PLATAFORMA DE CONTROL DE ACCESO Y HORARIO DE ASISTENCIA SUPREMA - BioStar 2

ESPECIFICACIONES TÉCNICAS

22/12/17

ABREVIATURAS

AC Control de acceso

AES Estándar de cifrado avanzado

AoC Tarjeta de acceso

APB Anti retorno

Auth Autenticación

DB Base de datos

DHCP Protocolo de configuración dinámica de host

HTTPS Protocolo de transferencia de hipertexto sobre conexión segura

PIN Número de identificación personal

SHA Algoritmo de hash seguro

TA Horario de asistencia

VE Evento de video

PARTE 1 - ASPECTOS GENERALES

El propósito de este documento es especificar los estándares mínimos para el diseño, suministro, instalación y puesta en funcionamiento de BioStar 2, que es una plataforma de seguridad basada en la web.

1.01. RESUMEN

A. La sección incluye los requisitos de la plataforma de seguridad basada en la web

B. Producto: se trata de una plataforma de seguridad basada en la web, capaz de administrar el sistema de control de acceso, administrar el sistema de horarios de asistencia y grabar registros de video con conectividad de red Ethernet.

1.02. PRESENTACIONES

1.03. CERTIFICACIONES

A. Toda la instalación, configuración y montaje de la plataforma debe ser realizado por técnicos calificados.

B. El fabricante debe capacitar a los instaladores para instalar, configurar y poner en funcionamiento el sistema de control de acceso y horarios de asistencia.

FIN DE LA SECCIÓN

PARTE 2 - PRODUCTOS

2.01. FABRICANTE

A. Suprema Inc.
17F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi, 463-863, República de Corea
Teléfono: 82-31-783-4502, Fax: 82-31-783-4503, www.supremainc.com
support@supremainc.com

B. Esta especificación se basa en BioStar 2.5.0, fabricado por Suprema Inc.

2.02. REQUISITOS DEL SISTEMA

A. Control de acceso y horarios de asistencia

1. Servidor para negocios pequeños
   a. Total de usuarios: 500
   b. Total de dispositivos: 50
   c. Equipo
      1) CPU de doble núcleo de 2 GHz
      2) 6 GB de RAM
      3) 500 GB de espacio libre en el disco
   d. Sistema operativo
      1) Windows 7 Home Basic de 64 bits o posterior
      2) Windows 7 Home Basic de 32 bits SP1 o posterior
   e. Base de datos
      1) MariaDB 10.1.10
      2) MS SQL Server 2012
      3) MS SQL Server 2012 Express
      4) MS SQL Server 2014
      5) MS SQL Server 2014 Express
2. Servidor para negocios medianos
   a. Total de usuarios: 5000
   b. Total de dispositivos: 100
   c. Equipo
      1) CPU de cuatro núcleos de 4 GHz
      2) 10 GB de RAM
      3) 1 TB de espacio libre en el disco
   d. Sistema operativo
      1) Windows Server 2008 R2 Standard de 64 bits SP2 o posterior
      2) Windows 7 Home Premium de 64 bits SP1 o superior
   e. Base de datos
      1) MariaDB 10.1.10
      2) MS SQL Server 2012
      3) MS SQL Server 2012 Express
      4) MS SQL Server 2014
      5) MS SQL Server 2014 Express

3. Servidor para negocios medianos
    a. Total de usuarios: 10000
    b. Total de dispositivos: 1000
    c. Equipo
        1) CPU de cuatro núcleos de 4 GHz
        2) 16 GB de RAM
        3) 4 TB de espacio libre en el disco
    d. Sistema operativo
        1) Windows Server 2008 R2 Standard de 64 bits SP2 o posterior
        2) Windows 7 Home Premium de 64 bits SP1 o superior
    e. Base de datos
        1) MariaDB 10.1.10

B. Registro de video
    a. Equipo (mínimo)
        1) CPU de cuatro núcleos de 4 GHz
        2) 8 GB de RAM
        3) 2 TB de espacio libre en el disco
    b. Equipo (recomendado)
        1) CPU de cuatro núcleos de 4 GHz
        2) 16 GB de RAM
        3) 4 TB de espacio libre en el disco

