both sides of a connection by specifying a Local and Remote port number for the connection.
- **Scope** – specifies if the rule applies to a connection attempt made using a specific IP Address or set of IP Addresses. The IP Address mentioned in the rule can cover both sides of a connection by specifying a local and remote addresses for the connection.
- **Action** – specifies the action that needs to be taken when its corresponding condition mentioned in the rule matches. The action specified can either allow a connection or block a connection.
- **Profile** – specifies when a rule needs to be taken into account based on the network to which COM600 is connected.



windows_firewall.png

Figure 3.2.3-1 Windows Firewall

Windows allows three types of classification to the network to which COM600 is connected to. These classifications provide a way of grouping firewall rules and their combinations to achieve a varied connection behavior when communicating on the network.

The network classifications include:

- **Private profile** – Can be used when COM600 is connected to a network through LOCAL LAN adapter. This can be a network of devices which shares the same physical perimeter along with COM600.
- **Public profile** – Can be used when COM600 is connected to a network through REMOTE LAN adapter. This can be a network using which, an authorized user/process can get electronic access to COM600 from devices that may be located outside the physical perimeter of COM600. This network should still be private, isolated from internet or any other public networks.
- **Domain profile** – Can be used as an alternative option to Public profile when COM600 is connected to a network maintained by a domain controller.

Default Firewall Rules

There are few firewall rules defined in COM600 by default. These firewall reflects minimum configuration that could be done at factory. We recommend to further refine these rules by editing the existing ones or creating new rules to achieve a desired security profile.

To access Windows Firewall:
1. Login to COM600 using a user account that has administrative priveleges.
2. Go to **Control Panel**.
3. Click **Windows Firewall**.
4. Click **Advanced Settings** to open the Windows Firewall settings window.
5. Select
   - **Inbound Rules** to further configure rules affecting incoming connection requests.
   - **Outbound Rules** to further configure rules affecting outgoing connection requests.

The table below shows a brief summary of the inbound rules available by default.

Rule name	Rule description
CALServer-UDP	Allows UDP connection on port 514. This rule allows incoming syslog messages which are further processed by CAL Server in COM600.
CALServer- TCP	Allows TCP connection on port 1468. This rule allows incoming syslog messages which are further processed by CAL Server in COM600.
DNP-TCP	Allows TCP connection on port 20000. This rule allows incoming DNP messages which are further processed by a DNP slave in COM600.
DNP-UDP	Allows UDP connection on port 20000. This rule allows incoming DNP messages which are further processed by a DNP slave in COM600.
DNP-TCP-TLS	Allows TCP connection on port 19999. This rule allows incoming DNP messages using TLS which are further processed by a DNP slave in COM600.
HTTP	Allows TCP connection on port 80. This rule allows incoming HTTP traffic for COM600 WebHMI.
HTTPS	Allows TCP connection on port 443. This rule allows incoming secure HTTP traffic for COM600 WebHMI.
IEC 61850	Allows TCP connection on port 102. This rule allows incoming MMS messages which are further handled by IEC 61850 Proxy Server in COM600.
IEC 870-5-104	Allows TCP connection on port 2404. This rule allows incoming IEC-104 messages which are further handled by IEC104 Slave in COM600.

Rule name	Rule description
MODBUS-TCP	Allows TCP connection on port 502. This rule allows incoming Modbus messages which are further handled by Modbus Slave in COM600.
SPA-TCP	Allows TCP connection on port 7001. This rule allows incoming SPA messages which are further handled by SPA client process in COM600.
SNTP	Allows TCP connection on port 123. This rule allows incoming SNTP messages which are further handle by SNTP client in COM600.
Offside remoting	Allows TCP connection on port 4934. This rule allows incoming messages for Offside related application in COM600.
GATServer	Allows TCP connection on port 8089. This rule allows incoming messages for GOOSE Analyzer application in COM600.
RemoteDesktop(UDP)	Allows UDP connection on port 3389. This rule allows incoming connection requests for Windows Remote Desktop application.
RemoteDesktop(TCP)	Allows TCP connection on port 3389. This rule allows incoming connection requests for Windows Remote Desktop application.
IEC 61850 OPC Server	Allows any connection on any port for program IEC 61850 client in COM600.
SAB600	Allows any connection on any port for COM600 Configuration Service. This rules allows connection requests from SAB600 Gateway Management tool to COM600.
Vtrin	Allows any connection on any port for VTRIN Server. This rule allows incoming connection requests for Data Historian application in COM600.
Gateway Service	Allows any TCP/UDP connection for CoDeSys Gateway Service. This rule allows connection requests from Logic Editor in SAB600 to Logic Processor in COM600.
CodeMeter Runtime Server	Allows any TCP/UDP connection for CodeMeter. This application is used in license management for Logic Processor (CoDeSys) application.

3.2.4. COM600 Configuration Service

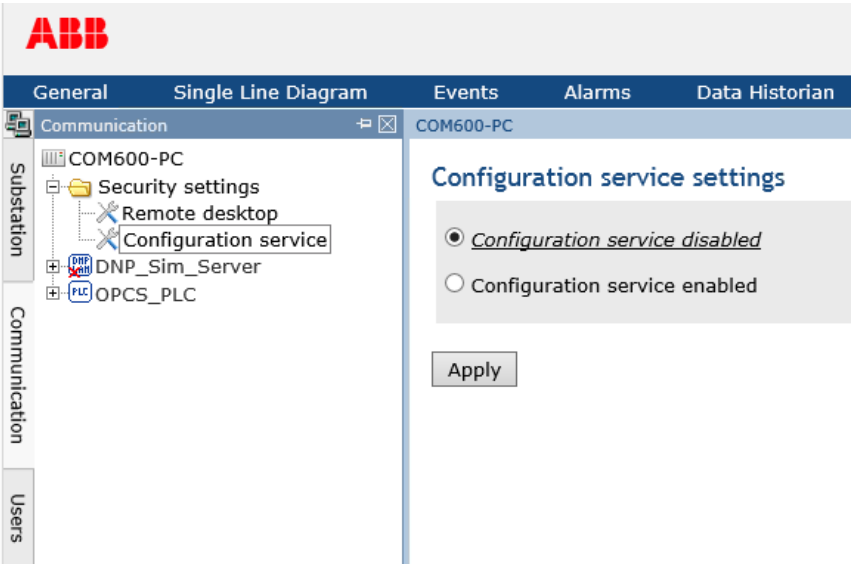
The Configuration Service running in COM600 allows a configuration to be loaded into COM600. A typical COM600 engineering workflow involves a COM600 application engineer performing application configuration using SAB600 application in a workstation. After the configuration is ready, it is uploaded to COM600 using Gateway Management tool in SAB600. See Appendix 1 for details on how to launch Gateway Management Tool.

When Gateway Management tool is launched in SAB600, it will attempt to establish a network connection to COM600 to upload additional configuration settings. Configuration Service running in COM600 will accept the connection.

A COM600 user with administrative privileges can enable/disable Configuration Service using COM600 WebHMI. ABB recomments that Configuration Service is enabled only at times when a new application configuration needs to be loaded into COM600, and leave it disabled otherwise. This allows a tighter control for managing the configuration loaded into COM600.

To control Configuration Service from WebHMI:

1. Login to COM600 WebHMI as an admin user.
2. Select **Communication** tab.
3. Select **Security settings** node from the communication tree.
4. Select **Configuration service** child node.
5. Select
   - **Configuration service disabled** option to disable Configuration Service.
   - **Configuration service enabled** option to enable Configuration Service.
   - Click **Apply**.



Enable_COM600_Configuration_Service.png

Figure 3.2.4-1 Enable COM600 Configuration Service

Configuration Service can use any one of the two built-in NICs available in COM600 to listen for any incoming connection requests to perform Gateway Management. By default, Configuration Service is preconfigured to use LOCAL NIC.

Although Configuration Service can be changed to use REMOTE NIC, ABB recommends that LOCAL NIC is used for Gateway Management purposes. Allowing Configuration Service to use REMOTE NIC implies that this service is available for remote connection from entities which may be located outside the physical perimeter of COM600.

Configuration Service should be reconfigured whenever there is a change in IP Address of the NIC to which it is associated.

