Radicado N.º 0122013597002/ MDN-COGFM-JEMCO-SEMAI-DCCAE-ATECI-29.25

Bogotá D.C., 30 de noviembre del 2022

Señora Coronel
VERÓNICA PEDRAZA MARTINEZ
Directora Administrativo y Financiero COGFM
Comando General Fuerzas Militares
Avenida el Dorado CAN Carrera 54 No 26-25
Bogotá D.C.

Asunto: Informe de Supervisión y Seguimiento No 03 del contrato de bienes y servicios No. 183COGFM DIADF 2022

Mensual _ ó Final _X

Mensual ☐ o Final ☐

Respetuosamente, me dirijo a la señora Coronel Directora Administrativo y Financiero, con el fin de presentar el informe de supervisión y seguimiento del contrato de servicios No 183COGFM DIADF 2022, de acuerdo con la siguiente información:

1. Datos del supervisor

Nombre del supervisor	PD-06. Jaime Ernesto Gutierrez Plazas
Dependencia	Departamento Control Comercio Armas Municiones Y Explosivos
Cargo	Jefe ATECI
Apoyo a la supervisión	N/A

2. Datos del contrato

Número y fecha del Contrato	Contrato de Servicios No 183COGFM DIADF 2022
Contratista	BIRDUN S.A.S.
Cedula de Ciudadanía o Nit.	901.161.285-0
Objeto	suministrar, instalar, configurar, probar y poner en funcionamiento una herramienta de backup, mediante el uso de almacenamiento tipo NAS, para el Departamento Control Comercio de Armas, Municiones y Explosivos (DCCAE) todo incluido, para garantizar la disponibilidad, integridad y confidencialidad de la información, de conformidad con las especificaciones técnicas, aspectos técnicos ponderables, personal para la ejecución del contrato y cuadro de precios descritos en el Anexo Único, el cual forma parte integral del presente contrato.
Valor del Contrato	$ 387.300.000,00
Plazo de ejecución	Hasta el 30 de noviembre del 2022

Modificatorio No. 1			
Adición	Prorroga	Suspensión	Otros x
No. Modificatorio	Tipo	Objeto	

Número	Obligación especificas del contratista y/o cumplimiento de las especificaciones técnicas del contrato	Cumple	No cumple	Evidencia del cumplimiento de las obligaciones específicas del contratista y/o cumplimiento de las especificaciones técnicas del contrato
1	Cumplir con las especificaciones técnicas, estudio previo, el pliego de condiciones y el Contrato, en particular, con los plazos máximos establecidos	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
2	Proveer a su costo, todos los bienes y servicios necesarios para el cumplimiento de los objetivos y funcionalidades requeridas en el contrato	x		Cumple Según Lo Especificado en el Anexa Tecnico se se anexa informe mes de noviembre
3	Rechazar los bienes y servicios que no cumplan con las Especificaciones Técnicas, establecidas en el Anexo Único del contrato	x		No se presento ninguna novedad con la recepción de bienes y servicios que entrego el contratista.
4	Garantizar que ningún funcionario suministrará ninguna clase de información o detalle a terceros y que mantendrá como documentación clasificada todos los aspectos relacionados con el presente contrato, así como los asuntos técnicos e instalaciones del Comando General de las Fuerzas Militares, conocidos por el Contratista, durante el desarrollo de este contrato y con posterioridad al mismo	x		Se anexo acuerdo de confidencialidad en el informe No 1
5	Asumir en su totalidad los gastos ocasionados como transporte, perdida del material o daños ocasionados, que cubra la garantía	x		Cumple Según Lo Especificado en el Anexo Tecnico se anexa garantía.
6	Obtener con la oportunidad debida, las licencias, autorizaciones y permisos a que hubiere lugar para el cumplimiento de todas las obligaciones derivadas del contrato	x		Cumple Según Lo Especificado en el Anexa Tecnico se se anexa informe mes de noviembre

7	Elaborar y suscribir conjuntamente con el supervisor el cronograma de actividades del contrato, dentro de los cinco (05) días calendario siguientes a la comunicación de inicio del plazo de ejecución	x		Cumple Según Lo Especificado en el Anexo Tecnico se anexo en el informe No 1
8	Entregar al Supervisor del Contrato, dentro de los cinco (05) días siguientes al perfeccionamiento del mismo el certificado del curso virtual de cincuenta horas sobre Seguridad y Salud en el Trabajo (Artículo 2.2.4.6.35 del Decreto 1072 de 2015), el cual deberá permanecer vigente durante el plazo de ejecución del contrato	x		Cumple Según Lo Especificado en el Anexo Tecnico se anexo en el informe No 1
9	Cumplir con el protocolo de bioseguridad MDN-COGFMPROGESHU-DIPEC.GI.95.1-2 V. 04 de fecha 19 de enero de 2022, expedido por el Comando General de las Fuerzas Militares y aquel que lo modifique o derogue	x		Cumple con los protocolos de bioseguridad MDN-COGFMPROGESHU-DIPEC.GI.95.1-2 V. 04 de fecha 19 de enero de 2022
	Dar cumplimiento a todas las medidas que en materia sanitaria y de bioseguridad adopten el Gobierno Nacional, las autoridades Distritales y el Comando General de las Fuerzas Militares, para la prevención y mitigación de la propagación del COVID-19	x		Cumple con las medidas que en materia sanitaria y de bioseguridad adopten el Gobierno Nacional, las autoridades Distritales y el Comando General de las Fuerzas Militares
10	Cumplir con las especificaciones técnicas, estudio previo, el pliego de condiciones y el Contrato, en particular, con los plazos máximos establecidos	x		Cumple Según Lo Especificado en el Anexa Tecnico se anexa informe mes de noviembre
	ALMACENAMIENTO TIPO NAS PARA PROPÓSITO DE BACKUP			
11	EQUIPO REF: EX27 FABRICANTE EXAGRID La capacidad RAW de la solución debe ser de mínimo 72TB. La capacidad usable de la solución debe ser de mínimo 54TB.	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
12	La solución debe tener un crecimiento mínimo de 700TB usables con duplicación global en el mismo centro de datos y la capacidad aportada por opciones de integración Cloud no debe ser considerada	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
13	La solución con crecimientos futuros debe permitir llegar a tasas de transferencia de 120TB/hr	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
14	Los componentes de la solución no deben estar descontinuados ni cercanos	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento

	a su fin de soporte (Backup support), mínimo durante los próximos 7 años, el Contratista debe incluir como parte de la entrega del equipamiento un certificado emitido por el fabricante, en el que se indique que los equipos mantendrán una vigencia tecnológica de al menos 7 años			tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
15	La solución de almacenamiento de respaldo deberá ser de propósito específico, no se aceptan almacenamientos de propósito general, teniendo en cuenta que el único uso por parte de la entidad es la de realizar sus copias de seguridad. Todo el hardware requerido para que la solución funcione de manera óptima según el diseño propuesto para cumplir las especificaciones técnicas deberá ser incluido en la oferta y proporcionado por el oferente	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
16	No se aceptarán equipos remanufacturados, los equipos ofertados deben ser nuevos de fábrica	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
17	Debe ser rackeable estándar de 19 pulgadas			Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
18	La solución debe ir acompañada de todas las licencias de software o hardware necesarias para obtener las funcionalidades requeridas y la capacidad total de la solución, incluyendo: deduplicación, replicación, replicación con cifrado AES-256 y nivel de protección contra ransomware, esto debe considerar arquitecturas de múltiples sitios	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
19	Contar con una interfase única basada en web o GUI que permita administrar uno o más equipos de la solución no importando su ubicación física, incluyendo opciones para Cloud	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
20	- La solución debe llegar a tasas de deduplicación de hasta 20:1. - Soporte a deduplicación global incluyendo una o varias controladoras o nodos. - Soporte de envío de alertas usando SNMP. - Integración con herramientas para manejo de syslog centralizado.	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa

	- Capacidad de replicación por hardware con deduplicación entre dos o más sitios.			
21	El almacenamiento tipo NAS debe ser instalado directamente por el fabricante de los equipos ofertados	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
22	El Contratista deberá generar y entregar toda la documentación que requiera el DCCAE, pero como mínimo, la asociada a la definición, diseño, planeación e implementación de la arquitectura para la solución ofertada, una vez adjudicada la operación	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
23	La solución con sus crecimientos debe permitir arquitecturas de controladoras o nodos activos participando en las tareas de Backup a disco y manteniendo la deduplicación global	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
24	Los componentes de la solución se deben entregar con todas las fuentes de poder que soporte el chasis las cuales deben ser redundantes para tolerancia a fallas	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
25	Se deben entregar con todos los ventiladores que soporte el chasis y deben ser módulos redundantes	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
26	La solución de Backup a disco debe tener RAID 6 con doble paridad, que permita el fallo de hasta dos discos	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
27	Todos los nodos, controladoras de la solución deben tener puertos ILO o similar para administración	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
28	La solución propuesta debe incluir configuraciones de red de al menos 4 puertos de red de 1Gbps y 2 puertos de red de 10Gbps	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
29	La solución propuesta debe poder crecer con equipos de conexión a red de 10GbE y 25GbE, incluso los equipos propuestos deben poder actualizarse a este tipo de conectividad	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
30	Se debe soportar bonding para las interfaces de red	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa

31	La solución adquirida debe contar con todos los elementos necesarios para su conectividad (Fibras, cables, Gbits, etc) según cantidad de puertos requeridos e integración con el SW Core de la entidad	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
32	La solución debe incluir características de ransomware recovery que eviten el borrado o cifrado de los datos protegidos	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
33	Las características para ransomware recovery de la solución debe ser independiente a la aplicación de backup, siendo así más seguro cuando esta ha sido afectada	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
34	La solución debe tener una arquitectura donde una versión de los datos protegidos no este expuesta a la red	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
35	La solución debe garantizar la inmutabilidad de los datos respaldados	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
36	La solución debe soportar doble factor de autenticación para los usuarios de administración local y de la integración con el directorio activo	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
37	La solución debe incluir niveles de protección basados en hardware y software ante apagados repentinos no programados, como fallas en el fluido eléctrico	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
38	La solución debe permitir configurar usuarios y grupos basado en roles incluyendo roles de solo visibilidad, administradores, operadores, y roles de seguridad para el nivel de protección contra ransomware	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
39	El término de la garantía técnica (o garantía legal de conformidad con el art. 7° y siguientes de la Ley 1480 de 2011). Se requiere garantía técnica y soporte directamente con el fabricante de la solución, por un plazo mínimo de tres (03) años contados a partir de la fecha de recibo a satisfacción	x		Cumple se anexa acta de La garantía del fabricante .
40	La solución de Backup a disco debe ser entregada con un soporte y garantía por 3 años, 7x24	x		Cumple Según Lo Especificado en el Anexa Tecnico Se anexa acta de garantia y soporte
41	Debe incluir el acompañamiento de un ingeniero del fabricante por el tiempo de soporte contratado Este ingeniero debe implementar con la	x x		Cumple Según Lo Especificado en el Anexao Tecnico se anexa informe mes de noviembre

	entidad, eventos correctivos, preventivos o derivados de buenas prácticas recomendadas. Debe incluirse, sin costo adicional para el COGFM, las actualizaciones del firmware y sistema operativo de los equipos			
42	El soporte del fabricante de la solución de appliance de Backup a disco debe ser entregado con soporte avanzado de nivel 2, para la atención en temas reactivos como errores, cambios de parte y temas proactivos como modificación a la configuración e incluso actualizaciones de las versiones del firmware y software de los equipos. sin límite de intervenciones	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
43	La solución debe tener opciones de monitoreo y alertas al fabricante, con el objetivo de agilizar tareas de soporte	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
	LICENCIAMIENTO HERRAMIENTA DE BACKUP			
44	Herramienta Fabricante Veeam	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
45	El licenciamiento tendrá una vigencia de un (1) año contado a partir de la entrega y recibo a satisfacción	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
46	La solución deberá poseer una única consola que se integre con la herramienta de backup del Comando General de las Fuerzas Militares, con capacidades para procesos de respaldo para ambientes virtuales, replicación de máquinas virtuales Onpremises, gestión y distribución de agentes para maquinas físicas y nube privada de ORACLE	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
47	La solución debe proporcionar una copia de seguridad eficiente "incremental para siempre" e incluir opciones de copias de seguridad completas y ad-hoc para cualquiera que sea la carga objetivo (VM Onpremises, VM Cloud privada, NAS, Servidor Físico)	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
48	La solución debe detectar automáticamente el espacio libre del Datastore productivo y evitar la creación de snapshot para respaldo, si el espacio está por debajo del umbral definido	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa

