



CRITICAL PRODUCT SECURITY INFORMATION FOR INSTALLERS, COMMISSIONING ENGINEERS AND USERS

VESDA-E ACCESSORIES

WARNING: Failure to comply with the requirements below exposes the system to malicious interference which could disable alarm reporting

Commissioning Requirements

- All VESDAnet wiring and connection ports must be secured against unauthorized access.
- Ethernet ports must ONLY be connected to networks which are secure and physically or logically separate from business IT infrastructure.
- VESDA-E Accessories and VESDA devices including HLIs must not be accessible from the Internet. Any provision of remote access to VESDA-E Accessories must be subjected to a full cyber security risk assessment and regular review.
- Passwords must be chosen in line with the guidelines in the detector user guide and provided to trusted users only.
- Default PIN codes must be changed as part of the initial configuration.
- Access to PCs on which Xtralis VSC or VSM configuration software and system configuration information are installed must be restricted to authorized persons if saved passwords are used.
- Xtralis PC software such as VSC or VSM, must only be installed on PCs with current active Windows support from Microsoft.
- Product should be checked prior to installation to determine if there are any broken seals which may indicate unauthorised tampering. If this is the case, please contact Xtralis for advice.
- VESDA-E Accessories access point uses UDP port 22094 for communicating through Ethernet. No other ports shall be enabled in firewall if used.

System Maintenance Requirements

- Do NOT use the USB port for long-term monitoring or allow it to be permanently wired to building infrastructure. It is only to be used for configuration and maintenance by authorized personnel.
- If Xtralis product requires firmware upgrade, ensure that the upgrade package is genuine and obtained directly from Xtralis.
- VESDA-E Accessory shall be reset to factory default before decommissioning the device using Xtralis VSC software.

WICHTIGER PRODUKTSICHERHEITSHINWEIS FÜR ERRICHTER, INBETRIEBNAHMETECHNIKER UND BENUTZER

VESDA-E ZUBEHÖR

WARNUNG: Die Nichteinhaltung der unten angeführten Richtlinien kann das System für schwerfällige Störungen anfällig machen, die zur Außerkraftsetzung der Warmmeldefunktion führen können

Richtlinien zur Inbetriebnahme

- Sämtliche Kabel und Anschlüsse von VESDNAnet sind gegen unbefugten Zugang zu schützen.
- Ethernet-Anschlüsse dürfen NUR mit sicheren Netzwerken verbunden werden, die physisch und logisch von der IT-Infrastruktur des Unternehmens getrennt sind.
- Der Zugriff auf VESDA-E-Zubehör und VESDA-Geräte, einschließlich HLIs, darf nicht vom Internet aus möglich sein. Einrichtungen zum Fernzugriff auf VESDA E-Zubehör sind einer vollständigen Netzwerksicherheitsanalyse und einer regelmäßigen Überprüfung zu unterziehen.
- Passwörter sind in Übereinstimmung mit den Richtlinien in der Benutzeranleitung der Rauchmelder festzulegen und nur vertrauenswürdigen Benutzern weiterzugeben.
- Standard-PIN-Codes müssen während der ersten Konfiguration geändert werden.
- Nur zertifiziertes Personal darf Zugriff auf PCs erhalten, auf denen Passwort geschützte Xtralis VSC oder VSM Konfigurationen installiert sind.
- Xtralis Software, wie z.B. VSC oder VSM sollten auf aktiven Windows, durch Microsoft unterstützt, PCs laufen.
- Vor der Installation überprüft werden, um festzustellen, ob es beschädigte Siegel gibt, die auf unbefugte Manipulationen hinweisen können. Wenn dies der Fall ist, wenden Sie sich bitte an Xtralis.
- Der Zugriffspunkt zum VESDA-E-Zubehör verwendet den UDP-Port 22094 für die Kommunikation über Ethernet. Wenn er verwendet wird, dürfen keine anderen Ports in der Firewall freigegeben werden.