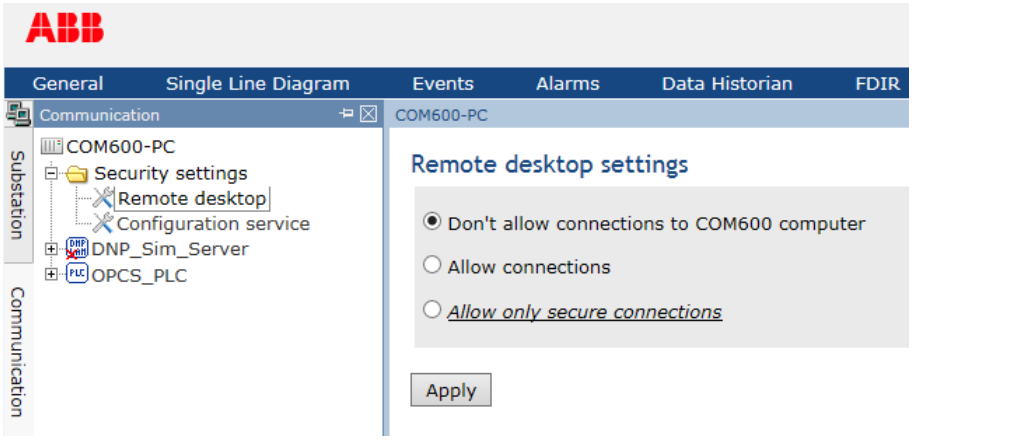
To reconfigure Configuration Service from WebHMI:
- Click **SetRemotingParameters** shortcut on COM600 desktop. **COM600 Remoting Settings** window opens.
- Select the new IP address of the **LOCAL NIC** and click **Apply**.
- Verify that the change reflects in **Current IP and Port number**.

3.2.5. Remote desktop

Windows remote desktop application in COM600 can be used to perform any maintenance activities on COM600. These activities may involve managing for example any OS related configuration, files/folder in hard drive, or network configuration. COM600 can be made available for remote connection from peer Windows devices located outside its physical perimeter by connecting it to a REMOTE LAN.

Before using Windows remote desktop application, the remote settings in COM600 should be enabled to allow remote desktop connections. This can be done using COM600 WebHMI. ABB recommends that remote desktop connections are enabled only when needed.

To configure Remote desktop settings from WebHMI:
1. Login to COM600 WebHMI with a user account that has administrative privileges.
2. Select **Communication tab**.
3. Click **Security Settings** node in the tree displayed.
4. Select **Remote desktop** child node.
5. Select
   a. **Allow connections / Allow only secure connections** option to enable remote desktop connection to COM600.
   b. **Don’t allow connections to COM600 computer** option to disable remote desktop connection to COM600.
6. Click **Apply**.



Enable_Remote_Desktop.png

Figure 3.2.5-1 Enable Remote Desktop Connection

3.2.6. Time service

Time used in COM600 can be synchronized using SNTP to an external clock device either by using Windows time service or by using COM600 SNTP OPC Sever.

The SNTP OPC Server available in COM600 offers an SNTP server and an SNTP client. The SNTP client enables time synchronization of COM600 to an external SNTP server, such as a GPS Clock device. The SNTP server can be used to serve time to peer devices (such as protection relays and RTUs), which share the same physical perimeter along with COM600. See SNTP OPC Server User's manual for detailed information on how to configure and use SNTP OPC Server.

Windows Time service should be disabled whenever SNTP OPC Server is in use. These two software application are mutually exclusive, since both receive SNTP messages from an external SNTP server to sync time. By default, Windows Time service is disabled in COM600 at factory.

3.3. Security Event Monitoring

3.3.1. Windows Security Events

Audit policies provide a means to monitor various actions by a user or a software process at the Windows Operating System level in COM600. The events generated by a specific audit policy denote a success or failed result for some action.

The tracked events can be viewed and inspected using **Windows Event Viewer** tool. These events are available under **Security Events** category in **Windows Event Viewer Tool**. In addition, using CAL & SEV OPC server in COM600 application configuration,

COM600 WebHMI can also be used to view a subset of these events which may be relevant to a COM600 administrator/operator.

Audit policies allow monitoring for the following actions initiated by a user or a software process:

- **Account Management** – Use policies under this category to monitor user account name changes, enabling/disabling user account, creating/deleting user account, password changes, and user group change for a user account.
- **Detailed Tracking** – Use policies under this category to monitor when a process starts/terminates, inbound remote procedure call connections, encryption/decryption requests that are made to Data Protection application interface.
- **DS Access** – Use policies under this category to monitor use of Active Directory Domain Services related objects.
- **Logon/Logoff** – Use policies under this category to monitor when a user is logged in/ logged off, either physically at your computer or over a network.
- **Object Access** – Use policies under this category to monitor access to a file, folder, and printer.
- **Policy Change** – Use policies under this category to monitor changes to local security policies, user rights assignments, auditing policies and/or trust policies.
- **System** – Use policies under this category to monitor startup/shutdown on COM600, change in time.

There are multiple options to configure audit policies. These policies can be configured locally in COM600 either by using Local Security Policy editor or by using **auditpol** command line tool. In addition, these policies can also be managed by a domain controller in cases where COM600 is part of a domain. Policy configuration made using any one of these options may not necessarily reflect configuration made by another. Therefore, ABB recommends that “auditpol” command line tool in COM600 is always used to view/edit any audit policy.

The audit policies that are preconfigured in COM600 at factory are listed below. These policies are configured to generate both success and failure events when applicable.

- Account Management
  - Computer Account Management
  - Security Group Management
  - User Account Management
- Logon/Logoff
  - Account Lockout
  - Logoff
  - Logon
- Policy Change
  - Authentication Policy Change
  - Authorization Policy Change
- System
  - Security State Change.

3.3.2. COM600 Security Events

Security Events (SEV) OPC server

COM600 application related security events can be generated using SEV OPC Server. These events include for example COM600 WebHMI user logon/logoff actions, operator control operations, and configuration upload and download action. See CAL and SEV OPC Server User's Manual for additional details on how to configure and use it in COM600.

The security events generated for various COM600 software components can be forwarded to external entities using syslog messages. One such entity is COM600 CAL server.

Centralized user Activity Logging (CAL) server

The CAL server in COM600 is capable of receiving and storing security events in the form of syslog messages. The security events include events generated both from within COM600 and/or from other devices (such as protection relays/RTUs) that share the same physical perimeter with COM600.

The security events received by CAL server, can be stored within COM600 for a maximum configurable time period of up to ninety days. The security events can also be electronically forwarded to up to six entities located outside the physical perimeter of COM600, through syslog messages. This allows for remote security event monitoring from devices outside the physical perimeter of COM600.

The security events captured by CAL server can be viewed using COM600 WebHMI. These security events can be viewed only with COM600-Administrator privileges.

3.4. Malicious Code Prevention

3.4.1. Data Execution Prevention

Data Execution Prevention (DEP) is a Windows Operating System security feature that protects from malicious code execution.

In general, software is loaded into memory for execution. It also uses heap and stack from memory to manage its data for its functioning. Any vulnerabilities in software like buffer overrun, could allow malicious code to be injected in to the memory through the data it uses. Once the malicious code is loaded in to memory there is always the risk of it being executed.

The operating system provides isolation in memory for a software process between the code being executed and the data it uses. Any attempt to execute code from the region

of memory marked for data used by a process will be blocked by using this DEP feature. DEP can be hardware or software enforced.

DEP can be configured either to protect all programs or to protect only essential Windows programs or services. In COM600 DEP is by default configured to protect essential Windows program or services.

To configure DEP:
1. Login to COM600 using a user account that has administrative privileges.
2. Go to **Control Panel**.
3. Click on **System**.
4. In the subsequent **System properties** dialog, go to **Advanced** tab. Click **Settings** under **Performance**.
5. In the subsequent **Performance Options** dialog, either select
   - **Turn on DEP for essential windows programs and services only**,
   - **Turn on DEP for all programs and services except for few selected options**.
6. Click **Apply**.

3.4.2. Antivirus programs

Anti-virus software that provide real-time protection against malicious software, can be used on COM600 computer and on workstations from where SAB600 is used.

An anti-virus software typically uses a background scan engine, virus definition files and a quarantine policy for its functioning. The scan engine scans for files in a computer and uses virus definitions to identify files with potential malignant intent. The files identified are then quarantined and restricted from further access. Additional alerting mechanism may be available whenever infected files are quarantined and/or accessed.

The virus definitions used by a scan engine to identify an infected file can change as more and more threats become known. Therefore it is highly critical to keep these definitions up to date for a security strategy to be successful. Multiple methods are offered by various anti-virus vendors to keep these definitions up to date. ABB recommends to choose a convenient method, without exposing COM600 to internet or to any public networks.

The scan engine may offer protection through an on-access and/or on-demand scanning mechanism. On-access scanning provides a strict continuous protection mechanism where any requested file is scanned prior to loading. On-demand scanning provides a more relaxed protection mechanism in where files are scanned only at periodic intervals scheduled as per choice. Each of this options has an impact on the performance of the computer, with on-access scanning having a greater impact and on-demand scanning a lower impact.