49	La solución debe monitorear automáticamente la latencia del datastore productivo durante la copia de seguridad y reducir la velocidad de la copia de seguridad si la latencia del datastore supera un umbral definido	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
50	La solución debe detectar automáticamente los snapshot´s de respaldo de hyper v huérfanos y eliminarlas. La solución deberá permitir tomar respaldos de Snapshots generados por el almacenamiento de producción	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
51	La solución debe permitir la recuperación de máquinas virtuales, archivos granulares de sistema operativo y de aplicación desde los snapshot's	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
52	La solución deberá permitir la creación de backup full sintéticos para máquinas virtuales del ambiente virtual de hyper v sin importar el sistema operativo de la maquina objetivo (Linux - Windows) La solución no debe requerir agentes implementados en máquinas virtuales para facilitar el respaldo de aplicaciones y la ejecución de tareas de recuperación granular de aplicaciones	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
53	No se debe requerir que la solución realice respaldos separados de los datos de aplicación de las máquinas virtuales para facilitar la recuperación granular de elementos de esta	x		Cumple Según Lo Especificado en el Anexo Tecnico se anexa informe mes de noviembre
54	En los procesos de respaldo se debe permitir truncar los registros de transacciones o archivos de aplicaciones como Microsoft SQLServer, Microsoft Exchange y Oracle Database sin el uso de agentes en las máquinas virtuales en ningún momento del proceso	x		Cumple Según Lo Especificado en el Anexo Tecnico
55	Los respaldos sin agente de máquinas virtuales deben proporcionar respaldo de logs o archivos de transacciones de Microsoft SQLServer y Oracle Database junto con copias de seguridad basadas en snapshots	x		Al ejecutarse los respaldos en las copias de seguridad se realiza el respaldo de logs y archivos de transacciones de Microsoft SQLServer y Oracle Database
56	La solución debe utilizar la tecnología Changed Block Tracking para copias de seguridad incrementales de cargas de trabajo físicas o basadas en la nube			Para las copias de seguridad se realiza tecnología Changed Block Tracking para la copia de backup en modo incremental
57	La solución debe proporcionar complementos de respaldo y recuperación para Oracle RMAN	x		La solución de Backup genera copias respaldo y recuperación en Oracle RMAN

58	La solución debe respaldar de forma consistente aplicaciones de base de datos MySQL y PostgreSQL que se ejecutan en Linux de forma consistente	x		La solución de copias respalda aplicaciones de base de datos MySQL y PostgreSQL
59	La solución debe proporcionar una portabilidad completa en cualquier archivo de respaldo ejecutado por la solución y no debe depender de ninguna infraestructura de respaldo en un punto en el tiempo, por ejemplo, el catálogo central, para la recuperación	x		La solución ejecuta en modo de portabilidad completa en cualquier archivo de respaldo en la ejecución de recuperación de archivos
60	La solución debe proporcionar tecnología de recuperación de respaldo de máquinas virtuales y maquinas físicas x86 de forma instantánea (encendido en menos de 10 minutos y automática) sobre la infraestructura Hyper v desde el repositorio de respaldos ya sea que se encuentren Onpremises o sobre un almacenamiento de Objetos en una nube privada. La solución debe poder utilizar la copia de seguridad o réplica de la máquina virtual para iniciar la máquina virtual en un entorno de red aislado para fines de prueba o certificación de respaldos	x		La Solución proporcionar tecnología de recuperación de respaldo de máquinas virtuales y maquinas físicas x86
61	La solución debe proporcionar la tecnología de recuperación Changed Block Tracking para máquinas virtuales hyper v, es decir, tener la capacidad de recuperar solo los bloques modificados desde el ultimo respaldo y no la VM completa. La solución debe poder escanear los datos de la máquina virtual a recuperar con un software antivirus antes de iniciar la restauración de la máquina al entorno de producción de forma integrada y automática. La solución debe abortar la operación de recuperación si se detecta malware	x		La solución ofrece tecnología de recuperación Changed Block Tracking para máquinas virtuales hyper v
62	La solución debe proporcionar la capacidad de iniciar la máquina virtual en un entorno de red aislado durante el proceso de recuperación e inyectar un script que permita que el servidor se modifique para fines de cumplimiento antes de la recuperación	x		La solución ofrece capacidad en maquinas virtuales en un entorno de red aislado durante cualquier proceso de recuperación
63	La solución debe permitir la recuperación de archivos de sistema operativo directamente sobre una máquina virtual incluso cuando no haya conexión de red entre el servidor de respaldo y la máquina virtual	x		La solución ofrecida permite recuperrar archivos de sistema operativo directamente sobre una máquina virtual
64	La solución debe proporcionar una interfaz de usuario de autoservicio	x		La solución ofrece interfaz de usuario de autoservicio basada en la web.

	basada en la web con la capacidad de buscar un archivo específico en todas las copias de seguridad			
65	La solución debe admitir la recuperación granular de bases de datos Oracle a partir de copias de seguridad basadas en imágenes u Oracle RMAN desde la consola de la solución	x		La solución permite recuperación granular de bases de datos Oracle a partir de copias de seguridad
66	La solución debe proporcionar una interfaz de usuario de autoservicio basada en web con la capacidad de examinar y recuperar elementos de Microsoft Exchange, bases de datos SQLServer u Oracle	x		La solución ofrece interfaz entre el usuario de autoservicio basada en web.
67	La solución debe permitir capacidades de Alta Disponibilidad (HA) donde se permitir la integración de varios repositorios de respaldos incluso de fabricantes diferentes en un solo repositorio virtual	x		Permite capacidades de Alta Disponibilidad (HA) donde se permitir la integración de varios repositorios para realizar sus copias de seguridad
68	La solución debe proporcionar un mecanismo fácil para expandir o adicionar el almacenamiento de respaldo de destino	x		Ofrece mecanismos de fácil acceso para adicionar almacenamiento de respaldo con un destino especifico
69	La solución debe admitir copias de seguridad de duplicada	x		La solución admite copias de seguridad en forma duplicada
70	La solución debe admitir de forma nativa el traslado de archivos de respaldo a Amazon S3, IBM Cloud Object Storage, Azure Blob Cloud Storage y otras plataformas de almacenamiento en la nube compatibles con protocolo S3	x		La solución admite forma nativa el traslado de archivos de respaldo a Amazon S3, IBM Cloud Object Storage, Azure Blob Cloud Storage
71	La solución debe proporcionar una recuperación incremental y granular del almacenamiento de objetos basado en la nube	x		La solución proporcionar una recuperación incremental y granular
72	La solución debe ofrecer inmutabilidad para el repositorio de primer nivel	x		Cumple Según Lo Especificado en el Anexa Tecnico se se anexa informe mes de noviembre
73	La solución debe tener la opción de copiar o mover datos al almacenamiento de objetos al finalizar la copia de seguridad. incluso, ambas opciones se pueden habilitar en una misma política	x		Cumple Según Lo Especificado en el Anexa Tecnico se se anexa informe mes de noviembre
74	La solución debe encriptar los archivos de respaldo usando el encriptado AES de 256 bits. El cifrado no debe depender de la plataforma de almacenamiento de respaldo	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
75	La solución debe integrarse con SAML 2.0 para la autenticación extendida	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
76	Deberá permitir la delegación de tareas de recuperación, a nivel de elementos de aplicación, hacia otros usuarios, de	x		Cumple Según Lo Especificado en el Anexa Tecnico se se anexa informe mes de noviembre

	forma tal a poder descargar la cantidad de maniobras a ejecutar por el administrador de la plataforma			
77	La solución debe leer y verificar automáticamente la consistencia de los datos de producción en el archivo de copia de seguridad una vez completada la copia de seguridad. En caso de que se detecte corrupción de datos, la solución debe reconstruir automáticamente el bloque dañado con datos de producción	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
78	La solución deberá poder programar tareas de encendido automático de las máquinas virtuales a partir de los respaldos y ejecutar tareas de verificación de sistema operativo y la disponibilidad de aplicaciones. Esta prueba no debe tener impacto en la red de producción	x		La solución permite generar encendido automático de las máquinas virtuales a partir de los respaldos y ejecutar tareas de verificación de sistema operativo y la disponibilidad de aplicaciones.
79	La solución debe proporcionar un informe de verificación de recuperación			La solución proporciona informe de verificación de recuperación
80	La solución debe escanear automáticamente los datos de producción en busca de virus durante la verificación de respaldo	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
81	La solución debe presentar la tecnología de replicación directa de máquina virtuales sobre hyper v sin depender de tareas de respaldo para lograr la replicación, igualmente debe implementar procesos de failover y failback La solución debe integrar una consola para gestionar la automatización de los planes de contingencia (DRP) basados en los respaldos y replicas	x		Cumple Según Lo Especificado en el Anexa Tecnico se se anexa informe mes de noviembre
82	Se debe incluir la generación de reportes y documentación de forma automática de cada uno de los planes generados, como también de las pruebas de ejecución de estos. Estos reportes o documentación deben tener el detalle de cada paso realizado en las tareas de recuperación y su resultado	x		Cumple Según Lo Especificado en el Anexa Tecnico se anexa informe mes de noviembre
83	La solución para automatizar el proceso de recuperación a desastres debe tener la capacidad de extender los pasos preestablecidos para ser implementados en cada plan de recuperación	x		La solución permite automatizar el proceso de recuperación a desastres
84	La solución debe alertar sobre trabajos de respaldo fallidos y trabajos que exceden la ventana de respaldo	x		La solución alerta sobre trabajos de respaldo fallidos y exitosos

85	La solución debe alertar por adelantado si el repositorio de los respaldos se acerca a la capacidad	x		La solución genera alertas cuando un repositorio de los respaldos se acerca a su capacidad total
86	Las copias secundarias de respaldo deberán ser independientes de la copia principal y podrán seleccionar diferentes puntos de retención con soporte a estrategias GFS	x		Las copias secundarias de respaldo son independientes de la copia principal
87	La solución debe presentar tecnología de aceleración WAN incorporada para la replicación de datos con la capacidad de optimizar la utilización del ancho de banda	x		La solución presentar tecnología de aceleración WAN
88	La solución debe proporcionar alertas proactivas para eliminar problemas. Estos problemas deben detectarse automáticamente, abarcar la configuración y el rendimiento, y el proveedor debe actualizar dinámicamente la detección	x		La solución ofrece alertas proactivas para eliminar problemas
89	La solución debe proporcionar un informe de evaluación de Infraestructura hyper v para asegurar que el entorno esté preparado para las operaciones de respaldo basadas en snapshot y detectar máquinas virtuales que requieren implementación de respaldo basada en agente	x		La solución proporciona informes de evaluación de Infraestructura hyper v
90	La solución debe proporcionar un informe de autoevaluación. El informe debe detectar si la solución se implementa de acuerdo con las mejores prácticas	x		La solución proporciona informes de autoevaluación
91	La solución debe proporcionar un informe sobre máquinas virtuales que no están protegidas por copia de seguridad y un informe de cumplimiento de RPO (Objetivo del punto de recuperación) para las máquinas virtuales protegidas	x		La solución proporciona informes sobre máquinas virtuales que no están protegidas
92	La solución debe proporcionar planificación de capacidad y pronosticar la utilización del espacio de almacenamiento de respaldo	x		Cumple Según Lo Especificado se anexa informe automatizado sobre todas las operaciones de recuperación
93	La solución debe proporcionar un informe automatizado sobre todas las operaciones de recuperación para fines de auditoría	x		Cumple Según Lo Especificado se anexa informe automatizado sobre todas las operaciones de recuperación
94	La solución debe ofrecer la capacidad de generar alarmas y acciones de remedición en monitoreo de procesos y servicios de VM de ambientes Windows	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa

95	Se debe proveer la capacidad de generar reportes personalizados basados en datos de inventario y uso de recursos de la plataforma virtual, como también de la plataforma de respaldo	x		Cumple Según Lo Especificado se anexo en el informe No 1
96	La solución debe proporcionar informes de cambios de configuración de la plataforma virtual de hyper v y de respaldos con fines de auditoría. Deberá ofrecer un conjunto de reportes capaces de presentar información de tipo: - Reportes que permitan la planificación de la capacidad. - Reportes que permitan la determinación de inefectividad en el uso de recursos. - Reportes que faciliten la visibilidad de tendencias negativas y anomalías. - Envió automático y programado de reportes de auditoria para operaciones de recuperación y modificaciones a políticas de respaldos o replicación. - Tableros de control claros, presentables e integrables en sitios web	x		Cumple Según Lo Especificado en el Anexa Tecnico se anexa informe mes de noviembre
97	Se deberá realizar la instalación de cada una de las instancias en los servidores físicos y la nube privada de ORACLE. Para lo cual se deben instalar 02 instancias en la solución de virtualización del DCCAE y 04 instancias en la base de datos y aplicación del SIAEM que se encuentra en la nube privada de ORACLE, en las instalaciones del Ministerio de Defensa Nacional			Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
	SERVICIO DE INSTALACIÓN, CONFIGURACIÓN, PRUEBA Y PUESTA EN FUNCIONAMIENTO DE LA SOLUCIÓN			
98	Se deberá realizar la instalación del licenciamiento adquirido para la solución de Backup, el cual será desplegado en los servidores del Comando General de las Fuerzas Militares	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
99	Se deberá realizar la conexión física entre la solución de nube privada ORACLE ubicada entre el Datacenter del Ministerio de Defensa Nacional y el Datacenter del Comando General de las Fuerzas Militares	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
100	Se deberá realizar las configuraciones necesarias para la puesta en funcionamiento del agente o licencia de Backup con el RMAN de la nube privada Oracle, para cual se deberá tomar	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa

	contacto con el DBA de entidad en previa coordinación con el supervisor del contrato designado			
101	Se deberá realizar la configuración de la copia de seguridad de las bases de datos y aplicación SIAEM hacia el repositorio de la solución NAS adquirida	x		Cumple Según Lo Especificado en el Anexa Tecnico Se entrega equipo de Almacenamiento tipo NAS realizando configuración, instalación y puesta en funcionamiento de la solución. Según acta de entrega equipos la cual se anexa
	OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO			
102	El contratista y los recursos humanos que formarán parte del proceso, deberán firmar al inicio del plazo de ejecución del contrato, un acuerdo de confidencialidad donde garantizan la reserva de la información institucional a la cual tengan acceso directa o indirectamente o por intermedio de terceros, así como la que genere, como producto de la ejecución del presente contrato, y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros. Por lo anterior, es indispensable que el contratista se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Comando General de las Fuerzas Militares	x		Cumple Según Lo Especificado en el Anexa Tecnico se anexo en el informe No 1
103	En tal virtud, adoptará todas las medidas necesarias para impedir la duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida de información. Bajo ninguna circunstancia dicha información y/o documentación podrá ser utilizada para fines distintos al desarrollo del contrato respectivo. Al finalizar la ejecución del proyecto toda la información y documentos entregados por el Comando General de las Fuerzas Militares, deberán ser retornados	x		Cumple Según Lo Especificado en el Anexa Tecnico se anexa informe mes de noviembre
104	ESTUDIO DE SEGURIDAD PERSONAL: El contratista debe aceptar y permitir que el COGFM efectúe un Estudio de Seguridad Personal (ESP) a los funcionarios designados para el desarrollo del proyecto, a fin de comprobar datos y establecer antecedentes disciplinarios; que garanticen la seguridad de la información	x		Cumple Según Lo Especificado en el Anexa Tecnico
105	Una vez firmado el contrato y dentro de los cinco (05) días calendario siguientes, el contratista entregara al supervisor del contrato los formatos de Estudio de Seguridad Personal	x		Cumple Según Lo Especificado en el Anexo técnico

	debidamente diligenciados junto con los soportes requeridos, para realizar los respectivos estudios de seguridad del personal contratista que va a realizar los trabajos			
106	En el evento en que el resultado del Estudio de Seguridad sea negativo el contratista se obliga a reemplazar al personal allegando copia de la hoja de vida y de todos los documentos exigidos en el proceso, del nuevo personal, para aprobación por parte de la Entidad; éste deberá tener un perfil igual o superior al que va a ser reemplazado	x		Durante el presente periodo no se presentó este evento sobre los estudios de Seguridad.
107	El contratista debe comprometerse a tomar las medidas necesarias para prevenir, mitigar, controlar, compensar y corregir los posibles efectos e impactos negativos sobre el ambiente que se causen durante la ejecución y desarrollo del objeto contractual, de conformidad con lo establecido en las normas ambientales vigentes	x		Cumple Según Lo Especificado en el Anexo técnico el contratista toma las medidas necesarias para prevenir, mitigar, controlar, compensar y corregir los posibles efectos e impactos negativos sobre el ambiente
108	Todos los gastos del personal que el proveedor disponga para realizar las actividades de instalación y configuración como: Desplazamiento, alojamiento y demás actividades deberán ser asumidos por el Contratista, sin que se genere costo adicional para el COGFM	x		Cumple Según Lo Especificado en el Anexo técnico
109	El contratista deberá garantizar el personal suficiente, idóneo con profesionales calificados y técnicos necesarios para la completa ejecución y cumplimiento del contrato, sin que esto genere costo adicional para el Comando General de las Fuerzas Militares, de igual manera disponga de instalaciones y equipos propios para la ejecución del proyecto	x		Cumple Según Lo Especificado en el Anexo técnico
110	Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. En todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del presente proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos del contrato derivado del presente proceso	x		Cumple Según Lo Especificado en el Anexo técnico

111	Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos	x		Cumple Según Lo Especificado en el Anexo técnico
112	Dentro de los primeros cinco (05) días calendario del plazo de ejecución, el contratista deberá presentar el cronograma para la ejecución del objeto del contrato, para aprobación del supervisor del contrato.	x		Cumple Según Lo Especificado en el Anexo técnico se anexo en el informe No 1
113	PERSONAL PARA LA EJECUCIÓN DEL CONTRATO - GERENTE DE PROYECTO: JUAN CARLOS CELY RICO, Ingeniero de Sistemas, Especialista en Proyectos Informáticos - ESPECIALISTA HERRAMIENTA DE BACKUP: CARLOS ANDRES ALVARADO NOVOA, Ingeniero de Telecomunicaciones - ESPECIALISTA NUBE ORACLE: IVAN DARÍO CORTES WILCHES, Ingeniero de Sistemas	x		Cumple Según Lo Especificado en el Anexo técnico
114	En el evento que el contratista requiera cambiar el personal propuesto, deberá tramitar a través del supervisor y allegar copia de la hoja de vida y de todos los documentos exigidos en el proceso, experiencia del nuevo personal, para aprobación por parte de la Entidad; éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado y cumplir con los requerimientos estipulados en esta ficha técnica. Se deberá reemplazar en un periodo máximo de 3 días calendario. Deberá informarse al supervisor, de tal situación, con mínimo 10 días calendario de antelación, anexando la hoja de vida del nuevo funcionario. Así mismo los recursos asignados para el presente contrato, solo podrá ser cambiados a solicitud de supervisor del contrato en el caso que este sea desvinculado de la empresa	x		Durante el presente periodo no se presentó este evento sobre cambio de personal.
115	La Entidad se reserva el derecho de exigir al contratista, previo escrito emitido por el competente contractual y el supervisor designado, el reemplazo de cualquier persona vinculada al proyecto			Durante el presente periodo no se presentó este evento sobre cambio de personal.

116	La supervisión podrá solicitar al contratista en cualquier momento, información sobre la nómina del personal y cumplimiento de aportes al sistema de seguridad social del personal contratado por prestación de servicios. El contratista atenderá esta solicitud con el detalle requerido y en el plazo razonable que la supervisión haya fijado	x		Cumple Según Lo Especificado en el Anexo técnico
117	El supervisor evaluará el desempeño laboral del profesional asignado y estará en facultad de solicitar su remplazo si lo considera necesario, en dado caso el oferente adjudicatario deberá reemplazarlo en un tiempo no mayor a cinco (5) días luego de la solicitud formal por parte del supervisor del contrato	x		Cumple Según Lo Especificado en el Anexo técnico
118	El Contratista deberá cumplir todas las normas de seguridad industrial en la ejecución del contrato	x		Cumple Según Lo Especificado en el Anexo técnico
119	El Contratista deberá asumir la responsabilidad en el manejo del personal empleado, así como la seguridad y responsabilidad de los elementos y materiales que se requieran para el desarrollo de la misma	x		Cumple Según Lo Especificado en el Anexo técnico
	Ponderables			
1	El contratista ofrece un SERVICIO DE TRANSFERENCIA DE CONOCIMIENTO EN ADMINISTRACIÓN DEL ALMACENAMIENTO TIPO NAS OFERTADO (hardware) de mínimo cuarenta (40) HORAS PARA DOS (2) FUNCIONARIOS DEL COGFM; sin que este ofrecimiento genere costo adicional para el COGFM	x		Cumple Según Lo Especificado se anexa acta de trasferencia del conocimiento
2	El contratista ofrece un SERVICIO DE TRANSFERENCIA DE CONOCIMIENTO EN ADMINISTRACIÓN DE LA HERRAMIENTA DE BACKUP OFERTADA de mínimo cuarenta (40) HORAS PARA CUATRO (4) FUNCIONARIOS DEL COGFM; sin que este ofrecimiento genere costo adicional para el COGFM	x		Cumple Según Lo Especificado se anexa acta de trasferencia del conocimiento

4. Cumplimiento de Obligaciones al Sistema de Seguridad Social y Parafiscales

Que la Planilla Integrada de Liquidación de Aportes N° 63295600, con fecha de pago 15 de noviembre del 2022, evidencian el cumplimiento de las obligaciones al Sistema de Seguridad Social Integral, la cual es anexada al presente informe.

Que mediante certificación de fecha 30 de noviembre del 2022, suscrita por la señor(a) CLAUDIA MILENA MATEUS SANCHEZ, con TP. 185745-T de la empresa BIRDUN S.A.S. estipula encontrarse al día en el pago al Sistema de Seguridad Social en Pensiones y en Salud, riesgos profesionales, aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje (SENA). Se anexa certificado del cumplimiento por parte del contratista.

NOTA: El certificado de aportes parafiscales lo puede firmar el representante legal cuando en cámara de comercio no reporta revisor fiscal, cuando el contratista tiene revisor fiscal este es el único competente para firmar las certificaciones de paz y salvo de seguridad social y parafiscal.

5. Aspectos Financieros

Valor Inicial del Contrato Incluido IVA:	387.300.000,00
Que al contrato se le efectuó una adición el XX de XXX de 20XX por valor de:	$ 0
Valor Total del Contrato es de:	387.300.000,00

Que se tramitaron las siguientes facturas con cargo al contrato supervisado:

No Factura	Fecha	Valor de la Factura
BIRD 81	18-11-2022	$387.182.353,00
Valor Facturado		$387.182.353,00
Saldo por Facturar		$ 0
Valor de Reintegro		$ 0
Valor Total del Contrato		$ 387.300.000,00

Nota: En el anterior cuadro se deberán relacionar todas las facturas que se hayan tramitado para pago durante la ejecución del contrato.