Richtlinien zur Instandhaltung

- Der USB-Anschluss ist NICHT zur Langzeitüberwachung zu verwenden und darf nicht permanent mit der Gebäudeinfrastruktur verbunden sein. Er ist ausschließlich von autorisierten Personen zur Konfiguration und Wartung zu nutzen.
- Wenn ein Xtralis Produkt ein Upgrade erfordert, ist darauf zu achten, dass es sich um ein originales Upgrade-Paket handelt und dieses direkt von Xtralis bezogen wurde.
- Das VESDA-E-Zubehör muss vor der Inbetriebnahme des Geräts über die Xtralis VSC-Software auf Werkseinstellung zurückgesetzt werden.



INFORMACIÓN DE SEGURIDAD CRÍTICA DEL PRODUCTO PARA INSTALADORES, INGENIEROS INGENEROS DE COMISIOS Y USUARIOS

ACCESORIOS VESDA-E

ADVERTENCIA: el incumplimiento de los requisitos siguientes expondrá el sistema a acciones malintencionadas que podrían desactivar la notificación de alarmas

Requisitos de la puesta en funcionamiento

- Todos los puertos de conexión y cableados de VESDAnet deben protegerse contra accesos no autorizados.
- Los puertos de Ethernet SOLO deben conectarse a redes seguras y separadas física o lógicamente de infraestructuras informáticas de las empresas.
- No debe accederse a los accesorios VESDA-E y los dispositivos VESDA que incluyen HLI desde internet. Cualquier aplicación de acceso remoto a accesorios VESDA-E debe estar sujeta a una evaluación de riesgos de la seguridad informática y a una revisión regular.
- Las contraseñas deben elegirse en consonancia con las directrices de la guía del usuario del detector y solo deben proporcionarse a usuarios de confianza.
- Deben cambiarse los códigos PIN predeterminados como parte de la configuración inicial.
- El acceso a los ordenadores en los que se hayan instalado los programas VSC o VSM de Xtralis, deben ser restringidos a personal autorizado si se han usado identificaciones y sus contraseñas correspondientes.
- Los programas de Xtralis, tales como VSC o VSM, solo deben ser instalados en ordenadores con versiones de Windows soportadas por Microsoft y convenientemente actualizadas.
- El producto debe ser revisado antes de su instalación para determinar si hay algún recinto roto que pueda indicar una manipulación no autorizada. Si este es el caso, póngase en contacto con Xtralis para que le asesore.
- El punto de acceso de los accesorios VESDA-E utiliza un puerto UDP 22094 para comunicarse a través de Ethernet. No deben habilitarse más puertos en el cortafuegos, si se usa.

Requisitos de mantenimiento del sistema

- NO utilice el puerto USB para el seguimiento a largo plazo ni lo deje permanentemente conectado a la infraestructura del edificio. Solo debe utilizarse para la configuración y mantenimiento por parte del personal autorizado.
- Si el producto Xtralis requiere una actualización del firmware, asegúrese de que el paquete de actualización es original y se obtiene directamente de Xtralis.
- Los accesorios VESDA-E deben reiniciarse a los ajustes de fábrica antes de retirar el dispositivo con el software VSC de Xtralis.

INFORMATIONS ESSENTIELLES CONCERNANT LA ISÉCURITÉ DES PRODUITS POUR LES INSTALLATEURS, LES TECHNICIENS DE MISE EN SER- VICE ET LES UTILISATEURS

ACCESSOIRES VESDA-E

AVERTISSEMENT : Le non-respect des exigences ci-dessous expose le système à des actions malveillantes qui pourraient désactiver la signalisation d'alarme