Tradeoff in performance impact can be achieved by carefully configuring various options offered by the chosen anti-virus software. Below is a list of configuration selections that

can help achieve a reasonable security profile in COM600 at a reasonable performance cost:

- Restrict CPU utilization of anti-virus software to 20%. This limit can be further adjusted if the anti-virus software cannot complete an on-demand scan within a reasonable time.
- Disable email scan feature if the anti-virus software has it enabled by default.
- Disable network scans and scan only for files within local file system. Each computer in the network should have its own antivirus scanning mechanism. In addition also have a stricter network policy to allow mapping of only authorized network shares by authorized personnel.
- Enable buffer overflow protection, access protection and script scan features if available.
- In general, ABB recommends not to exclude any files from local file system during an anti-virus scan. In case of a considerable impact to application performance in COM600, selectively exclude folders containing COM600 application related executable files. Some of these folders are,
  - C:\Program Files(x86)\3S CODESYS\GatewayPLC
  - C:\Program Files(x86)\3S CODESYS\CODESYS OPC Server 3
  - C:\Program Files(x86)\ABB Oy\Vtrin
  - C:\Program Files(x86)\ABB Oy\RTDB\bin
  - C:\Program Files(x86)\ABB Oy\CSCommon\bin
  - C:\Program Files(x86)\COM610 GW SW\GAT
  - C:\Program Files\COM610 GW SW

Never exclude Windows operating system related directories from virus scan.

Quarantine policy enforced should exclude any COM600 related executable files from any automatic delete or cleanup action. These files should be handled manually by a qualified security personnel.

3.5. Secure Patch Management

3.5.1. Windows Operating System updates

Microsoft releases updates periodically to patch found issues and/or vulnerabilities in various software components included in Windows operating system. These updates are categorized as:

- **Critical updates** – Updates to fix specific, non-security related issues.
- **Security updates** – Updates to fix security vulnerability.
- **Critical** – Updates to fix a vulnerability which could allow further degradation of system and does that without any user action.
- **Important** – Updates to fix a vulnerability which could allow confidentiality/integrity of user data being compromised.

- **Low** – Updates to fix a vulnerability whose exploitation can be extremely difficult, or whose impact can be minimal.
- **Moderate** – Updates to fix a vulnerability whose exploitation can be mitigated through a configuration change.

Available updates from Microsoft should be tracked periodically and checked for compatibility prior to installation. The compatibility of latest updates from Microsoft with COM600 specific functionality is tested and verified periodically by ABB. The test results can be found from COM600 product page, which includes a COM600 Patch Compatibility Report specifying the details. While these reports may not cover engineering workstation from where SAB600 application may be used, it is recommended to install all relevant updates to these workstations. For any incompatible updates found, ABB recommends to create/revise a dated mitigation plan until compatibility issues can be addressed.

Latest available updates can be obtained and updated on COM600 by creating either an online or an offline setup. The online setup includes adding and maintaining a local Windows Server Updates Services (WSUS) server infrastructure. The offline setup includes manually obtaining update installation files from Microsoft update catalog website and transferring those files to COM600 through a physical medium for installation. For both online and offlines setups, careful measures should be taken for this purpose without compromising electronic security perimeter of COM600. ABB recommends that the updates are installed by an authorized system administrator.

Online Updates through WSUS

Updates can be made to COM600 by setting up a local WSUS infrastructure. This setup requires a Windows server running Windows 2012 R2 in a 64 bit machine, connected to COM600 in a private network. This server would also need access to internet through a public network, capable of connecting to Microsoft Update Server as shown in Figure 3.5.1-1. It is important to achieve a proper network isolation between various devices involved, by careful implementation of firewall policies and secured access profiles.

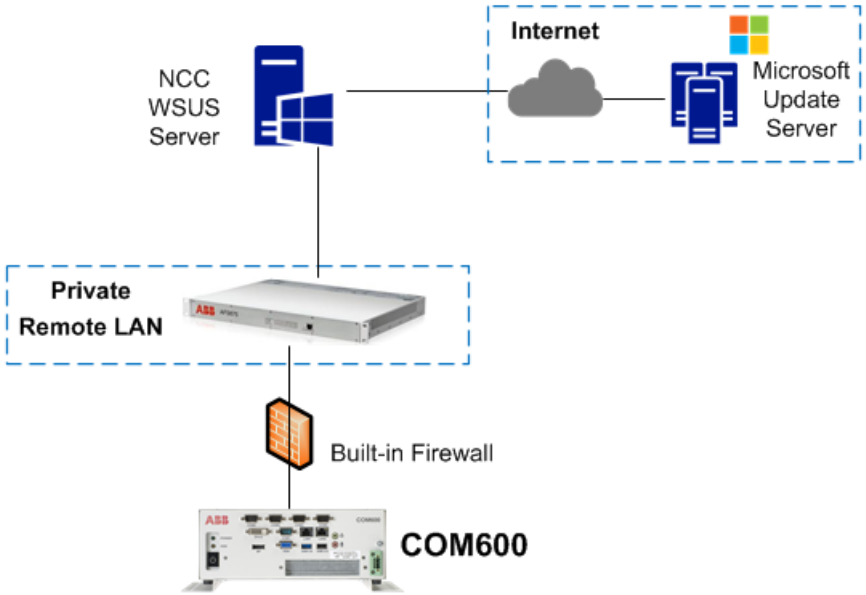


Figure 3.5.1-1 WSUS setup to update COM600

With this setup, available updates from Microsoft Update server can be analyzed before installation for compatibility and approved locally for further installation. Approved updates can be installed automatically in COM600 by additional configuration made locally within COM600. See Appendix 2 for details on how to manage this setup, browse for available updates and approve those for further installation in COM600.

Offline Updates manually

To manually get Windows security updates for Microsoft Update Catalog website:

1. Check available security updates that are tested and verified for compatibility from COM600 compatibility reports.
2. Go to Microsoft Update Catalog website (http://catalog.update.microsoft.com/).
3. Enter the bulletin ID mentioned in the patch compatibility report and/or the operating system of COM600 to the search field, for example “Windows Embedded 8” and click **Search**.
4. There might be several search results for example for different system architectures. Find the correct security update for the architecture and click **Add** to add it to a basket, which represents the list of updates to be downloaded.
5. Repeat above two steps for each update needed.
6. Click **View Basket** to view all updates that are selected for further download.
7. Click **Download** and choose a folder location to where the updates will be downloaded.
8. Manually transfer all updates through a storage medium (like USB drive, or an authorized network share) to COM600 and install them in COM600 in the recommended order.

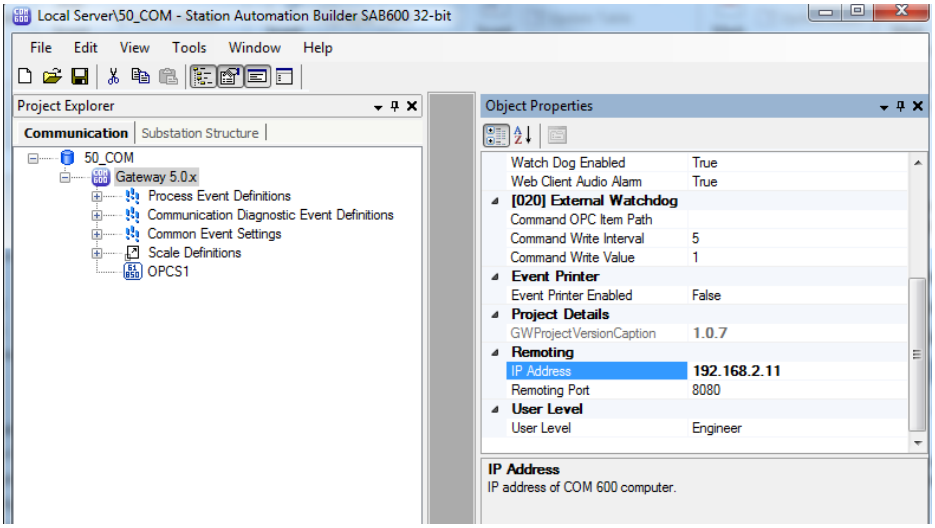
Appendix 1

Launch Gateway Management Tool

Gateway Management tool can be used to maintain application configuration in COM600-

To launch Gateway Management tool from SAB600:

1. Open SAB600 from Engineering PC/workstation.
2. Open an existing project if available, or create a new project
3. Select the Gateway object available
4. Go to **Remoting** section in the object properties window and edit the **IP Address** property. The value of IP Address property should indicate COM600 IP Address in use.