C. Cliente
    a. Equipo
        1) CEP de 1 GHz
        2) 4 GB de RAM
    b. Navegador web
        1) Google Chrome 49 o posterior

2.03. ESTÁNDARES DE RENDIMIENTO

A. Arquitectura del sistema

1. Una plataforma de seguridad basada en la web, capaz de administrar el sistema de control de acceso, administrar el sistema de horarios de asistencia y grabar registros de video con conectividad de red Ethernet.
    a. Control de acceso
        1) Administración de usuarios
        2) Administración de dispositivos
        3) Administración de las puertas
        4) Administración del ascensor
        5) Administración de zona (Anti retorno, alarma de incendios, programación de bloqueo y desbloqueo, alarma de intrusión)
        6) Administración de grupos de acceso
        7) Monitoreo (registro de eventos, registro en tiempo real, estado del dispositivo, estado de las puertas, estado de los pisos, estado de las zonas, registro de imágenes e historial de alertas)

8) Administración de alarmas
9) Administración de tarjetas RFID
10) Registro de auditoría

b. Horario de asistencia
1) Administración de código de horario
2) Administración de turnos
3) Administración de plantillas de programas
4) Administración de reglas de horas extra
5) Administración de programas
6) Administración de salida
7) Monitoreo (salida y excepción)
8) Generación de informes de horarios de asistencia

c. Registro de video

2. Protocolo de comunicación en red del Protocolo de control de transmisión estándar (TCP/IP) entre el servidor, los clientes y los dispositivos.
3. Compatible con el Protocolo de configuración dinámica de host (DHCP) o la dirección IP estática.
4. Compatible con la configuración en red.
5. Compatible con el Protocolo de hora en red (NTP).
6. Compatible con la comunicación HTTPS protegida por la Capa de conexión segura (SSL) entre el cliente (navegador web) y la plataforma.
7. Compatible con AES-256 para el nombre de usuario, plantilla de huella dactilar y plantilla de rostro.
8. Compatible con SHA-256 para PIN y contraseña.
9. Compatible con la exportación a SVG o PDF para los elementos de la lista.

B. Asistente de instalación

1. Paquete de instalación independiente.
2. Admite inglés y coreano.
3. Permite que un usuario realice la configuración inicial.
a. Establece la contraseña para la cuenta de administrador.
b. Selecciona la instalación de la base de datos (MariaDB 10.1.10 o personalizada).
c. Establece la contraseña raíz para MariaDB.
d. Establecerá la información de la base de datos personalizada, incluidas la IP del servidor, el puerto del servidor, el nombre de la base de batos del control de acceso, la información de inicio de sesión de la base de datos del control de acceso, la información de inicio de sesión de la base de datos del horario de asistencia, el nombre de la base de datos del horario de asistencia, la información de inicio de sesión de la base de datos de eventos de video y el nombre de la base de datos de eventos de video.
e. Comprueba la conexión de la base de datos.
f. Genera las tablas de la base de datos.
g. Cambia el número de puerto para el servidor.
h. Debe instalar el agente de dispositivo USB para BioMini y DUALi DE-620.

C. Capacidad del sistema y licencia

1. Licencia básica

a. Control de acceso
    1) Para usuarios ilimitados (* según el tamaño de la base de datos).
    2) Para las plantillas de huellas dactilares ilimitadas (* según el tamaño de la base de datos).
    3) Para las plantillas de rostro ilimitadas (* según el tamaño de la base de datos).
    4) Para las tarjetas ilimitadas (* según el tamaño de la base de datos).
    5) Para un máximo de 31 dispositivos esclavos RFID por dispositivo maestro.
    6) Para un máximo de 8 dispositivos esclavos de huellas dactilares por dispositivo maestro.
    7) Para un máximo de 128 niveles de acceso.
    8) Para un máximo de 128 puertas por nivel de acceso.
    9) Para un máximo de 128 grupos de acceso.
    10) Para un máximo de 16 grupos de acceso por usuario.
    11) Para un máximo de 1000 dispositivos.
    12) Para un máximo de 1000 puertas.
    13) Para un máximo de 1000 zonas.
    14) Para un máximo de 8 tarjetas por usuario.
    15) Para un máximo de 10 plantillas de huellas dactilares por usuario.
b. Horario de asistencia
    1) Para el turno ilimitado (* según el tamaño de la base de datos).
    2) Para un programa.
    3) Para un máximo de 99 usuarios por programa.
    4) Para las salidas ilimitadas por usuario.

