

Clarification Request

References: "ASHRAE 135.1-2007"

Background / Proposed Solution:

While the 135.1 test, 8.24.2 'Indefinite Duration, Disable, Password' and 8.24.3 'Time Duration, Disable, Password' require "password of at least 5 characters", the test 8.24.7 'Time Duration, Disable-Initiation, Password' require "password of up to 20 characters".

8.24.2 and 8.24.3 (8.24.7) seem not to have max (lowest) acceptance number of characters for password.

Question:

Should all the passwords not be "password of at least 5 characters and up to 20 characters | (5characters \leq password \leq 20characters)"?

Response:

There is no requirement within the ASHRAE 135 standard that a password must be a minimum of 5 characters. The tests will be modified to remove this requirement. The proposed test changes are noted below:

8.24 DeviceCommunicationControl Service Initiation Tests

8.24.1 Indefinite Duration, Disable, No Password

Reason For Change: This test was modified to include the responding ACK.

Purpose: To verify that the IUT can initiate DeviceCommunicationControl service requests that indicate communication should cease for an indefinite time duration and do not convey a password.

Test Steps:

1. RECEIVE DeviceCommunicationControl-Request,
'Enable/Disable' = DISABLE,
2. TRANSMIT BACnet-SimpleACK-PDU

8.24.2 Indefinite Duration, Disable, Password

Reason For Change: This test was modified to remove the requirement of a minimum password length of 5 but include the requirement of up to 20 characters.

Purpose: To verify that the IUT can initiate DeviceCommunicationControl service requests that indicate communication should cease for an indefinite time duration and convey a password.

Test Steps:

1. RECEIVE DeviceCommunicationControl-Request,
 'Enable/Disable' = DISABLE,
 'Password' = ~~(a password of at least 5 characters)~~ (a password of up to 20 characters)
2. TRANSMIT BACnet-SimpleACK-PDU

8.24.3 Time Duration, Disable, Password

Reason For Change: This test was modified to remove the requirement of a minimum password length of 5 but include the requirement of up to 20 characters.

Purpose: To verify that the IUT can initiate DeviceCommunicationControl service requests that indicate communication should cease for a specific time duration and convey a password.

Test Steps:

1. RECEIVE DeviceCommunicationControl-Request,
 'Time Duration' = (any unsigned value > 0),
 'Enable/Disable' = DISABLE,
 'Password' = ~~(a password of at least 5 characters)~~ (a password of up to 20 characters)
2. TRANSMIT BACnet-SimpleACK-PDU

8.24.4 Enable, Password

Reason For Change: This test was modified to remove the requirement of a minimum password length of 5 but include the requirement of up to 20 characters.

Purpose: To verify that the IUT can initiate DeviceCommunicationControl service requests that indicate communication should resume and convey a password.

Test Steps:

1. RECEIVE DeviceCommunicationControl-Request,
 'Enable/Disable' = ENABLE,
 'Password' = ~~(a password of at least 5 characters)~~ (a password of up to 20 characters)
2. TRANSMIT BACnet-SimpleACK-PDU

8.24.5 Enable, No Password

Reason For Change: This test was modified to include the responding ACK.

Purpose: To verify that the IUT can initiate DeviceCommunicationControl service requests that indicate communication should resume and do not convey a password.

Test Steps:

1. RECEIVE DeviceCommunicationControl-Request,
 'Enable/Disable' = ENABLE,
2. TRANSMIT BACnet-SimpleACK-PDU

8.24.6 Time Duration, Disable, No Password

Reason For Change: This test was modified to include the responding ACK.

Purpose: To verify that the IUT can initiate DeviceCommunicationControl service requests that indicate communication should cease for a specific time duration and do not convey a password. If the IUT does not support the “no password” option, this test shall not be performed.

Test Steps:

1. RECEIVE DeviceCommunicationControl-Request,
 'Time Duration' = (any unsigned value > 0),
 'Enable/Disable' = DISABLE
2. TRANSMIT BACnet-SimpleACK-PDU

8.24.7 Time Duration, Disable-Initiation, Password

Reason For Change: This test was modified to remove the requirement of a minimum password length of 5 but include the requirement of up to 20 characters.

Purpose: To verify that the IUT can initiate DeviceCommunicationControl service requests that indicate communication should cease for a specific time duration and that convey a password.

Test Steps:

1. RECEIVE DeviceCommunicationControl-Request,
 'Time Duration' = (any unsigned value in the range from 1 to 65535),
 'Enable/Disable' = DISABLE
 'Password' = (a password of up to 20 characters)
2. TRANSMIT BACnet-SimpleACK-PDU

8.27.2 COLDSTART with a Password

Reason For Change: This test was modified to remove the requirement of a minimum password length of 5 but include the requirement of up to 20 characters.

Purpose: To verify that the IUT can initiate ReinitializeDevice service requests that indicate a COLDSTART should be performed and convey a password.

Test Steps:

1. RECEIVE ReinitializeDevice-Request,
 'Reinitialized State of Device' = COLDSTART,
 'Password' = ~~(a password of at least 5 characters)~~ (a password of up to 20 characters)
2. TRANSMIT BACnet-SimpleACK-PDU

8.27.4 WARMSTART with a Password

Reason For Change: This test was modified to remove the requirement of a minimum password length of 5 but include the requirement of up to 20 characters.

Purpose: To verify that the IUT can initiate ReinitializeDevice service requests that indicate a WARMSTART should be performed and convey a password.

Test Steps:

1. RECEIVE ReinitializeDevice-Request,
 'Reinitialized State of Device' = WARMSTART,
 'Password' = ~~(a password of at least 5 characters)~~ (a password of up to 20 characters)

2. TRANSMIT BACnet-SimpleACK-PDU