Configuring_Gateway_IP_Address.png

Figure 4.1-1 Configuring Gateway IP address

5. After editing the IP Address, right click the Gateway object and launch **Gateway Management** tool.

Appendix 2

Setting up local WSUS server to update COM600

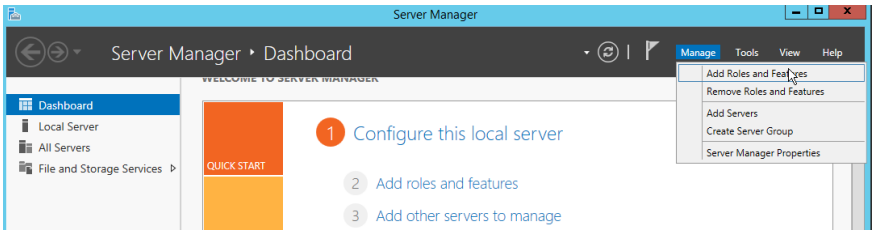
Updates from Microsoft for Windows and related features are managed through WSUS. This setup requires a server running Windows 2012 R2 in a 64 bit machine, connected to COM600 in a private network. The server would also need access to internet through a public network capable of connecting to Microsoft Update Server, as shown in Figure 3.5.1-1.

Add WSUS Server Role

The typical installation of Windows Server 2012 R2 does not include WSUS functionality by default. This functionality has to be added to Windows Server 2012 R2 if not available already.

To add WSUS feature to Windows Server 2012 R2:

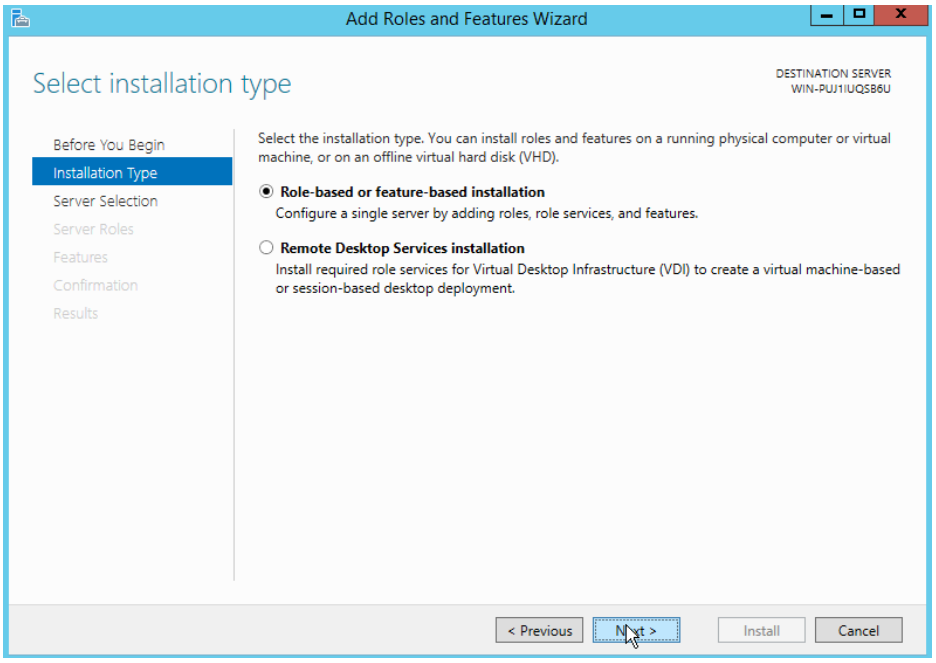
1. Launch Server Manager Application. Click **Manage** and **Add Roles and Features** as shown in Figure 5.2-1.



Server_Manager_Add_Roles_and_Features.png

Figure 5.2-1 Server Manager, Add Roles and Features

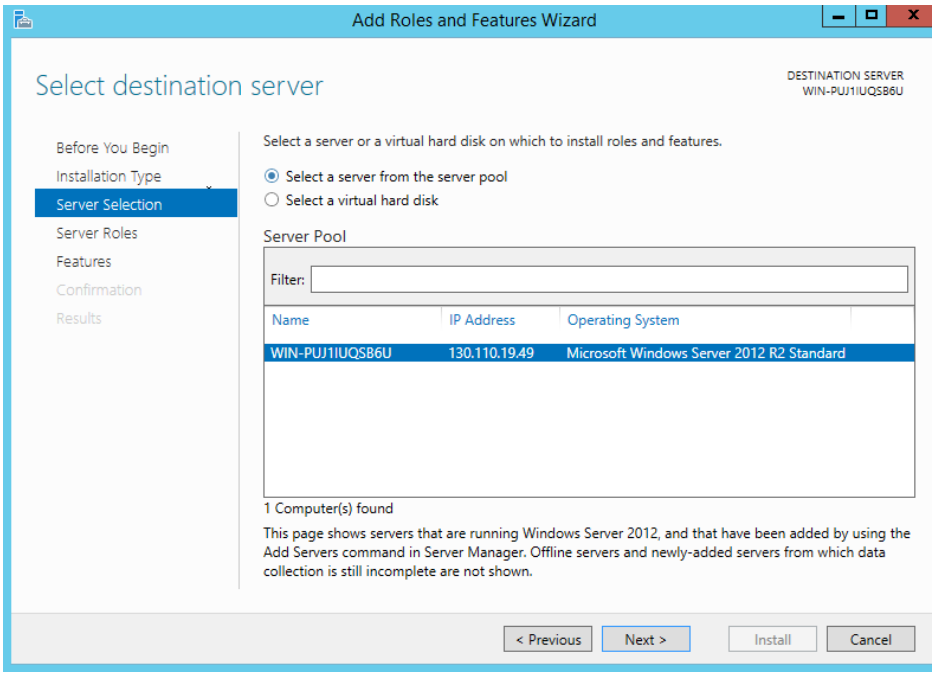
2. The **Add Roles and Features Wizard** opens. Select **Role-based or feature-based installation** in the **Installation Type** section and click **Next** as shown in Figure 5.2-2.



Add_Roles_Wizard_Installation_Type.png

Figure 5.2-2 Add Roles Wizard, Installation Type

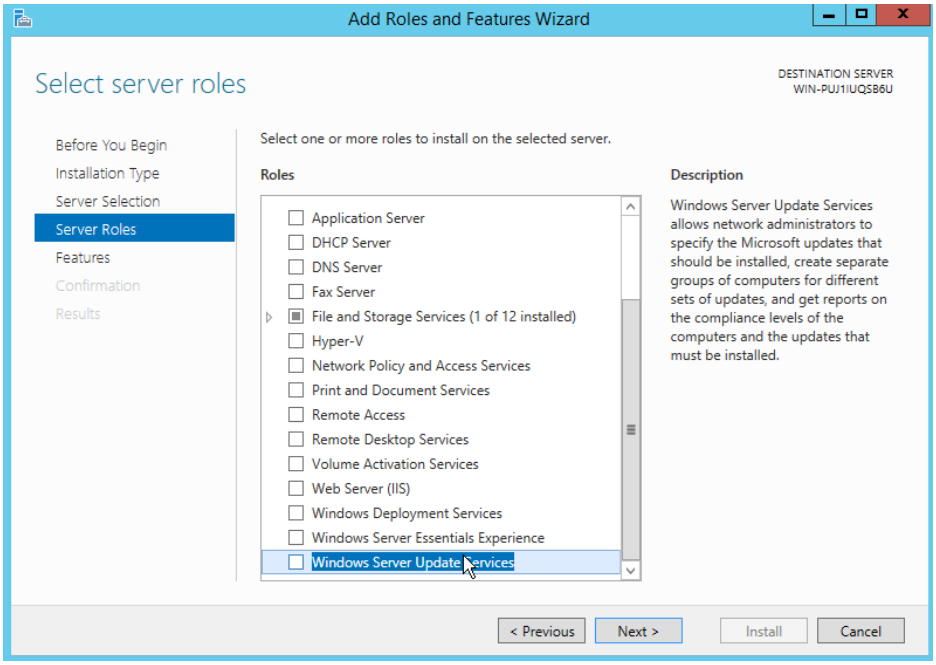
3. In the **Server Selection** section click **Select a server from the server pool**. Make sure the intended machine running Windows Server 2012 is selected in **Server Pool** and click **Next** as shown in Figure 5.2-3.