Exigences relatives à la mise en service

- Tous les ports de connexion et borniers de câblage VESDAnet doivent être protégés contre tout accès non autorisé.
- Les ports Ethernet doivent UNIQUEMENT être connectés à des réseaux sécurisés physiquement ou logiquement séparés de l'infrastructure informatique de l'entreprise.
- Les accessoires VESDA-E et les appareils VESDA, HLI inclus, ne doivent pas être accessibles depuis Internet. Tout accès à distance aux accessoires VESDA-E doit faire l'objet d'une évaluation complète des risques de cybersécurité et à une révision régulière.
- Les mots de passe doivent être choisis conformément aux directives du manuel d'utilisation du détecteur et fournis uniquement aux utilisateurs qualifiés.
- Les codes PIN par défaut doivent être modifiés lors de la configuration initiale.
- L'accès aux ordinateurs sur lesquels le logiciel de configuration Xtralis VSC ou Xtralis VSM et les informations de configuration du système sont installés doit être réservé aux personnes autorisées si des mots de passe enregistrés sont utilisés.
- Le logiciel sur PC, tel que Xtralis VSC ou Xtralis VSM, ne doit être installé que sur les PC avec le support Windows actif actuel de Microsoft.
- Le produit doit être vérifié avant l'installation pour déterminer s'il y a des scellées brisées qui pourraient indiquer une altération non autorisée. Si tel est le cas, veuillez contacter votre représentant Xtralis.
- Le point d'accès aux accessoires VESDA-E utilise le port UDP 22094 pour communiquer par Ethernet. Aucun autre port ne doit être activé dans le pare-feu, le cas échéant.

Exigences relatives à la maintenance du système

- Le port USB n'est pas destiné à une surveillance permanente du système, et de ce fait, il ne doit pas être connecté de façon durable sur le réseau informatique de l'entreprise. Il ne doit être utilisé que lors de la configuration et de la maintenance par du personnel autorisé.
- Si le produit Xtralis nécessite une mise à jour du micrologiciel, assurez-vous que le kit de mise à niveau est obtenu directement auprès de Xtralis.
- Avant de mettre l'appareil hors service à l'aide du logiciel Xtralis VSC, l'accessoire VESDA-E doit être réinitialisé aux valeurs usine par défaut.

INFORMAZIONI ESSENZIALI SULLA SICUREZZA DEL PRODOTTO PER GLI INSTALLATORI, GLI ADDETTI ALLA MESSA IN SERVIZIO E GLI UTENTI

ACCESSORI VESDA-E

ATTENZIONE: il mancato rispetto dei requisiti descritti di seguito espone il sistema a interferenze nocive che potrebbero disabilitare la funzione di rapporto degli allarmi

Requisiti per la messa in servizio

- Impedire l'accesso non autorizzato a tutte le porte di collegamento e connessione VESDAnet.
- Connettere le porte Ethernet SOLO a reti sicure e separate fisicamente o logicamente dall'infrastruttura IT aziendale.
- L'accesso da Internet agli accessori VESDA-E e ai dispositivi VESDA, compresi gli HLI, non deve essere consentito. Sottoporre tutti i servizi di accesso remoto agli accessori VESDA-E a una valutazione completa dei rischi di sicurezza informatica e a verifiche periodiche.
- Scegliere le password rispettando le indicazioni del manuale utente del rilevatore e comunicarle solo al personale di fiducia.
- Nel corso della configurazione iniziale, modificare i codici PIN predefiniti.
- L'accesso ai PC con installato i software di configurazione e supervisione VSC e VSM, su cui risiedono le informazioni di configurazione dei sistemi, devono essere accessibili solo a personale autorizzato se viene impiegata una password salvata.
- I software Xtralis per PC come VSC o VSM, devono essere installati solamente su PC con sistema Windows attivamente supportato da Microsoft.
- Il prodotto deve essere verificato prima dell'installazione per determinare se sono presenti sigilli rotti che potrebbero indicare una manomissione non autorizzata del prodotto stesso. In tal caso, contattare Xtralis.
- Il punto d'accesso degli accessori VESDA-E utilizza la porta UDP 22094 per comunicare attraverso la rete Ethernet. Se si usa il firewall non occorre abilitare altre porte.

Requisiti di manutenzione del sistema

- NON utilizzare la porta USB per il monitoraggio a lungo termine oppure provvedere a cablarla in modo permanente all'infrastruttura dell'edificio. Utilizzare la porta solo per la configurazione e la manutenzione a opera del personale autorizzato.
- Se il prodotto Xtralis richiede un aggiornamento firmware, verificare che il pacchetto di aggiornamento sia originale e fornito direttamente da Xtralis.
- Prima di disattivare il dispositivo utilizzando il software Xtralis VSC, ripristinare le impostazioni di fabbrica dell'accessorio VESDA-E.