6. Observaciones relevantes del supervisor:

No se tienen observaciones

7. Documentos anexos:

Relacione los documentos anexos conforme al clausulado del contrato y el anexo técnico. (Garantías, Actas, Cronogramas, Informes, Registros Fotográficos y Medios Magnéticos, etc.)

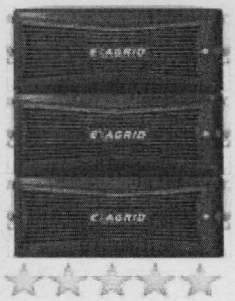
Atentamente,

PD-06. Jaime Ernesto Gutierrez Plazas
Supervisor Contrato No 183COGFM DIADF 2022
Correo electrónico jaimgut@cgfm.mil.co
Teléfono 3150111 - Ext. 1256

Espacio para ser diligenciado en la Dirección Administrativa y Financiera

CONTROL DE APROBACIONES Y DE TIEMPOS PARA PUBLICAR				
CONTRATOS	FECHA DE RECEPCIÓN DEL INFORME	FECHA DE APROBACIÓN Y CARGUE DEL INFORME.	NOMBRE DE FUNCIONARIO REVISOR	FIRMA DEL FUNCIONARIO AVALANDO INFORME
	02 DIC/22	02 DIC/22	PS. LOURDES FONSECA 02 DIC/22 4:23 PM	

EXAGRID



ExaGrid Tiered Backup Storage

Fastest Backups.
Fastest Recoveries.
Unparalleled, Cost-effective Scale-out.

Administrator's Guide For ExaGrid Software Version 6.0 and Later

Copyright

No part of this document may be reproduced or transmitted in any form or by any means without the express written permission of ExaGrid Systems, Inc.

© 2003-2022 ExaGrid Systems, Inc. All rights reserved. Printed in USA.

This document, the associated software, and the associated online documentation are the property of ExaGrid Systems, Inc. or its licensor, as applicable, and are loaned to the user under the terms of the ExaGrid Systems, Inc. End User License Agreement. Unauthorized copying or use of the software or any associated materials is contrary to the property rights of ExaGrid Systems and is a violation of state and federal law. ExaGrid reserves the right to change specifications or other product information without notice.

Trademarks

ExaGrid is a registered trademark of ExaGrid Systems, Inc. ExaGrid Systems (Logo), InstantDR, InfiniteFiler, GRIDdisk and Intelligent Disk-based Data Protection are all trademarks of ExaGrid Systems, Inc. All third-party trademarks are the property of their respective owners.

License Agreement

This document, the associated software and the associated online documentation are the property of ExaGrid Systems, Inc. or its licensor, as applicable. The use of these materials and the software is strictly limited to those users who have signed the ExaGrid Systems, Inc. End User License Agreement.

For any software acquired directly or indirectly on behalf of a unit or agency of the United States Government, whether for civilian agencies or for units of the Department of Defense, the software is a commercial item or commercial computer software (and documentation), and pursuant to Section 12.212 of the Federal Acquisition Regulations (FAR) or DoD FAR Supplement Section 227.7202, is provided under restricted rights as enumerated in the End User License Agreement.

ExaGrid Patents

This section is intended to serve as notice under 35 U.S.C. § 287(a).

U.S. Patent Nos. 7,246,140; 7,246,275; 7,593,966; 7,925,623; 8,412,848; 8,589,363; 8,812,738; 9,223,794; 9,223,812; 9,703,797; 9,430,546; 10,067,946; 10,073,855; 10,114,831; 10,303,656; 10,387,374; 10,452,617; 10,498,356. Other patents pending.

European Pat. Nos. 1,537,496; 1,540,441; 1,540,478; 1,540,510; 2,256,934; 3,059,677; 3,062,227; 3,159,811; 3,401,790. Other patents pending.

Preface

This guide provides an overview of the ExaGrid System and getting started instructions for the novice ExaGrid Administrator.

Detailed descriptions of the ExaGrid System and advanced administrator procedures can be found in the ExaGrid System's online help.

Related Documentation

Title	Part Number
Assembling and Initializing Your ExaGrid Appliance	210-0164-xx
ExaGrid Release Notes	210-0174-xx

Contacting ExaGrid Technical Support

If you have technical questions about this product that are not answered in this document contact ExaGrid Support:

- Email: **support@exagrid.com**
- Phone: 800-868-6985 and at the prompt, press 2.

Glossary

Understanding these terms will help you better understand ExaGrid .

Available for Next Backup - The amount of space a backup application sees as available for the next set of backups.

Available for Retention - The amount of allocated retention space remaining. If there is no available Retention Allocation across the site, then this is an indication that more ExaGrid capacity is needed.

Backup Data – Total (pre-deduplicated) data written to the ExaGrid Appliance by your backup applications. Does not include data replicated to this ExaGrid Appliance from ExaGrid Appliances on other ExaGrid Sites

Capacity - Total capacity of the selected ExaGrid Site or ExaGrid Appliance.

Dedupe Rate - How fast data is deduplicating on the ExaGrid Appliance.

Disaster Recovery – In multi-site systems, in the event of a catastrophic loss of an ExaGrid Site, the ability to recover backup data that has been replicated to one or two surviving ExaGrid Sites.

ExaGrid Appliance - The hardware on which the ExaGrid Software runs. There are several ExaGrid Appliance models, each with a different capacity.

ExaGrid Site - A logical collection of ExaGrid Appliances. An ExaGrid can be made up of one or more ExaGrid Sites.

File Collection - A set of files associated with a backup application's backup to an ExaGrid Share. ExaGrid reports will report one or more file collections associated with a backup job.

Hub – ExaGrid uses a hub-and-spoke topology. In multi-site ExaGrid environment, one site is designated the hub. When logged into the hub, the hub and all spoke sites are displayed in the navigation tree and system-level reports roll up information from all spokes. When logged

into a spoke, only the spoke site and its hub are displayed in the navigation tree. system and site-level reports roll up information for the spoke site only.

InstantDR™ Share - A copy of a share at a second ExaGrid Site. When you create an ExaGrid Share you have the option of also creating an InstantDR Share on an ExaGrid Appliance in another ExaGrid Site. InstantDR Shares are used in disaster recovery operations, remote tape copy operations, and in testing data recovery from another ExaGrid Site.

Landing Zone - The space allocated for landing and caching backups. The Landing Zone size varies by ExaGrid model. During installation, the Landing Zone can be tuned to meet the specific needs of your environment. Landing Zone size is configurable by your ExaGrid support representative.

Member - An ExaGrid Appliance that is included in a Pooled Share.

Modified (Bytes) - The amount of undeduplicated data in the Landing Zone that has changed since the last backup was deduplicated.

Not Shared – Deduplicated data that is not shared with any other ExaGrid Share in an ExaGrid Site.

Pending Purge - Data pending purge includes:

- Deduplicated data deleted by a backup application and no longer referenced in the Landing Zone
- Data held for Retention Time Lock.

  Data pending purge is automatically managed and purged by the ExaGrid.

Pooled Share - An ExaGrid Share that can take advantage of the storage space across all ExaGrid Appliances in an ExaGrid Site.

Primary Retention - Space consumed by deduplicated data from backups written to this site or server.

Queue Size - Total data waiting to be replicated.

Queue Age - The time data has been waiting to be replicated.

Read Rate - How fast data is being read from an ExaGrid Appliance.

Rebalance – Amount of data the ExaGrid Site has moved to take advantage of under-used ExaGrid Appliances in the ExaGrid Site.

Reclaimable cache – Data that has been recently backed up and has completed deduplication. Since there is a deduplicated copy in the Retention space, the ExaGrid Appliance will keep a cached copy in the Landing Zone until additional disk space is needed. Landing Zone space is reclaimed by purging the oldest data first.

Replica - A copy of a share that has been replicated to another ExaGrid Site.

Replica Retention - Space consumed by data deduplicated by other sites and replicated to this site or server.

Replication - A share setting that instructs the ExaGrid to maintain copies of a share on one or more ExaGrid Sites.

Retention Allocation - The space allocated to storing deduplicated data. Retention Allocation is automatically configured based on the Landing Zone size.

Retention Tier – The portion of an ExaGrid Appliance that stores and manages deduplicated "Versions" of backup files.

Send Rate - The speed data is being replicated to other ExaGrid Sites.

Share - A mount point/folder on an ExaGrid Appliance to which backup applications write.

Share Migration - To move a share and its contents from one ExaGrid Appliance to another.

Shared – Total deduplicated data shared by two or more ExaGrid Shares in an ExaGrid Site.

Shared Consumption –Space used by data that is the same on two or more shares in the ExaGrid Site.

Spoke – ExaGrid use hub-and-spoke topology. In multi-site ExaGrid environments, one site is designated the hub. When logged into the hub, the hub and all spoke sites are displayed in the navigation tree and system-level reports roll up information from all spokes. When logged

into a spoke, only the spoke site and its hub are displayed in the navigation tree. system and site-level reports roll up information for the spoke site only.

Stage-in activity - Indication backup data being read is no longer cached in the Landing Zone.

System Reserved - Space reserved for ExaGrid operations.

Throttle Rate - Restrictions on the speed data can be sent to other ExaGrid Sites. Typically throttling is turned on during business hours.

Total Backup Data - Total (pre-deduplicated) data written to the ExaGrid Share.

Total Consumption - Space consumed by deduplicated backups (Primary Retention) and deduplicated data replicated to this ExaGrid Site.

Write Rate - How fast data is being written to the ExaGrid Appliance.

Versions – The deduplicated copies of a backup job.

Contents

Introduction 1

Shares 2

ExaGrid Hub Sites and Spoke Sites 2

Data Flow 3

Logging In 4

The ExaGrid User Interface 5

ExaGrid Main Menu Drop Downs 7

Show Device Model 9

Networking 10

Network Configuration Rules 11

Network Settings 12

Bonding 14

Ports Used Between ExaGrid Sites 15

Sites Joined Using IPsec Tunnels 15

Sites Joined NOT Using IPsec Tunnels 15

Enabling/Disabling IPsec Tunnels Settings 16

TLS Certificates 18

Applying TLS Certificates 19

Managing and Securing Access 23

Retention Time-Lock Overview 25

Modifying Retention Time-Locks 26

Approving and Rejecting Retention Time-Lock Modifications 27

User Roles 29

User Role Idle-Timeout Settings 30

Creating and Modifying ExaGrid Local Users 31

Valid Local User Names 32

Valid ExaGrid Local User Name Character Set 32

Valid ExaGrid Local User Password Character Set 32

Changing Your Password 33

Two-Factor Authentication 35

Setting Two-Factor Authentication 35

Managing Active Directory 38

ExaGrid User Interface Access Using Active Directory Credentials 38

Adding ExaGrid Appliances to An Active Directory Domain 38

Mapping an Active Directory User or Group to an ExaGrid Role 40

Share Access Policies 42

Managing SSH Keys 43

Support Accounts 44

Support Gateway 46

Root Access Management 47
Using Server Message Block (SMB) Signing 49

ExaGrid Shares 51

Primary Shares 51
Backup Application Specific Shares 52
Pooled Shares 52
Universal Backup Shares 52
Utility Shares 54
InstantDR™ Shares 55
Share Protection 56
Share Migration 57
Share Access Policies 58
Network Access Policies 58
User Access Policies 59
Share Delete Monitor 61
Delete Monitor Alarms 61
Creating Shares 62

Share Replication 66

Creating Replicas and InstantDR Shares 68
Creating a Replica 68
Creating an InstantDR Share 69
Hub Site To Spoke Site Replication Example 70
Spoke Site to Hub Site Replication Example 71

Deleting Shares and Replicas 72
Replication Scheduler 73
Throttling Replication 74
Encrypting Replication 76