Add_Roles_Wizard_Server_Selection.png

Figure 5.2-3 Add Roles Wizard, Server Selection

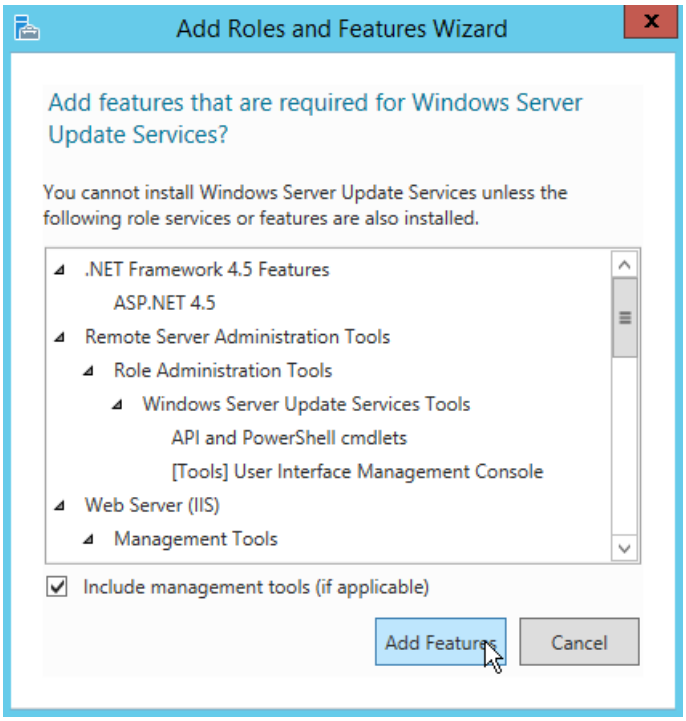
4. In the **Server Roles** section scroll to **Roles selection** and select **Windows Server Update Services**. Click **Next** as shown in Figure 5.2-4.



Add_Roles_Wizard_Server_Roles.png

Figure 5.2-4 Add Roles Wizard, Server Roles

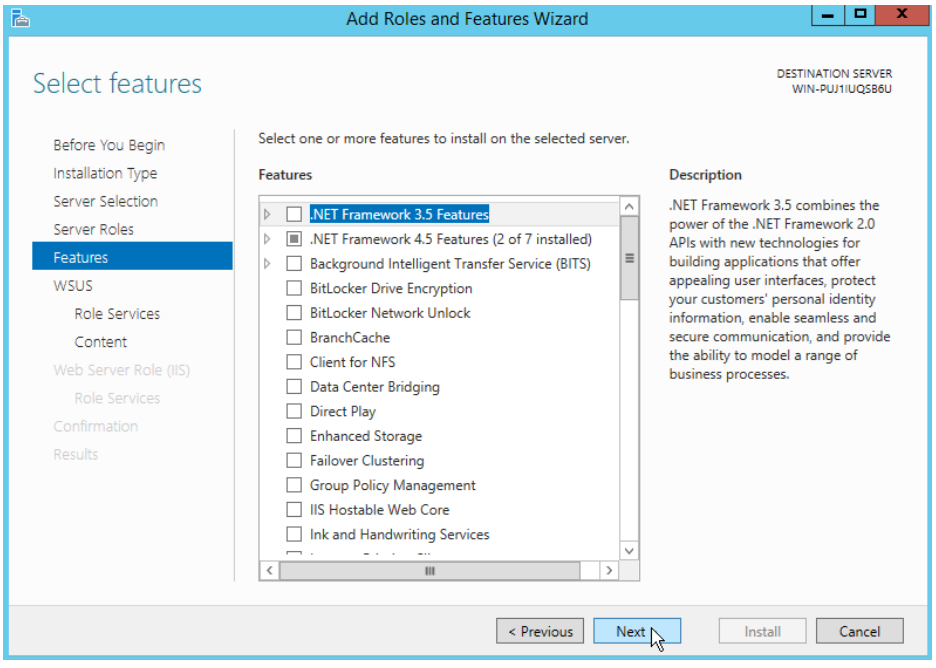
5. In the**Add Roles and Features Wizard** define additional **Roles** which are necessary for WSUS functionality, but are deemed to be missing in Windows Server 2012 R2. Click **Add Features** as shown in Figure 5.2-5.



Add_Roles_Wizard_Add_additional_features.png

Figure 5.2-5 Add Roles Wizard, Add additional features

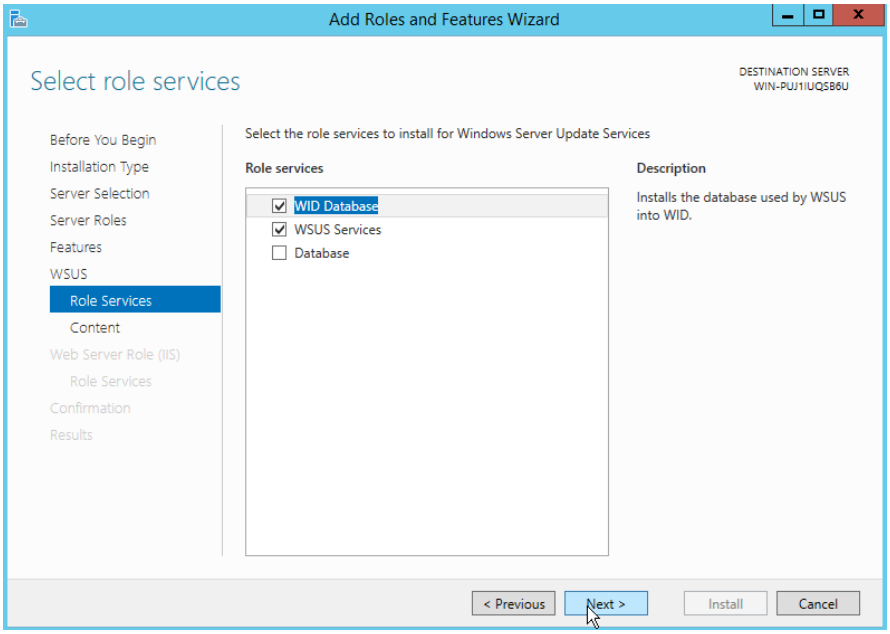
6. In the **Features** section click **Next** as shown in Figure 5.2-6.



Add_Roles_Wizard_Features.png

Figure 5.2-6 Add Roles Wizard, Features

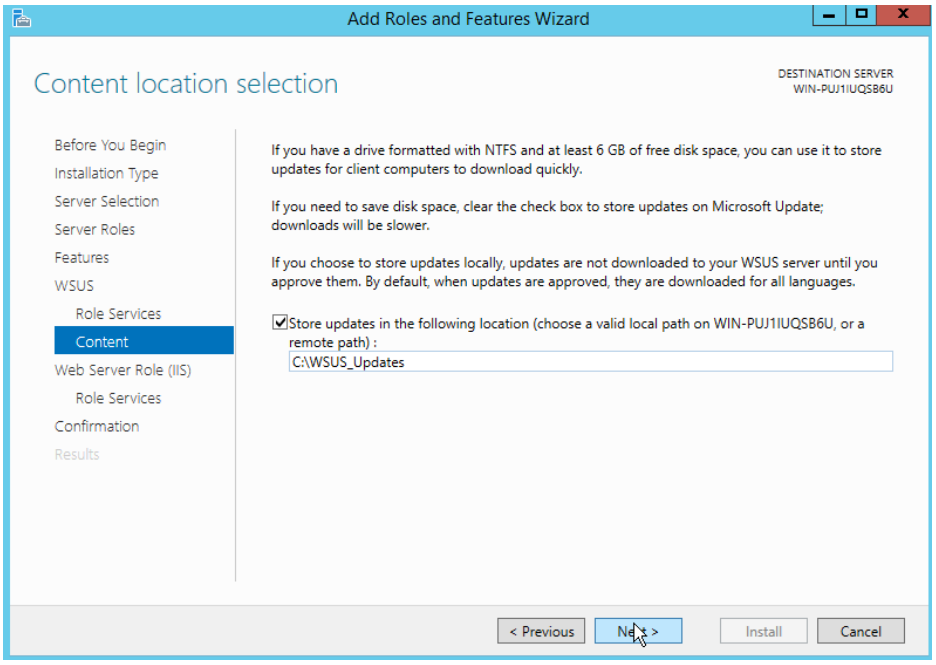
7. In the **WSUS/Role Services** section check that the **WID Database and WSUS Services** is selected and click **Next** as shown in Figure 5.2-7.



Add_Roles_Wizard_WSUS_Role.png

Figure 5.2-7 Add Roles Wizard, WSUS Role Services

8. In the**WSUS/Content** section choose a desired folder path to where the updates from Microsoft will be downloaded. Updates from this location will then be later pushed to any COM600 devices connected through a private network. Also note that as more and more updates are downloaded, the selected folder size can grow large. Take this into account when selecting the location.