2. Licencia estándar de control de acceso
    a. Incluye licencia básica:
        1) Para un máximo de 192 pisos por ascensor.
        2) Para un máximo de 4 lectores por ascensor.
        3) Para un máximo de 100 zonas.
        4) Para un máximo de 1000 dispositivos por zona global.
        5) Para un máximo de 32 dispositivos por zona local.
3. Licencia estándar de horario de asistencia (incluye la licencia básica)
    a. Incluye licencia básica:
        1) Para programas ilimitados.
        2) Para usuarios ilimitados por programa.

D. Interfaz

1. Utiliza una interfaz de usuario del cliente basada en la web para la configuración, administración, gestión y monitoreo.
2. Compatible con la interfaz de usuario multilingüe
    a. Inglés y coreano disponibles.
    b. Otros idiomas disponibles mediante el paquete de idiomas del sitio web. (Los idiomas admitidos pueden variar según la versión de BioStar 2)
        1) Alemán
        2) Español
        3) Francés
        4) Italiano

5) Japonés
6) Holandés
7) Portugués
8) Chino simplificado
9) Chino tradicional
10) Ruso
11) Ucraniano

E. Usuario

1. ID de usuario
   a. Compatible con la ID de usuario numérica.
   b. Compatible con la ID de usuario alfanumérica.
2. Admite fechas de vencimiento (período) para el usuario.
3. Niveles de operador
   a. Para un máximo de 6 niveles predefinidos.
   b. Para un máximo de 32 niveles de operador personalizados.
   c. Cada nivel debe tener un conjunto de permisos y debe ser capaz de configurarse para diferentes niveles de operador.
4. Campo personalizado
   a. Proporciona 3 tipos de campos de usuario personalizados.
      1) Compatible con el cuadro de entrada de texto, cuadro de entrada de número y cuadro combinado
   b. Para un máximo de 20 campos personalizados.
5. Huella digital
   a. Compatible con hasta 10 dedos (20 plantillas) por usuario.
   b. Compatible con 3 tipos de formato de plantilla de huella dactilar (SUPREMA/ISO 19794-2/ANSI 378).
6. Rostro
   a. Admite hasta 5 rostros (10 plantillas) por usuario.
7. Tarjeta Wiegand
   a. Para un máximo de 15 formatos, incluidos 5 formatos predefinidos.
   b. Compatible con formatos de tarjeta con bits totales, código de instalación, campos de ID personalizables y bits de paridad.
   c. Para un máximo de 5 formatos predefinidos.
      1) Estándar SIA de 26 bits (H10301)
      2) HID de 37 bits (H10302)
      3) HID de 37 bits (H10304)
      4) HID Corporate 1000
      5) HID Corporate 1000 de 48 bits
8. Tarjeta inteligente
   a. Compatible con 3 tipos de diseño de tarjeta inteligente y tarjeta móvil.
      1) MIFARE, iCLASS, DESFire y móvil
   b. Almacena hasta 4 plantillas de huellas dactilares en la tarjeta inteligente. (Tarjeta de acceso)
9. Importar y exportar información del usuario a través de un archivo CSV

a. Compatible con la importación y exportación de datos en formato de archivo de valores separados por comas (CSV).
b. Compatible con varios idiomas.
c. Permite al usuario importar y exportar la información del usuario y la información de la tarjeta en el archivo CSV.
d. Compatible con la asignación automática y manual de campos CSV a los campos de la base de datos.