System Record Keeping 78

ExaGrid Site Worksheet 79
ExaGrid Site Administrative Key 79
ExaGrid Appliance Worksheets 80
ExaGrid Share Worksheet 82

The IPMI Port 83

Configuring The IPMI Port 84
IPMI Port Login Credentials 85
Username Requirements 85
Password Requirements 86
Setting IPMI Port Login Credentials 86

Encryption Capable ExaGrid Appliances 89

Encryption at Rest 90
Encryption at Rest Passwords 90
Enabling Encryption at Rest 91
Adding a New Encryption Capable Server to a Site 92
Server's Encryption Password Does Not Match Site's Password 93
Boot Protection 95

Enabling Boot Protection 96

Using the IPMI Network Port to Enter Boot Protection Password 97

Recovering From Malicious Software Attacks, or a Loss of ExaGrid Appliances 100

Before an Event Occurs 101

Recovering From Malicious Software Attacks 102

Suspending All Shares 102

Recovering From a Point In Time 103

Post Recovery 107

Recovering From The Loss of ExaGrid Appliances - Disaster Recovery 107

ExaGrid Reports 108

MB, GB, and TB vs MiB, GiB, and TiB 109

Summary Reports 110

Summary Report Graphs 111

Summary Report Tables 113

The ExaGrid-level Summary Report 115

The ExaGrid Site-level Summary Report 116

The ExaGrid Appliance-level Summary Report 117

Statistical Reports 119

Controls For Statistical Reports 119

ExaGrid Site-level Statistic Reports 122

ExaGrid Appliance-level Statistics Reports 126

General Reports 133

Replication Topology Report 134
ExaGrid-level and ExaGrid Site-level Servers Report 136
ExaGrid-level and ExaGrid Site-level Network Status Report 136
ExaGrid Site-level Share Limits Report 136
ExaGrid Site-level and ExaGrid Appliance-level Event Reports 137
ExaGrid Site-level and ExaGrid Appliance-level Alarm Reports 138
ExaGrid Appliance-level Detailed Hardware Information 138
ExaGrid Appliance-level Software Upgrade History 139
Daily Status Reports 139

Monitoring Your ExaGrid 141

SMTP Emails 142
Configuring Outgoing Email Servers For SMTP Emails 142
Configuring SMTP Emails 146
SNMP Traps 149
Modifying SNMP Trap Destinations 150
Enabling SNMP on an ExaGrid Appliance 151
Status Monitor 152
Configuring the **Daily System Diagnostic Reports'** Delivery Options 154
Delivering Outstanding Report Data 156
Advanced Settings 157
ExaGrid MIB 157
Standard MIB Objects supported by ExaGrid 157
Example hrStorage MIB Objects 159
ExaGrid Specific MIB Objects 159

How to Calculate MIB Components 159
System Logging 161
Accessing the Syslog Management Page 162
Adding Syslog Servers to an ExaGrid Site 163

ExaGrid Maintenance 164

Shutting Down and Restarting an ExaGrid Appliance 165
Software Upgrade 166
Adding Additional ExaGrid Appliances 167
Hub Site and Spoke Sites 168
Reconfigure a Stand-alone Hub Site to a Spoke Site 169
Adding a Spoke Site to a Hub Site 169
Defining NTP Servers 172
Windows® NTP Servers 173
Replacing Disks 174
Disk Numbering 175
Replacing Power Supplies 175
Replacing Fans 176

Troubleshooting 177

Monitoring Status of Ongoing Operations 177

Disk Safety Halt Protection 178

Network Debugging Tools 179

Notifications 179

Consumption Issues 180

Landing Zone Tier Consumption 181

Landing Zone Tier used By Retention Tier 182

Retention Tier Consumption 182

Replication 183

Performance Tuning 184

Introduction

ExaGrid's tiered backup storage appliance is used as a target for your backup application.

Caution – ExaGrid **HIGHLY** recommends working with your ExaGrid Support Engineer to take advantage of ExaGrid's security features including Retention Time Lock and Two Factor Authentication. See ***"Managing and Securing Access" on page 23*** for detailed descriptions of ExaGrid's security features.

This chapter provides a high-level overview of the ExaGrid's features and capabilities.

Caution – Do not install third party software on your ExaGrid Appliance. Installing third party software can result in a loss of data and void your ExaGrid Warranty.

ExaGrid appliances differ in capacity, physical size and network connectors. All ExaGrid Appliances run the same ExaGrid software and can be commingled in an ExaGrid Site.

Shares

ExaGrid Shares are mount points to which your backup application backs up data.

There are two basic types of ExaGrid Shares:

- **Primary Shares:** Mount points created on ExaGrid Appliances to which your backup application can write.
- **InstantDR Shares:** Replicas of Primary Shares.

For details see ***"ExaGrid Shares" on page 51***

ExaGrid Hub Sites and Spoke Sites

The ExaGrid uses a hub and spoke topology in which there is a single ExaGrid Site known as the hub, connected to one or more ExaGrid Sites known as spokes.

Note – ExaGrid Hub Sites can replicate shares to one or two spoke sites. ExaGrid Spoke Sites can replicate shares to their Hub Site; the share replicated to the Hub Site can then be replicated to another Spoke Site. ExaGrid Spoke sites cannot replicate shares between each other.

When logged into an ExaGrid Appliance on a hub site you can:

- See the hub site and all spoke sites displayed in the ExaGrid user interface's navigation tree. The hub site is always listed as the top-most site in the navigation tree.
- View reports for the hub site and all spoke sites
- View events for the hub site and all spoke sites
- Perform hub and spoke site related management tasks

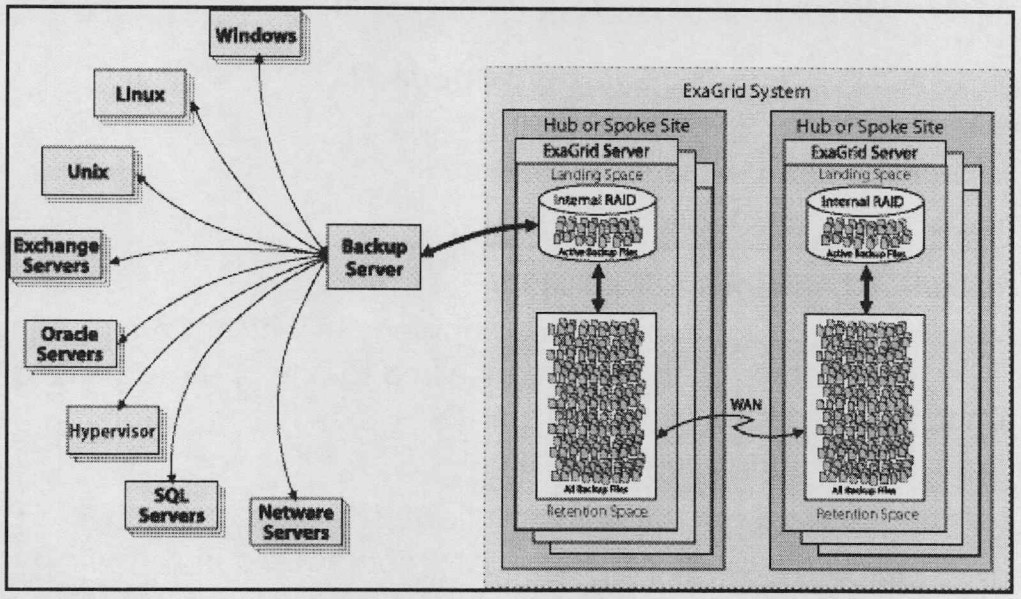
When logged into an ExaGrid Appliance on a spoke site you can:

- See the spoke site and the hub site displayed in the ExaGrid user interface's navigation tree. Other spoke sites in the system are not displayed.
- View reports for the spoke site

- View events for the spoke site
- View shares on the hub to which the spoke shares replicate
- Perform spoke site related management tasks

Data Flow

The following diagram details the data flow descriptions presented in this section:



Data flows into an ExaGrid Share from a backup application:

- Backup application writes to an ExaGrid share.
- When the backup is complete, the ExaGrid deduplication engine will deduplicate the backed up data.

Note – As more and more backups land, are retained, and deduplicated, deduplication ratios will improve.

- A full copy of the most recent backup is maintained in the Landing Zone Tier.
- The deduplicated versions are kept in the Retention Tier.
- In multi-site ExaGrid environments, you can specify whether or not to maintain a copy of a share on a second or optionally third ExaGrid Site.

When a backup application requests a restore:

- Since most restores are done from the most recent backup, the E most recent backup is kept in its entirety. This ensures extremely fast restores.
- Restores from an older backup are done by re-assembling the backup from backup versions.

Logging In

You can access the ExaGrid user interface through a web browser on your network. To log in to the ExaGrid user interface:

1. Open a browser and enter the URL or IP address of an ExaGrid Server. You can specify any ExaGrid Server. For example: `https://ExaGridServerName` or `https://192.168.55.3`

   To take advantage of all of your ExaGrid's capabilities, ExaGrid recommends that you log in using Hyper Text Transfer Secure (**HTTPS**) Protocol or employ TLS certificates.

2. Press **Return**. The ExaGrid Login screen is displayed.

3. Enter a user name and password for either an:
   - ExaGrid local user
   - Active Directory user or group that has been mapped into an ExaGrid role. For details, see ***"Managing Active Directory" on page 38***.

4. If two-factor authentication is enabled for your user, when prompted, provide the access code sent to your cell phone. See ***"Two-Factor Authentication" on page 35***.

5. Click **OK** and the ExaGrid user interface is displayed.

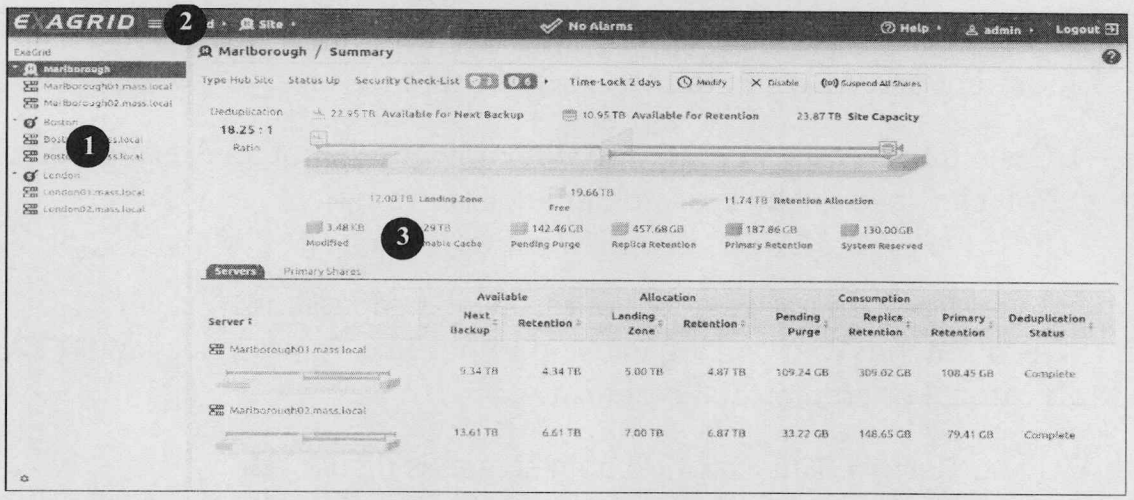
If you log in to an ExaGrid Hub Site, your user's role will determine what you can manage and view in the ExaGrid Hub site and its spokes. If you log in to an ExaGrid Spoke Site, your user's role will determine what you can manage on the spoke site, and what you can view on the spoke site and its associated hub site.

For details on local users and their roles see ***"User Roles" on page 29***.

The ExaGrid User Interface

ExaGrid presents a unified, browser-based user interface for all ExaGrid Sites and ExaGrid Appliances in an ExaGrid environment. A single login gives you reports on, and administrative access to, all ExaGrid Sites and ExaGrid Appliances in your ExaGrid environment.