Add_Roles_Wizard_WSUS_Content.png

Figure 5.2-8 Add Roles Wizard, WSUS Content

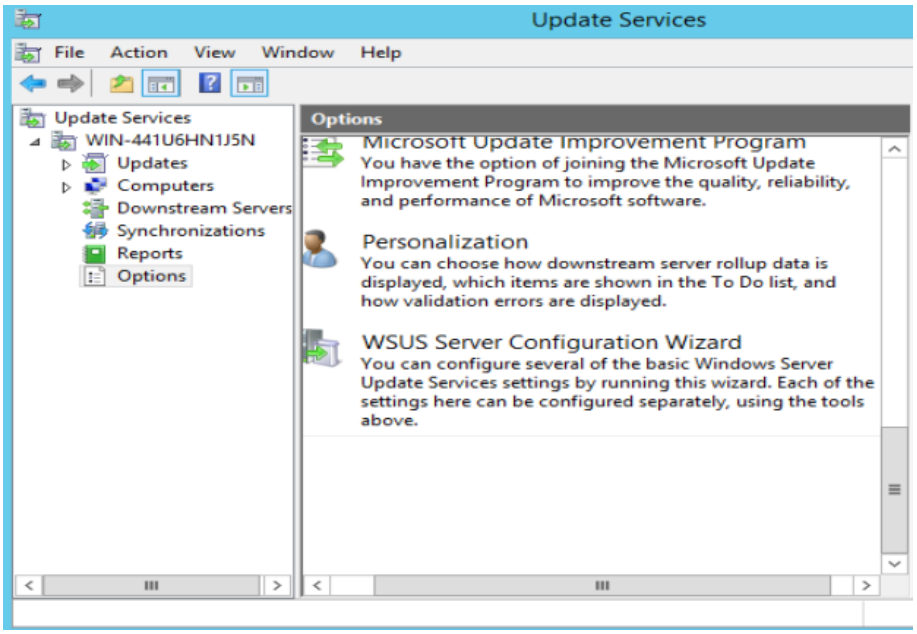
9. In the **Web Server Role (IIS)/Role Services** section click **Next** without changing the default settings.
10. In the **Confirmation** section click **Install** and wait for the installation to complete.

Open WSUS Configuration Wizard

After adding WSUS Role to Windows Server 2012 R2, the WSUS Configuration Wizard should open automatically. If not, the wizard can be launched manually.

To manually launch WSUS Configuration Wizard:

1. Launch **Server Manager**.
2. Go to **Dashboard**, and click **Tools > Windows Server Update Services**.
3. **Update Services management** console opens showing local Windows Server 2012 R2 information.
4. In the Update Services management console, select **Options** from the drop down available under Windows Server listed, scroll down and click **WSUS Server Configuration Wizard**as shown in Figure 5.3-1.



Open_WSUS_Configuration_Wizard.png

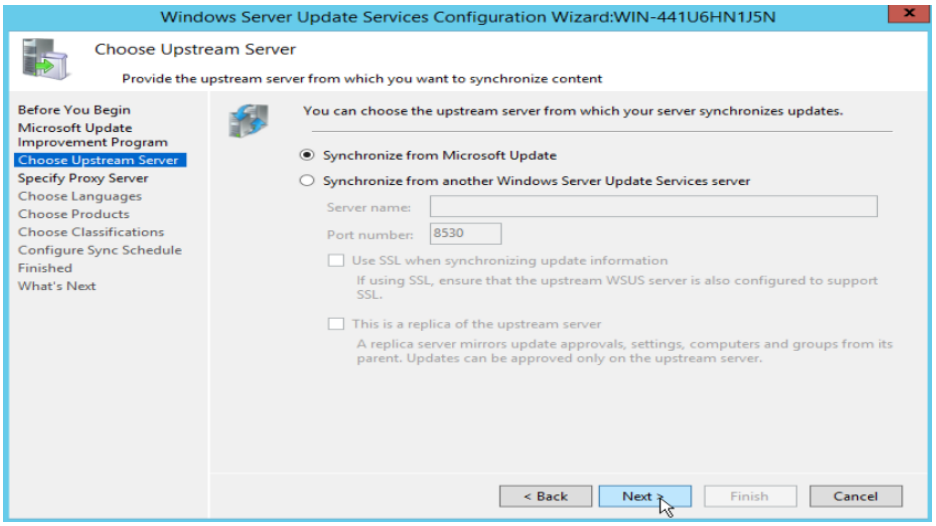
Figure 5.3-1 Open WSUS Configuration Wizard

Configuring WSUS

This section explains how to configure WSUS settings through WSUS Configuration Wizard. It is recommended to make appropriate settings that are specific to deployed environment.

To configure WSUS settings through WSUS Configuration Wizard:

1. The WSUS Configuration Wizard opens and prompts for information. Once the information is available click **Next**.
2. In the **Microsoft Update Improvement Program** section check/uncheck preference to participate in the program and click **Next**.
3. In the **Choose Upstream Server** section select **Synchronize from Microsoft Update** and click **Next** as shown in Figure 5.4-1. Make sure that the machine running the WSUS service is connected to the internet.



WSUS_Wizard_Choose_Upstream_Server.png

Figure 5.4-1 WSUS Wizard, Choose Upstream Server

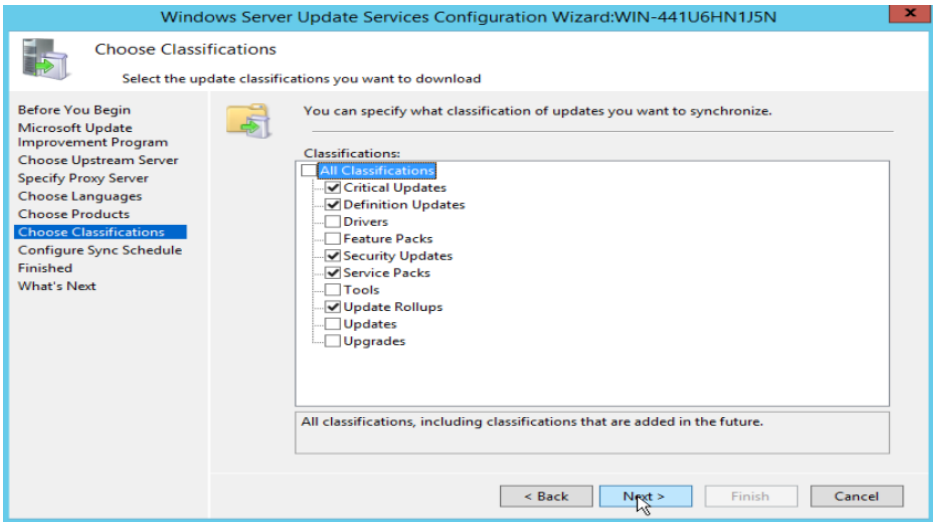
4. In the **Specify Proxy Server** section of the configuration wizard, specify any intermediary proxy settings to connect to internet, and click **Next**.
5. In the subsequent section, click **Start Connecting** to verify the connection to Microsoft Update Server. Once the connection is verified, click **Next**. If not, double check the internet connection in the local machine and proxy settings.
6. In the **Choose Languages** section, select **Download updates only in these languages** and click **English**.
7. In the **Choose Products** section, click on the products specified below, based on the COM600 product version being used, see Table A2-1.

Table A2-1 Microsoft Product for COM600 version

COM600 Product Version	Products chosen in WSUS Configuration
COM600 v4.1	1. Developer Tools, Runtimes, and Redistributables 1.1. Visual Studio 2005 1.2. Visual Studio 2010 1.3. Visual Studio 2012 2. Windows 2.1. Windows Embedded Standard 7

COM600 Product Version	Products chosen in WSUS Configuration
COM600 v5.0 and above	1. Developer Tools, Runtimes, and Redistributables 1.1. Visual Studio 2005 1.2. Visual Studio 2008 1.3. Visual Studio 2010 1.4. Visual Studio 2013 2. Windows 2.1. Windows 8 Embedded

8. In the **Choose Classifications** section, select update classifications as shown in Figure 5.4-2 and click **Next**.



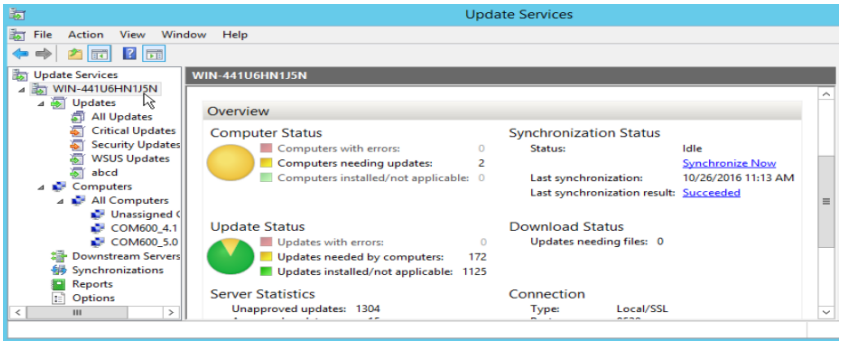
WSUS_wizard_Update_Classification.png

Figure 5.4-2 WSUS wizard, Update Classification

9. In the **Configure Sync Schedule** section, select desired synchronization schedule for updates from Microsoft and click **Next**.
10. In the **Finished** section, select **Begin initial synchronization** and click **Next**.
11. Click **Finish**.

The WSUS server should now be configured to load updates from Microsoft Update Server.