10. Compatible con la administración de usuarios inactivos a largo plazo.

F. Dispositivo

1. Compatible con la búsqueda automática y manual de un dispositivo.
2. Permite al usuario cambiar la configuración del dispositivo y realizar la acción, lo que incluye:
   a. Actualización del firmware
   b. Restablecimiento a los valores de fábrica
   c. Bloqueo/Desbloqueo
   d. Zona horaria
   e. Sincronización de hora
   f. Configuración de red
   g. Configuración de serie (RS-485)
   h. Configuración de autenticación
   i. Configuración del formato de la tarjeta
   j. Activación y acción
   k. Configuración de horario de asistencia
   l. Nivel de administrador
   m. Configuración de pantalla y sonido
   n. Configuración de Wiegand
   o. Sincronización automática con el servidor

G. Puerta

1. La configuración de la puerta admitida incluye:
   a. Dos dispositivos (dispositivo de entrada y de salida) para una puerta
   b. Dispositivo de entrada para una puerta con botón de salida
   c. Dispositivo de entrada para una puerta sin botón de salida
2. Admite dos tipos de ajuste de relé para el botón de salida y el sensor de puerta.
   a. Normalmente abierto y normalmente cerrado
3. Permite al usuario configurar los ajustes de la puerta, lo que incluye:
   a. Selección de dispositivo de entrada
   b. Selección de relé para el bloqueo de una puerta
   c. Puerto de entrada TTL para un botón de salida
   d. Puerto de entrada TTL para un sensor de puerta
   e. Tiempo de liberación del relé para el bloqueo de la puerta
   f. Configuración de autenticación doble
   g. Tiempo para mantener abierta y alarma
   h. Alarma de apertura forzada
   i. Alarma anti retorno

H. Ascensor

1. Compatible con el control de botón de piso.
2. Compatible con la asignación automática y manual de nombres de piso a los números de relé.
3. Permite al usuario configurar el control del piso, lo que incluye:
   a. Selección del controlador
   b. Selección del lector
   c. Selección del módulo
   d. Número total de pisos
   e. Tiempo de liberación del relé para el botón del piso
   f. Configuración de autenticación doble
   g. Configuración del puerto de seguridad
   h. Configuración de la alarma
   i. Activación y acción

I. Zona

1. Anti retorno
   a. El usuario puede definir las áreas y asignar los dispositivos de entrada y de salida para configurar una zona anti retorno.
   b. Compatible con la zona APB global que se puede configurar con todos los dispositivos inscritos en BioStar 2.
   c. Compatible con la zona APB local que se puede configurar con los dispositivos de entrada y de salida conectados con RS-485.
   d. Permite al usuario configurar una zona anti retorno, lo que incluye:
      1) Modo de zona APB (global o local)
      2) Establecer modo activo o inactivo temporalmente
      3) Tipo de APB (hardware o software de APB)
      4) Tiempo de restablecimiento automático
      5) Selección de dispositivos de entrada y salida para la zona APB
      6) Acción de falla de la red
      7) Salida de señal personalizable para la alarma
      8) Omitir la configuración de grupos de usuarios
2. Alarma de incendios
   a. El usuario puede definir las áreas y asignar las puertas o ascensores para configurar una zona de alarma de incendios.
   b. Compatible con la zona de alarma de incendios global que se puede configurar con todos los dispositivos inscritos en BioStar 2.
   c. Compatible con la zona de alarma de incendios local que se puede configurar con los dispositivos de entrada y salida conectados con RS-485.
   d. Permite al usuario configurar una zona de alarma de incendios, lo que incluye:
      1) Modo de zona de la alarma de incendios (global o local)
      2) Establecer modo activo o inactivo temporalmente
      3) Selección de la puerta o elevador para la zona de la alarma de incendios
      4) Salida de señal personalizable para la alarma
3. Bloqueo programado
   a. El usuario puede definir las áreas y asignar las puertas y programas para configurar una zona

de bloqueo programado.