The following screen capture details the main components of the ExaGrid user interface when ExaGrid Site is selected:.



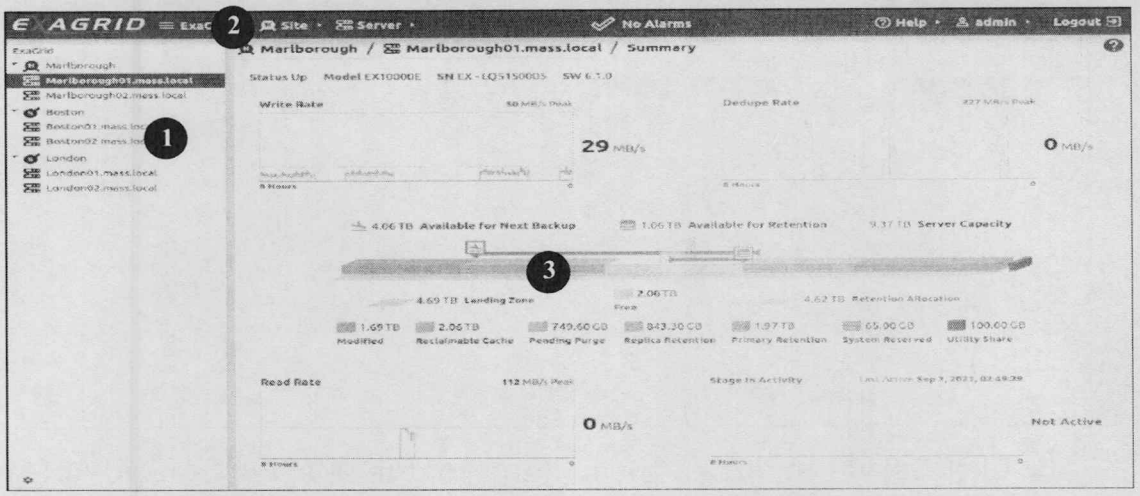
1. **Navigation Tree:** A tree view of the ExaGrid Sites and ExaGrid Appliances in the ExaGrid System. The hub site is always displayed as the top-most site.

2. **Main Menu:** Drop down menus that support functions for the currently selected item in the navigation tree.

3. **Report/Management Area for Sites**:
   - Type: Identifies the site as either a hub or spoke
   - Security checklists: These lists allow you to quickly determine whether the security settings in your ExaGrid Site meet ExaGrid's recommended best practices. Click on a list item to display the page where the security setting can be configured. For details on ExaGrid's security and access best practices. See ***"Managing and Securing Access" on page 23***.

- Time Lock: Displays the site's Retention Time-Lock setting in days and allows you to make Retention Time-Lock change requests to the site's Security Officer. See ***"Retention Time-Lock Overview" on page 25***.
- Suspend All Shares: If a ransomware or other malicious software attack is detected, you can suspend all shares in the ExaGrid Site and if necessary, begin recovering from the event. See ***"Recovering From Malicious Software Attacks" on page 102***.
- High-level deduplication and consumption reports for the site, its servers, and its shares

The following screen capture details the main components of the ExaGrid user interface when ExaGrid Appliance is selected



1. **Navigation tree:** A tree view of the ExaGrid Sites and ExaGrid Appliances in the ExaGrid System. The hub site is always displayed as the top-most site.

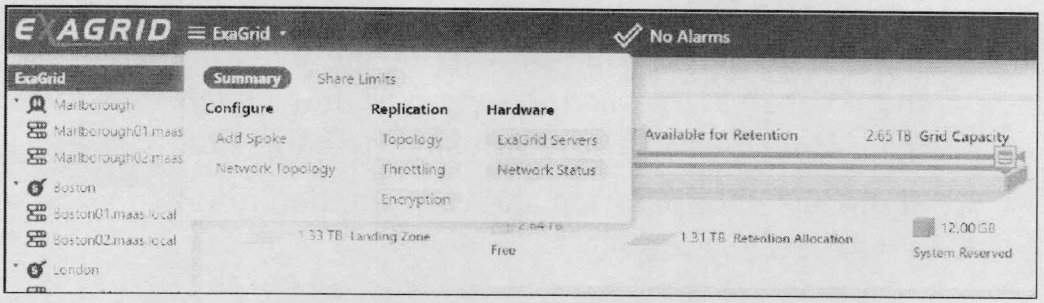
2. **Main menu:** Drop down menus that support functions for the currently selected item in the navigation tree. See ***"ExaGrid Main Menu Drop Downs" on page 7***.

3. **Report/Management Area**: Provides:
   - Graphs that detail Write Rates, Deduplication Rates, Read Rates, and Stage in Activity.
   - A graphical representation of the capacity and consumption of the selected ExaGrid Appliance.

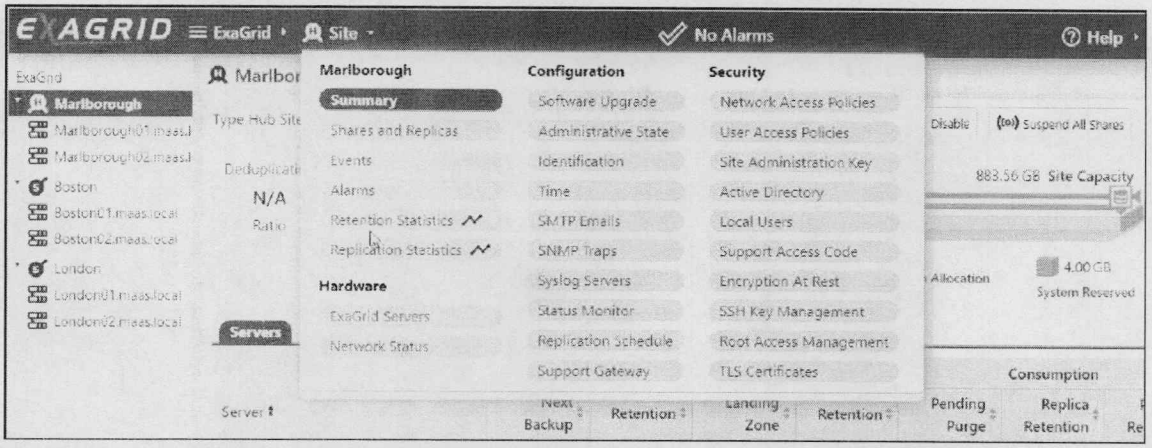
ExaGrid Main Menu Drop Downs

ExaGrid's main menu has drop down menus specific to the ExaGrid, its Site(s), Server(s), Help, and the currently logged in user:

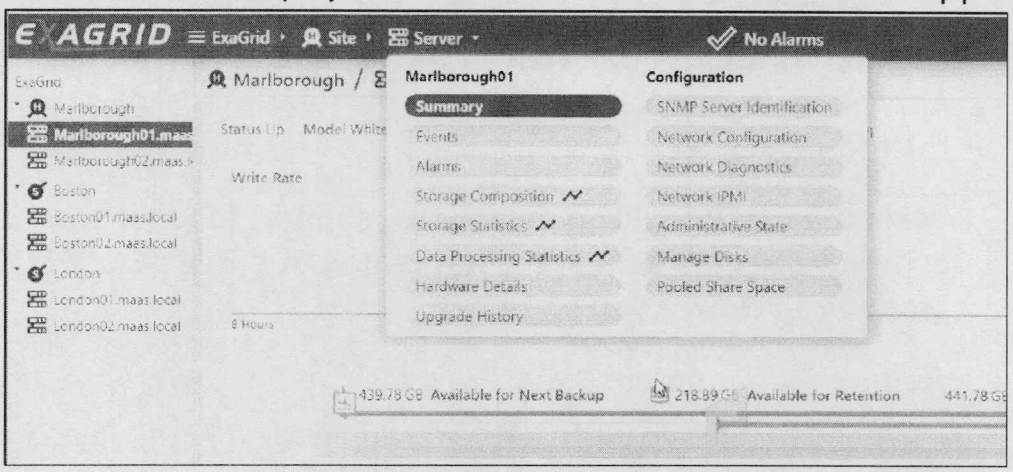
- Click **ExaGrid** to display menu items for ExaGrid.



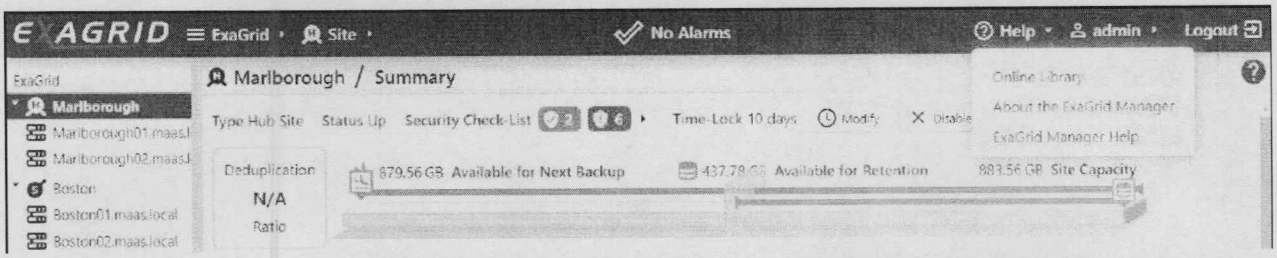
- Click **Site** to display menu items for the selected ExaGrid Site.



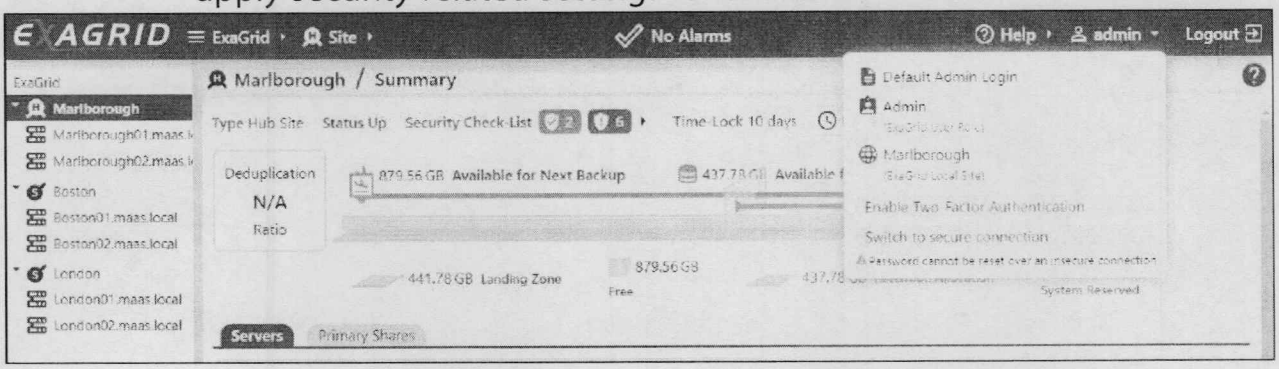
- Click **Server** to display menu items for the selected ExaGrid Appliance.