After **Begin Initial Synchronization** is complete, all applicable updates must be listed within **Update Services** management console. To get a cumulative view of updates, click on the server name in Update Services management console. An overview of all updates is shown, as shown in Figure 5.4-3. In addition, manual synchronize can be initiated by clicking **Synchronize Now**, from time to time to get latest updates from Microsoft Update Server.



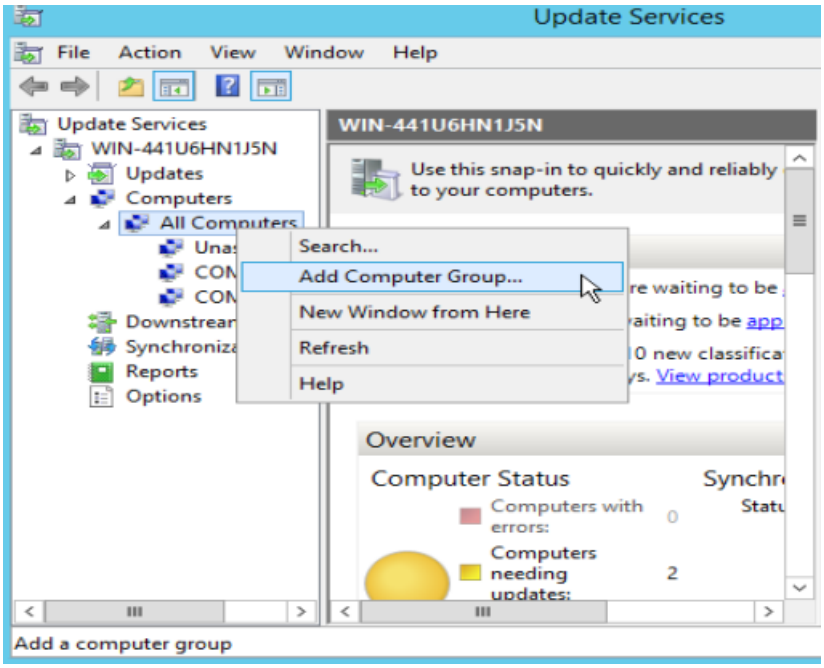
WSUS_Server_Status.png

Figure 5.4-3 WSUS Server Status

Add COM600 Computer group

Add a new computer group in WSUS server for each of the COM600 product versions deployed. This is done uder **Computers** as shown in Figure 5.5-1.

Choose a name that reflects the product versions such as COM600_4.1 or COM600_5.0. All subsequent updates approved for install will be made to this chosen computer group. Any subsequent changes to the computer group name might require reapproving all the updates to the new computer group name.



Add_Computer_Group.png

Figure 5.5-1 Add Computer Group

Rename COM600 computer name

This section describes configuration changes that need to be done in COM600 before connecting to WSUS server. Before proceeding, make sure COM600 device is assigned a unique computer name.

To rename COM600 computer:

1. Login to COM600 with a user account that has Windows administrator privileges.
2. Go to **Control Panel** and select **System**.
3. Select **Advanced system settings**.
4. In the subsequent **System Properties** dialog, select **Computer Name**.
5. Click **Change**.
6. Assign a unique name and click **OK**.

Enable Windows Update Service in COM600

The Windows Update service is by default disabled in COM600. To enable and start the service:

1. Open Control Panel.
2. Click **Administrative Tools**.
3. Click **Services**. **Services management Console** opens.

4. In the services listed, find **Windows Update** service and double click to open the properties dialog.
5. In the properties window, set
   a. Startup Type to be **Automatic**.
   b. Click **Start** to start the service.
   c. Then click **OK** to save and close the properties dialog.

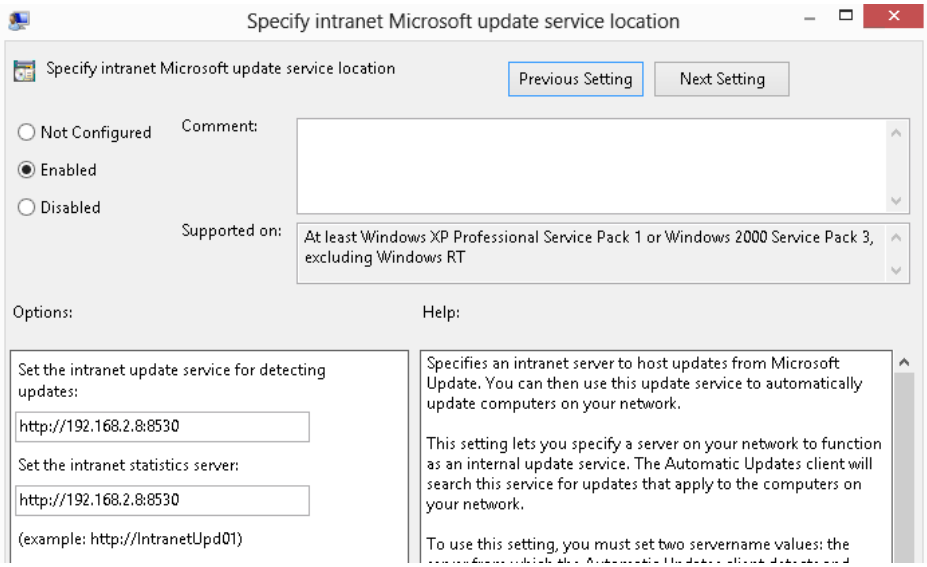
Group policy setting in COM600

Windows installed in COM600 is by default set to receive updates directly from Microsoft Update Server. Change this default setting to receive updates from the intermediary local WSUS server. The setting is changed in **Local Group Policy Editor**.

If COM600 is setup to be part of a domain, then the changes made to **Local Group Policy** will be overwritten by **Domain Group Policy**. In this case, contact the Domain Administrator to make the needed changes to **Domain Group Policy** object.

To connect COM600 to local WSUS server:

1. Open Control Panel.
2. Click **Administrative Tools** and select **Local Group Policy Editor**.
3. **Local Group Policy** editor window opens.
4. Go to **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Windows Update**. All settings related to Windows Update are shown.
5. Double click **Specify intranet Microsoft Update Service Location**.
6. Click **Enabled** and type in the URL that includes IP Address of WSUS server:
   a. Set the intranet update service for detecting updates to http://{IP Address or hostname of WSUS Server}:8530
   b. Set the intranet statistics server to http://{IP Address or hostname of WSUS Server}:8530
7. Click **OK**.



Specify_WSUS_server_in_COM600.png

Figure 5.8-1 Specify WSUS server in COM600

Connecting COM600 to WSUS Server

To connect to COM600 after changing group policy settings:

1. Open command prompt in administrator mode and execute command **`gpupdate /force`**.
2. Initiate the Windows update agent in COM600 to connect to WSUS server by executing the following commands from command prompt
   - **`wuauclt.exe /resetauthorization /detectnow`**
   - **`wuauclt.exe /reportnow`**

Assign COM600 to Computer Group in WSUS server

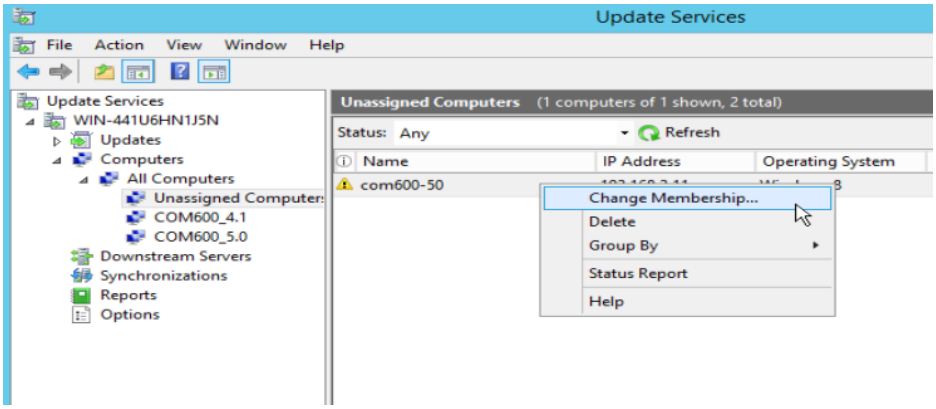
After executing the connection commands as explained in 5.9, Connecting COM600 to WSUS Server, go back to WSUS server and locate the connected COM600 using **Update Services Console**. For more information on how to open Update Services Console in WSUS server, see 5.2, Add WSUS Server Role.

In the Update Services Console, go to **Computers** > **All Computers** > **Unassigned Computers**. The computer name of COM600 from where the connection attempt was initiated, should be listed as an unassigned computer.

