Security Best Practices Checklists for Building Automation Systems (BAS)

Rev. 12/5/2018

Contents

Security checklist for a server/PC-installed Building Automation system (BAS)

Designing and Planning

- ☐ Separate user and BACnet networks either physically or with a VLAN.
- ☐ Discuss with your system installer the appropriate following internet connection scenarios and associated risks for your system.

Installing

If you have dual NICs:

- ☐ Enter the network IP address and subnet mask for users to log into the BAS server in SiteBuilder on the **Configure** > **Preferences** > **Web Server** tab.
- ☐ Enter the BAS BACnet network IP address and subnet mask in the BAS user interface on the **Connections** page > **Configure** tab.

If using an isolated network with no internet connectivity:

- ☐ Verify that IP addresses for the BAS server and controllers are in one of the private IP address ranges.

If using internet connectivity for public users to your BAS server:

- ☐ Verify that controller IP addresses are in one of the private IP address ranges.
- ☐ Verify that the NAT router or firewall exposing the BAS server only exposes TCP ports 80 and/or 443.

If using internet connectivity for public users to the BAS server and distributed BACnet devices:

- ☐ Verify that the NAT router or firewall exposing the BAS server only exposes TCP ports 80 and/or 443, and UDP port 47808.
- ☐ Verify that each NAT router or firewall used (for both the server and each controller) has been configured with an appropriate whitelist of allowed IP addresses in your internet connection device, or each controller is protected by its internal BACnet firewall feature.
- ☐ Test the whitelist protection from the internet. Use a separate BAS server on a public network by using a modstat like "modstat mac:0,b:1.2.3.4". Confirm you cannot access any of the system's controllers.
- ☐ Change the Administrator login name and password.
- ☐ Remove any anonymous user accounts.
- ☐ Verify that the BAS server's anti-virus software is up-to-date and is set to update automatically.
- ☐ Configure the database server to accept connections only from the BAS application using a whitelist.

After Commissioning

- ☐ **Disable Local Access to Server and Tools** is checked on the controller's **Properties** page. You can use Global modify to change this for all controllers simultaneously.
- ☐ Enable the Advanced password policy and set the minimum password length to at least 8 characters.

On the **System Settings** > **Security** tab, verify that:

- ☐ **Allow remote file management** is not checked
- ☐ **Log off operators after __ (HH:MM) of inactivity** is checked
- ☐ **Lock out operators for __ minutes after __ failed login attempts** is checked

System Maintenance

- ☐ Install the latest software updates to keep the system current with the most recent security enhancements.

Security checklist for Carrier Standard/Plus system

Designing and Planning

- ☐ Discuss with your system installer the appropriate following internet connection scenarios and associated risks for your system.

If using an isolated network with no internet connectivity:

- ☐ Verify that IP addresses for the Standard/Plus server and controllers are in one of the private IP address ranges.

If using internet connectivity for public users to your Standard/Plus server:

- ☐ Verify that controller IP addresses are in one of the private IP address ranges.
- ☐ Verify that the NAT router or firewall exposing the Standard/Plus server only exposes TCP ports 80 and/or 443.

If using internet connectivity for public users with distributed BACnet devices:

- ☐ Verify that the NAT router or firewall exposing the Standard/Plus server only exposes TCP ports 80 and/or 443, and UDP port 47808.
- ☐ Verify that each NAT router or firewall used (for both the server and each controller) has been configured with an appropriate whitelist of allowed IP addresses or each controller is protected by its internal BACnet firewall feature.
- ☐ Test the whitelist from a separate Standard/Plus server on a public network by using a modstat like "modstat mac:0,b:1.2.3.4". Confirm you cannot access any of the system's controllers.
- ☐ Change the Installer login name and password.

After Commissioning

- ☐ On the **System Options** > **Security** tab, enable the Advanced password policy and set the minimum password length to at least 8 characters.

On the **System Options** > **Security** tab, verify that:

- ☐ **Log off operators after __ (HH:MM) of inactivity** is checked
- ☐ **Lock out operators for __ minutes after __ failed login attempts** is checked

System Maintenance

- ☐ Install the latest software updates to keep the system current with the most recent security enhancements.