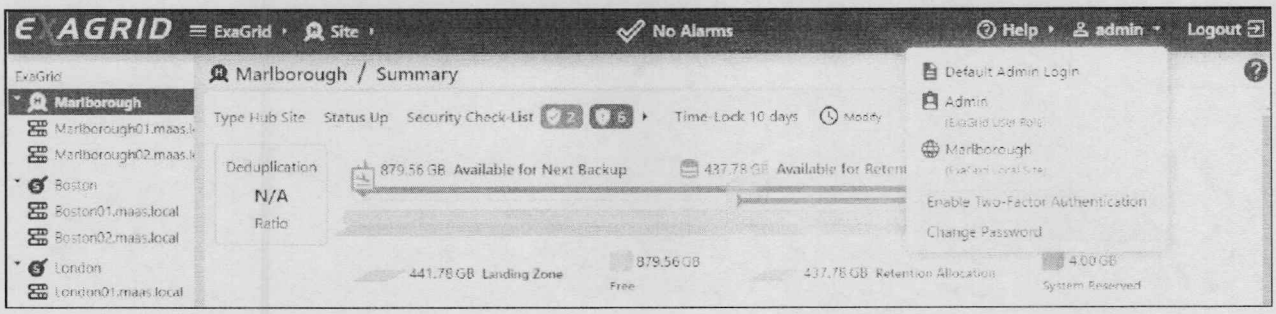
- Click **Help** to display a help menu:



- Click the **name of the currently logged in user** and a drop down is displayed that allows you to view information about the user and apply security related settings for the user:

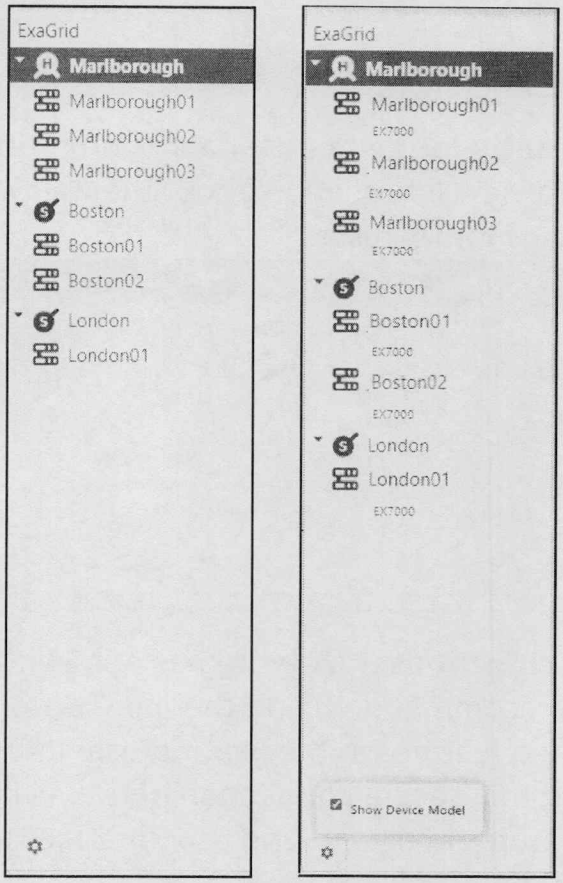


In the above example, the **current user (Admin)** has not Switched to a **Secure Connection** (not recommended) and therefore does not have access to all role-related features in the ExaGrid user interface. Once the user has switched to a secure connection, they will have access to all role-related features in the ExaGrid user interface and the contents of the drop down menu will change:



Show Device Model

The ExaGrid left-hand navigation provides a toggle the reveals the model numbers for each ExaGrid Appliance in your ExaGrid Sites. For Example:

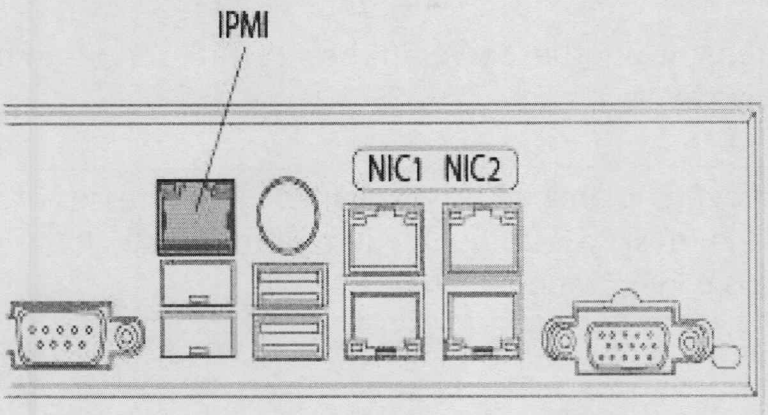


Networking

Depending upon the model, ExaGrid Servers come with two, four or six network interface connectors (NICs). By default, all NICs are 1 Gb, but 10 Gb and 40 Gb NIC options are available.

Network ports are located in the back of your ExaGrid Appliance. The actual location varies by ExaGrid Model. NIC ports are used for backup and administration and are labeled, the IPMI port is a standard 1GbE port without a label.

The following is an example of the back of an ExaGrid Appliance - note the labeled NIC ports and the unlabeled IPMI port.



Network Configuration Rules

- At least one network interface must allow ExaGrid traffic from All Sites.This rule applies to single-site systems as well as multi-site systems.
- All interfaces configured for Any Site traffic must use an address that is reachable from all such addresses on all ExaGrid Appliances in the ExaGrid environment - i.e. all hub Sties and all Spoke sites. An error will be returned if an interface set to All Sites cannot logically reach an interface in another site that is set to All Sites. This is a logical evaluation only based on IP networking rules - there is no testing done of actual physical connectivity.
- At least one network interface must allow Backup traffic.
- For multi-site systems, when changing ExaGrid traffic settings for ExaGrid Appliances in one ExaGrid Site, wait for the settings to take effect before changing the settings in another ExaGrid Site.
- If you rename an ExaGrid Appliance:
  - If the server belongs to an Active Directory domain, its name cannot be changed without first leaving the domain. After the name is changed, the server can be added back into the Active Directory domain.
  - Do not rename another server in the site until servers in the site see the newly changed name.

Note – Redefining an ExaGrid Appliance's IP addresses or name will in most cases require you to also update your backup job configurations.

Network Settings

Note – If you make changes to the Network Settings page, messages will be displayed that evaluate your choices.

The following list details the network settings allowed on the Network Settings page:

- **Name:** The name of each interface for this ExaGrid Appliance. If the ExaGrid Appliance is a member of an Active Directory Domain, then its fully qualified domain name (FQDN) must be used.

  An ExaGrid Appliance, depending on the model, will have two or more physical interfaces. Interfaces are typically used directly, but can be bonded together into virtual interfaces.

- **Type:** The speed of the network interface.
- **Link:** Indicates the links connection status: A check mark indicates the connection status is OK. An X indicates the connection status is disconnected. A question mark indicates the connection status is unknown. A triangle indicates that the link status is degraded.
- **VLAN**: Allows tagging an IP address with the specified VLAN ID. Use the + link under **Traffic** to add an IP address and/or VLAN ID.
- **Enabled:** A check mark indicates the interface is enabled.
- **IP MTU:** Maximum size of IP packets sent on the interface. In general, the maximum Ethernet packet size allowed on networking equipment connected to this interface must be larger than this number - refer to your networking equipment documentation
- **DHCP:** Whether DHCP is enabled.
- **IP Address:** The IP address assigned to the interface.
- **Mask:** The network mask applied to the interface.
- **Gateway:** The network gateway used by interface.
- **Traffic, ExaGrid:** Default setting is ***All Sites*** - All ExaGrid Appliances in this site and others can use this interface to replicate and balance data and communicate between each other. All addresses configured for Any Site traffic must be reachable from all such addresses on all ExaGrid Appliances in the ExaGrid environment. An error will be returned if an interface set to All Sites cannot reach an interface in

another site that is set to All Sites. In most cases All Sites will be the setting used for the interface. The other options are used only when fine tuning your ExaGrid Appliance is required:

Local Sites only ExaGrid Appliances in the site can use this interface to balance data and communicate with other ExaGrid Appliances in this site. You can use this setting to add additional bandwidth in a site without having to provision route-able network ports to your switch or when some interfaces are on a *site.local* private network.

None: Disallows any ExaGrid traffic from flowing through this interface.

- **Traffic, Backup:** Default is disabled (unchecked). This setting allows backup traffic to flow through its associated interface.

Caution – If a backup job is pointed at an interface whose Backup Traffic setting is disabled, the backup job will fail.

- + Allows you to apply multiple address definitions to a single network interface.
- **ExaGrid Server Name:** The name of the ExaGrid Appliance. Unqualified names can be up to 55 character long. Fully qualified names can be up to 63 characters long.
- **Default Gateway:** Static or DHCP
- **DNS Servers:** Name of DNS server. You can specify one or two DNS server names
- **DNS Search Path:** A space-separated list of domains. When looking up the address for unqualified host names on this server. Each domain will be appended to the name until one resolves.

Bonding

Network interfaces (NICs) can be bonded. Doing so provides a fall-back should one NIC fail. A bond requires at least two NICs. Bonded NICs must be of like type. For example, you cannot bond a 1GbE NIC with a 10 GbE NIC.

Caution – Bonding NICs does not automatically increase network bandwidth between the ExaGrid Appliance and the backup application(s). Work with your ExaGrid Customer Support engineer on the proper switch port configurations and backup configurations required to produce the concurrent backup streams and proper network paths that result in increased network bandwidth.

Ports Used Between ExaGrid Sites

To join ExaGrid Sites and replicate their data, the following port/protocols must be opened in the firewalls between the sites:

Sites Joined Using IPsec Tunnels

When joining an ExaGrid Spoke Site to an ExaGrid Hub Site, ExaGrid recommends enabling the IPsec option. Doing so requires fewer open ports between the ExaGrid Spoke Site and the ExaGrid Hub Site.

The following table lists the required ports for IPsec Tunnels:

Port	Protocol
500	UDP
4500	UDP

Sites Joined NOT Using IPsec Tunnels

When joining an ExaGrid Spoke Site to an ExaGrid Hub Site, if you do not enable the IPsec option, the following ports must be open between the ExaGrid Spoke Site and the ExaGrid Hub Site:

Port	Protocol	Purpose
22	TCP	SSH (including rsync)
88	TCP & UDP	krb5kdc (Kerberos)
123	UDP	NTP
464	TCP & UDP	kadmind (Kerberos)
749	TCP	kadmind (Kerberos)
5433	TCP	PostgreSQL
5434	TCP	PostgreSQL
5435	TCP	PostgreSQL
7201	TCP	Topology Service
8000	TCP	Management Service
28700 – 28799	TCP	ExaGrid Services
32768 – 61000	TCP	Replication Service (Ephemeral Ports)

Enabling/Disabling IPsec Tunnels Settings

Existing ExaGrid Sites can switch between not using and using IPsec Tunnels.

To enable/disable the use of IPsec Tunnels:

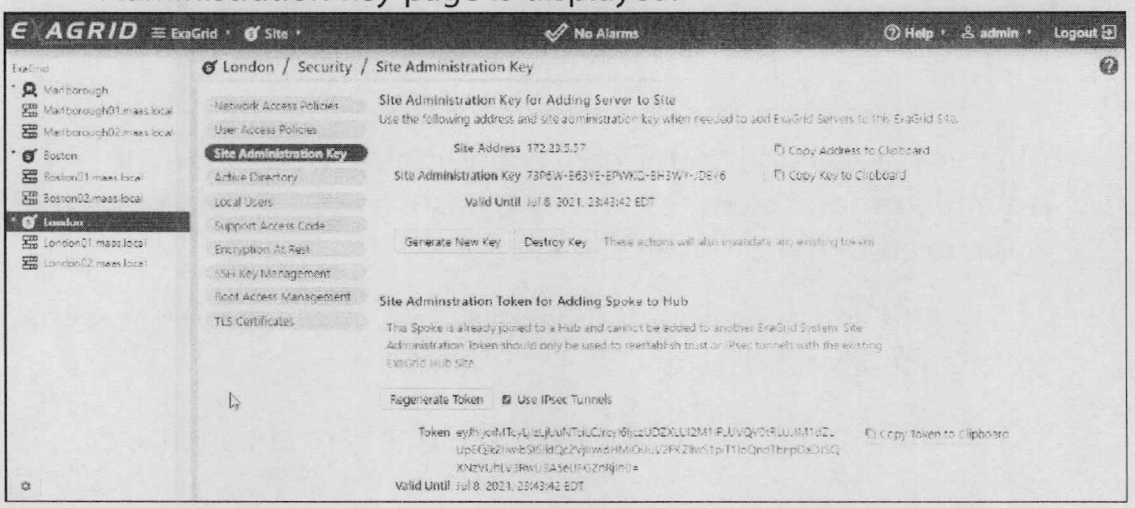
1. Ensure the required ports are open. See ***"Ports Used Between ExaGrid Sites" on page 15***.