b. Permite al usuario configurar una zona de bloqueo programado, lo que incluye:
    1) Establecer modo activo o inactivo temporalmente
    2) Selección del método de bloqueo de puerta
    3) Selección de la programación y la puerta para la zona de bloqueo programado
    4) Salida de señal personalizable para la alarma
    5) Omitir la configuración de grupos de usuarios

4. Desbloqueo programado
    a. El usuario puede definir las áreas y asignar las puertas y programas para configurar una zona de desbloqueo programado.
    b. Permite al usuario configurar una zona de desbloqueo programado, lo que incluye:
        1) Establecer modo activo o inactivo temporalmente
        2) Iniciado por la opción de autenticación del usuario
        3) Selección de la programación y la puerta para la zona de desbloqueo programado
        4) Grupo de acceso al que pertenece el usuario, quien puede iniciar un desbloqueo programado

5. Alarma de intrusión
    a. El usuario puede definir las áreas y asignar las puertas para configurar una zona de alarma de intrusión.
    b. Compatible con la zona de alarma de intrusión global que se puede configurar con todos los dispositivos inscritos en BioStar 2.
    c. Compatible con la zona de alarma de intrusión local que se puede configurar con los dispositivos de entrada y salida conectados con RS-485.
    d. Permite al usuario configurar una zona de alarma de intrusión, lo que incluye:
        1) Modo de zona de alarma de intrusión (global o local)
        2) Establecer modo activo o inactivo temporalmente
        3) Selección de puerta para detectar la intrusión
        4) Configuraciones de armado o desarmado
        5) Salida de señal personalizable para detectar la alarma de intrusión
        6) Salida de señal personalizable cuando se produce un evento especificado

J. Control de acceso

1. Proporciona el estado de permiso de acceso mediante cuatro filtros predefinidos.
    a. Permiso de puerta por puerta
    b. Permiso de puerta por usuario
    c. Permiso de ascensor por piso
    d. Permiso de ascensor por usuario

2. Nivel de acceso
    a. Admite que el usuario cree un nivel de acceso que se combina con las puertas y los programas.

3. Nivel de piso
    a. Admite que el usuario cree un nivel de piso que se combina con los ascensores, los nombres de pisos y los programas.

4. Grupo de acceso
    a. Admite que el usuario cree un grupo de acceso para el permiso de acceso de la puerta que se combina con los niveles de acceso y los grupos de usuarios o usuarios individuales.

b. Admite que el usuario cree un grupo de acceso para el permiso de acceso del piso que se combina con los niveles de piso y grupos de usuarios o usuarios individuales.

K. Monitoreo

1. Proporciona exportación de la lista de eventos de control de acceso a un archivo CSV.
2. Compatible con la funcionalidad de filtro para ordenar.
3. Proporciona todas las funciones de monitoreo del sistema de control de acceso, incluidas las siguientes:
   a. Registro de eventos
   b. Registro en tiempo real
   c. Estado del dispositivo
   d. Estado de la puerta
   e. Estado del piso
   f. Estado de la zona
   g. Historial de alertas
4. Proporciona las siguientes operaciones para la puerta seleccionada en el Estado del dispositivo.
   a. Bloquear la puerta manualmente
   b. Desbloquear la puerta manualmente
   c. Liberar el bloqueo o desbloqueo manual
   d. Abrir la puerta temporalmente
   e. Borrar todas las alarmas de la puerta
   f. Borrar la alarma APB
5. Proporciona las siguientes operaciones para el piso seleccionado en el Estado del piso.
   a. Bloquear el piso manualmente
   b. Desbloquear el piso manualmente
   c. Liberar el bloqueo o desbloqueo manual
   d. Abrir el piso temporalmente
   e. Borrar todas las alarmas del piso
6. Proporciona las siguientes operaciones para la zona seleccionada en el Estado de zona.
   a. Borrar la alarma APB
   b. Borrar todas las alarmas