Attempt to reassign the COM600 computer from unassigned computers group to the COM600 Computer group created. See 5.4, Configuring WSUS for more information on how to create COM600 Computer group in WSUS server. When updates are approved

later on for a computer group, all COM600 device under a group would automatically receive approved updates.

To change group membership from **Unassigned Computers** to **COM600 Computer Group**, right click the COM600 item and select **Change Membership**,as shown in Figure 5.10-1. In the subsequent **Set Computer Group Membership** dialog select the desired COM600 Computer group and click **OK**.



Reassign_Computer_Group_for_COM600.png

Figure 5.10-1 Reassign Computer Group for COM600

Approving Updates in WSUS

The Update Services console in WSUS server will load all latest available updates from Microsoft after being synchronized.

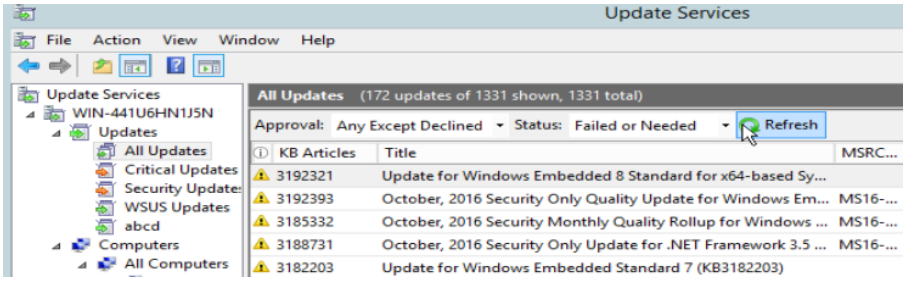
To synchronize WSUS server:

1. Click **WSUS server name** in **Update Services** console to open the **Overview** page in the console.
2. Click **Synchronize Now** to initiate Synchronization (see Figure 5.4-2).

To view all latest updates available, go to **Updates > All Updates**. The console view with all available updates is opened.

To view only relevant updates:

1. Select **Any Except Declined for Approval**.
2. Select **Failed or Needed for Approval**.
3. Click **Refresh** as shown in Figure 5.11-1.

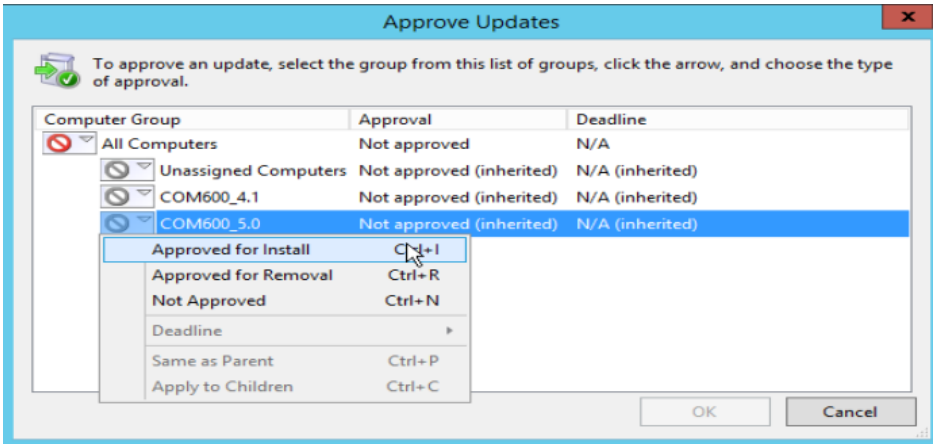


View_needed_updates_in_Update_Services_console.png

Figure 5.11-1 View needed updates in Update Services console

To approve each of the needed updates, right click on an update and select **Approve**. The **Approve Updates** dialog open (see Figure 5.11-2). Select the desired **COM600 Computer Group** and click **Approved for Install**. The update is downloaded from Microsoft Update Server and made available to COM600 device for further download and installation.

Before approving updates double check the COM600 patch management report for any recommendation to install/not to install a particular update for COM600 application compatibility.



Approve_Updates_Dialog.png

Figure 5.11-2 Approve Updates Dialog

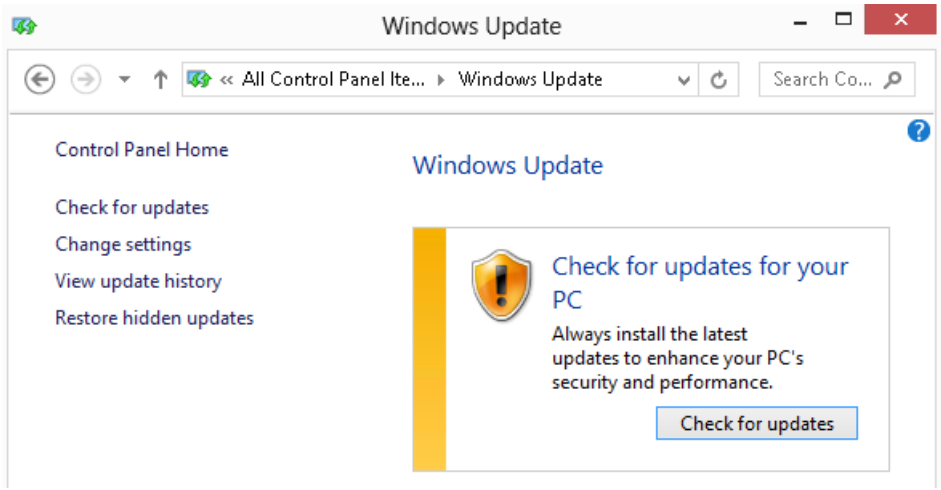
Installing Approved Updates in COM600

Approved updates from WSUS server are installed in COM600 by using typical Windows update process in COM600.

To install updates manually in COM600:

1. Log in to COM600 with administrative priviledges.

2. Open **Control Panel** > **Windows Update**.
3. Then click **Check for Updates** to install approved updates available from WSUS server.

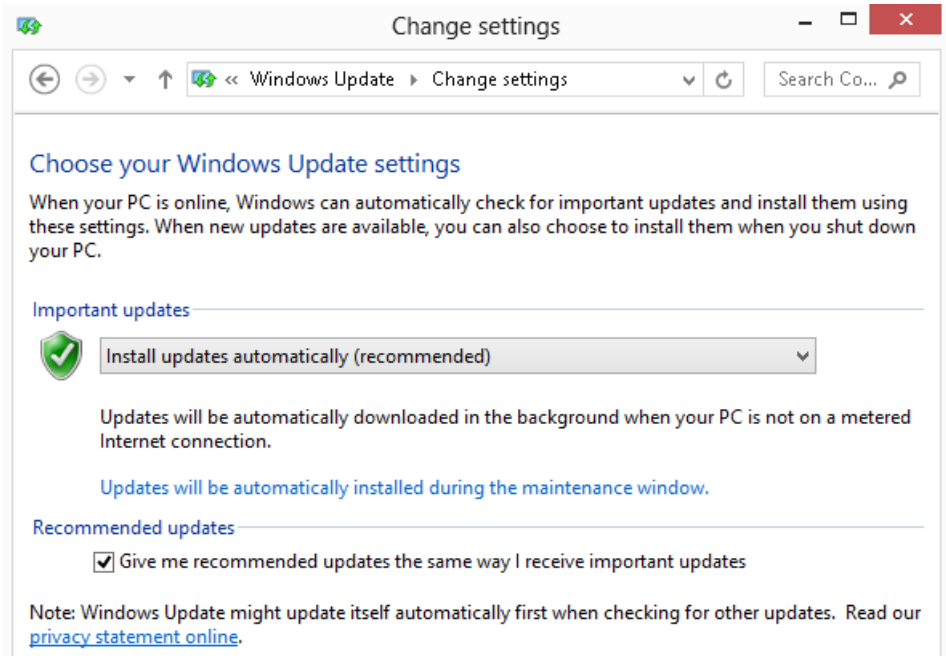


Install_updates_in_COM600.png

Figure 5.12-1 Install updates in COM600

To configure COM600 to install updates automatically:

1. Log in to COM600 with administrative privileges.
2. Go to **Control Panel** and click **Windows Update**.
3. Click **Change Settings**.
4. In the subsequent window, go to **Important Updates** > **Install updates automatically** and click the check box for **Give me recommended updates the same way I receive important updates**.
5. Click **Updates will be automatically installed during the maintenance window** and select an appropriate time during which the updates will be downloaded and installed from COM600.



COM600_Windows_Update_Change_Settings.png

Figure 5.12-2 COM600 Windows Update Change Settings

ABB Distribution Solutions
Distribution Automation
P.O. Box 699
FI-65101 Vaasa, Finland
Phone: +358 10 22 11

ABB Distribution Automation
4300 Coral Ridge Drive
Coral Springs, Florida 33065
Phone: +1 954 752 6700

www.abb.com/mediumvoltage
www.abb.com/substationautomation