ВАЖНЫЕ СВЕДЕНИЯ О БЕЗОПАСНОСТИ ПРОДУКТА ДЛЯ МОНТАЖНИКОВ, ИНЖЕНЕРОВ ПО ВВОДУ В ЭКСПЛУАТАЦИЮ И ПОЛЬЗОВАТЕЛЕЙ

ДОПОЛНИТЕЛЬНОЕ ОБОРУДОВАНИЕ VESDA-E

ВНИМАНИЕ: Несоблюдение указанных требований может
привести к отключению сигнализации в следствие
стороннего вмешательства

Требования к вводу в эксплуатацию

- Все провода и разъемы VESDAnet должны быть защищены от несанкционированного доступа.
- Используйте ТОЛЬКО безопасные сети, которые физически и логически отделены от IT-инфраструктуры, для подключения через порт Ethernet.
- Дополнительное оборудование VESDA-E и устройства VESDA, включая HLI, не должны иметь доступ через сеть Интернет. Любое предоставление удаленного доступа к дополнительному оборудованию VESDA-E должно подвергаться регулярному наблюдению и полной оценке риска в области кибербезопасности.
- Выбирайте пароль в соответствии с правилами в руководстве пользователя устройства и предоставляйте его только доверенным пользователям.
- PIN-код по умолчанию должен быть изменен при начальной настройке.
- Доступ в PC, на котором установлены программы VSM или VSC, а также размещается информация по конфигурации системы, должен быть запрещен неавторизованным пользователям если на компьютере используется система сохранения паролей.
- Программное обеспечение Xtralis VSC или VSM должно быть установлено на компьютере с официальной версией Windows от Microsoft.
- Перед установкой изделие следует проверить, нет ли сломанных уплотнений, которые могут указывать на несанкционированное вмешательство. Если это так, пожалуйста, свяжитесь с Xtralis для получения консультации.
- Точка доступа дополнительного оборудования VESDA-E использует UDP-порт 22094 для связи через Ethernet. Никакие другие порты не должны быть включены в брандмауэре, если он используется.

Требования по обслуживанию системы

- НЕ используйте USB-порт для длительного мониторинга или постоянного подключения к инфраструктуре здания. Порт может использоваться только для настройки и обслуживания уполномоченным персоналом.
- Если продукт Xtralis требует обновления встроенного ПО, убедитесь, что пакет обновления является подлинным и получен непосредственно от Xtralis.
- Перед выводом устройства из эксплуатации с помощью программного обеспечения Xtralis VSC дополнительное оборудование VESDA-E должно быть сброшено до заводских настроек по умолчанию.



面向安装人员、调试工程师和用 户的重要产品安全信息

VESDA-E附件

警告：如未遵循下面的要求，系统将遭受恶意干扰并可能导致报警失效

调试要求

- 所有VESDAnet接线和连接端口必须确保不会遭受非授权访问。
- 以太网端口必须且仅能与与物理/逻辑上于商用IT设施隔离的安全网络进行连接。
- 绝对不能通过互联网访问VESDA-E附件和VESDA设备（包括HLI）。任何VESDA-E附件的远程访问配置必须经过全面的网络安全风险评估和定期审核。
- 密码选择必须符合探测器用户指南中的准则，且仅向受信用户提供。
- 默认PIN码必须作为初始配置的一部分进行更改。
- 在电脑端安装的，涉及到账号密码的Xtralis VESDA探测器的参数配置软件或探测器联网监控软件的权限必须仅供授权者使用。
- Xtralis 电脑端的软件如VESDA探测器的参数配置软件或探测器联网监控软件必须安装在授权正版可正常使用的微软Window系统上。
- 安装前应检查产品以确定是否有任何可能未经授权篡改的密封破损。如果存在这种情况，请联系Xtralis公司寻求建议。
- VESDA-E附件的接入点使用UDP端口22094通过以太网进行通信。如果使用任何其他端口，则不得在防火墙中启用相应端口。

系统维护要求

- 不得使用USB端口进行长期监测，也不得使其永久连接至建筑物基础设施。仅用于授权人员执行的配置和维护用途。
- 如果Xtralis产品需要固件升级，请确保要升级的固件是Xtralis公司的原厂升级包。
- 在使用Xtralis VSC软件将设备停运之前，应将VESDA-E附件重置为出厂默认设置。