L. Video

1. Grabar el video cuando se produce un evento de control de acceso especificado en la puerta.
2. Admite que el usuario cambie la ruta del archivo de video.
3. Admite que el usuario cambie las semanas que se mantienen los archivos grabados.
4. Compatible con la configuración NVR y la configuración del IP de cámara.
5. La compatibilidad con los fabricantes NVR incluye:
   a. ACTi
   b. Dahua
   c. Hikvision

M. Horario de asistencia

1. Admite que el usuario configure una regla de horarios de asistencia y rastree los registros de los

mismos, incluso lo siguiente:

a. Código de horarios
b. Turno
c. Plantilla de programa
d. Regla
e. Programa
f. Informe de horario de asistencia

2. El informe de horario de asistencia incluye 7 tipos de informes predefinidos que el usuario puede personalizar de la siguiente manera:
   a. Diariamente
   b. Resumen diario
   c. Individual
   d. Resumen individual
   e. Salida
   f. Excepción
   g. Historial del registro de ingreso modificado
3. Compatible con la funcionalidad del filtro para el informe de horario de asistencia personalizado.
4. Admite que el usuario exporte los informes de horario de asistencia como archivos en formato CSV o PDF.
5. Admite que el usuario modifique los registros de horario de asistencia.

N. Alerta del sistema

1. Proporciona al usuario 28 eventos para la alerta del sistema, lo que incluye:
   a. Desconexión del dispositivo detectado
   b. Reinicia el dispositivo
   c. Desconectar RS-485
   d. Seguridad activada
   e. Entrada supervisada (corta)
   f. Entrada supervisada (abierta)
   g. Falla de la alimentación de control de acceso
   h. Puerta forzada abierta
   i. Mantener la puerta abierta
   j. Puerta forzada abierta con alarma
   k. Puerta que se mantiene abierta con alarma
   l. Habilitar todos los relés de piso
   m. Alarma de zona anti retorno detectada
   n. Alarma de zona de la alarma de incendios detectada
   o. Alarma de zona de bloqueo programado detectada
   p. Alarma de intrusión detectada
   q. Error de autenticación 1:1
   r. Autenticación de coacción exitosa 1:1
   s. Error de autenticación 1:N
   t. Autenticación de coacción exitosa 1:N
   u. Acceso denegado (grupo de acceso no válido)

v. Acceso denegado (usuario deshabilitado)
w. Acceso denegado (caducado)
x. Acceso denegado (lista negra)
y. Acceso denegado (anti retorno físico)
z. Acceso denegado (programación de bloqueo forzado)
aa. Acceso denegado (software de anti retorno)
bb. Huella dactilar falsa detectada

O. Registro de auditoría

1. Proporciona los 2 filtros predefinidos
   a. Último mes
   b. Últimos 3 meses
2. Admite que el usuario cree un filtro con cada elemento del campo, lo que incluye:
   a. Fecha y hora
   b. Nombre de usuario
   c. Nivel del operador
   d. Dirección IP
   e. Categoría
   f. Objetivo
   g. Acción
   h. Modificación

FIN DE LA SECCIÓN

PARTE 3 - PLAN DE ACCIÓN

3.01. INSTALADOR

A. El personal del contratista debe cumplir con todos los requisitos de licencia locales y estatales que corresponda.

B. Requisitos del instalador y del técnico

1. Deben contar con experiencia y estar calificados para realizar el trabajo en forma oportuna.

3.02. PREPARACIÓN

A. El direccionamiento IP se debe coordinar con el personal de TI responsable del propietario.

3.03. INSTALACIÓN

A. La señal de control, las comunicaciones y la conexión a tierra de la línea de transmisión de datos se deben instalar según sea necesario para evitar que los bucles de masa, ruidos y sobretensiones afecten negativamente la operación del sistema.

B. Siga cuidadosamente las instrucciones que se encuentran el manual de instalación del fabricante para asegurarse de que se hayan seguido todos los pasos para proporcionar un sistema confiable y fácil de operar.

3.04. PRUEBA

A. Todas las conexiones de red se deben probar para que funcionen con los niveles de rendimiento adecuados.

FIN DE LA SECCIÓN