2. Log into the ExaGrid Hub Site as a user assigned the Admin role.

3. Select the ExaGrid Site that will change its IPsec settings.

4. In the top, main menu, click **Site**, and all menu options for the ExaGrid Site are displayed.

5. Under **Security**, select **Site Administration Key**, and the Site Administration key page is displayed:



6. Under **Site Administration Token for Adding Spoke to Hub:**

- Select whether the Spoke Site will use IPsec tunnels (recommended) to communicate with the Hub Site.

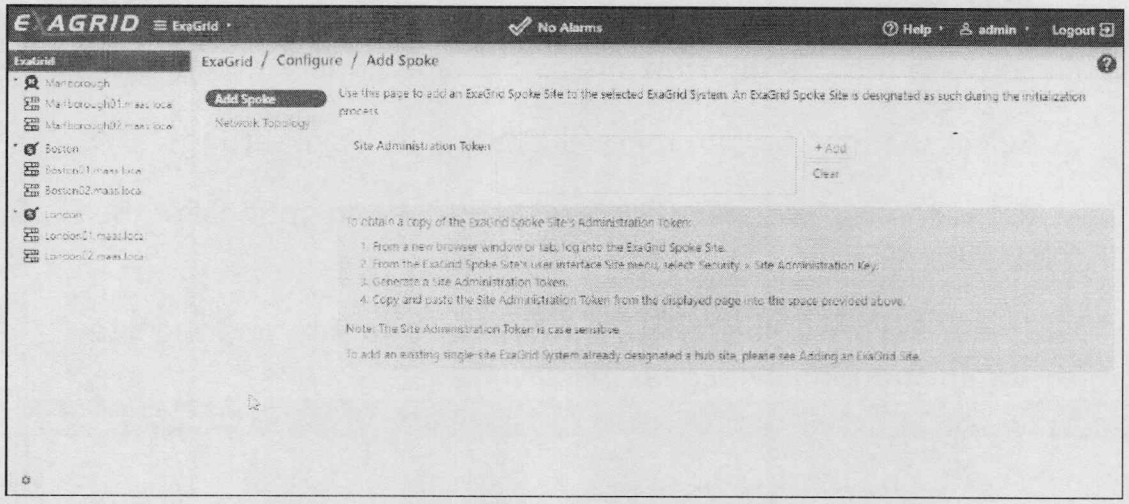
Note – This option controls the ports needed for replication between the two ExaGrid Sites. See ***"Ports Used Between ExaGrid Sites" on page 15***.

- Click **Generate Token** and the page is populated with the token.

7. Click the **Copy to Clipboard** button next to the new token. This will copy the token to the clipboard and allow you to paste the token to the ExaGrid Add Spoke page.

8. In the top, main menu click **ExaGrid** and the menu items for ExaGrid are displayed.

9. Under **Configure**, select **Add Spoke**, and the Add Spoke page is displayed:



10. In the ExaGrid Add Spoke page, right-mouse click in the **Site Administration Token** text box and **paste** the Spoke Site's token that was copied to the clipboard.

11. Click **Add** and a dialog box indicating the Spoke Site's IPsec settings are changed is displayed.

12. Click **OK** and the Spoke Site's IPsec settings are changed.

TLS Certificates

TLS certificates eliminate the browser security warnings associated with pages in the ExaGrid browser-based user interface that require an HTTPS connection.

TLS certificates used with an ExaGrid Server must:

- Have a common host name and a DNS name that matches the DNS name in the browser. IPs are not allowed.
- The browser must know the Certification Authority that signed the certificate.

TLS certificates are applied to ExaGrid Servers from an ExaGrid Site's Security menu's TLS Certificates page. Only users with the Admin role or Support role can apply certificates.

From the TLS Certificates page you can:

- Keep the ExaGrid default certificate.
- Upload a Personal Information Exchange File.
- Configure an SCEP Server to automatically update and serve up certificates.

- Revert to the ExaGrid default certificate. This option is only available if TLS certificates are in use.

Caution – When reverting back to the ExaGrid default option, you MUST ensure that HSTS is disabled.

ExaGrid recommends that each ExaGrid Server in an ExaGrid Site use the same TLS settings.

When a certificate approaches its expiration date, the ExaGrid will generate an alarm to remind you to apply an updated certificate.

Applying TLS Certificates

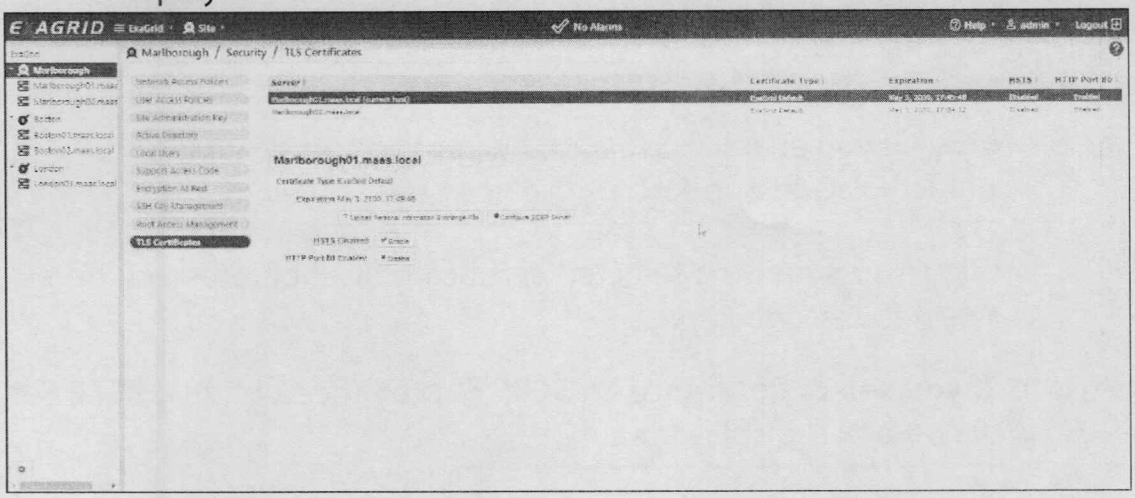
Note – When you change TLS settings, the ExaGrid web server will restart. During that brief interval, connection to the ExaGrid will be lost.

TLS settings are applied, one at a time, to each ExaGrid Server in an ExaGrid Site.

To apply a TLS certificate to an ExaGrid Server:

1. From the ExaGrid left-hand navigation frame, select the ExaGrid Site in which the ExaGrid Server resides.
2. In the top, main menu select **Site** and all menu options for the site are displayed.

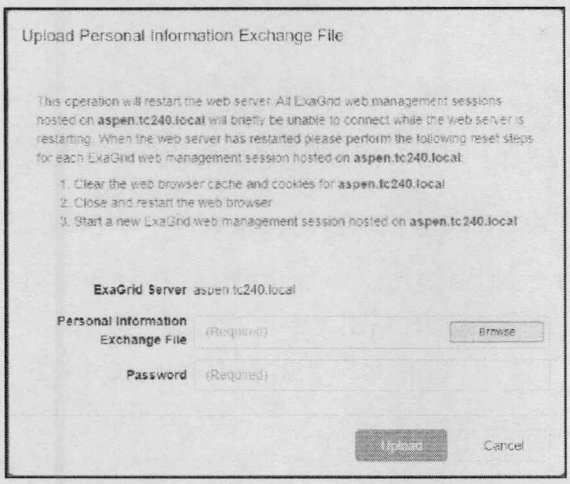
3. Under **Security**, select **TLS Certificates** and the TLS Certificates page is displayed



4. From the list of ExaGrid Servers, select the ExaGrid Server to which the certificate will be applied.

5. Select the certificate to be applied:

   a. If you select **Upload a Personal Information Exchange File,** the Personal Information Exchange File dialog box is displayed**:**



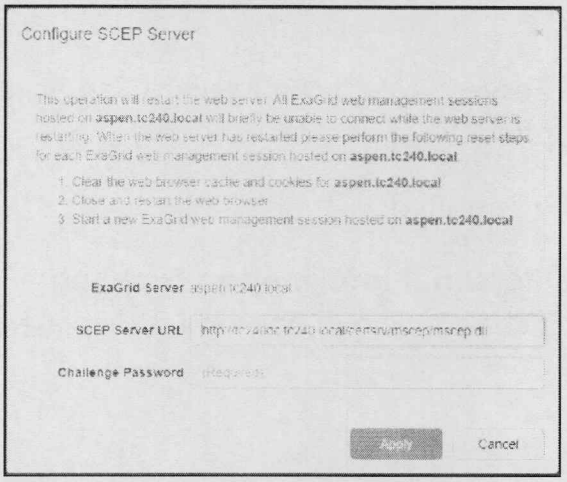
   - Enter the path, or browse to the Personal Information Exchange File.
   - Enter the Password associated with the Personal Information Exchange File.
   - Click **Upload** and the Personal Information Exchange File will be uploaded.

- Once you have confirmed that the certificate is good and the browser warnings in the ExaGrid GUI pages that require HTTPS are gone, enable/disable Port 80 and HSTS according to your corporate best practices.

Note – If you enable HSTS and the applied certificate is bad, contact ExaGrid Support to resolve issues you encounter.

- Click **Apply** and the selected certificated will be used on the selected ExaGrid Server.

b. **If you select Configure an SCEP Server**, the Configure SCEP Server dialog box is displayed**:**



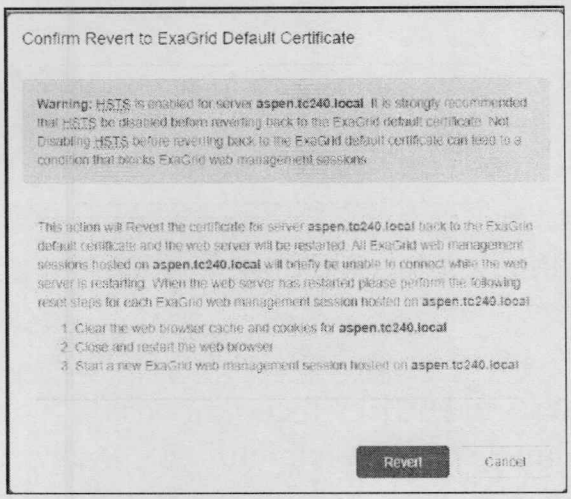
- **Enter the SCEP Server URL.**
- **Enter the Challenge Password associated with the SCEP server.**
- Once you have confirmed that the certificate is good and the browser warnings in the ExaGrid GUI pages that require HTTPS are gone, enable/disable Port 80 and HSTS according to your corporate best practices.

Note – If you enable HSTS and the applied certificate is bad, contact ExaGrid Support to resolve issues you encounter.

- Click **Apply** and the SCEP Server URL will be applied.

c. If you have an existing certificate you can select Revert to the ExaGrid default certificate and the Confirm Revert to ExaGrid Default Certificate dialog box is displayed:

Caution – When reverting back to the ExaGrid default option, you MUST first Disable HSTS.



- Click **Apply** and the certificate settings will revert to the ExaGrid default certificate.
- Enable/disable Port 80 according to your corporate best practices.

Note – If HSTS is enabled and you apply the default ExaGrid certificate, contact ExaGrid Support to resolve issues you encounter.

Once the TLS setting have been applied, the ExaGrid Server's web server will restart. During that brief interval, connection to the ExaGrid Server will be lost.

When the web server has restarted, you must:

1. Clear your web browser's cache and cookies.
2. Log out of the ExaGrid Server.
3. Close your web browsers.
4. Open a new browser session and log back into the ExaGrid Server.

Managing and Securing Access

Access to the ExaGrid user interface, its features, and backed up data is controlled in several ways:

Caution – In all cases, ExaGrid **HIGHLY** recommends configuring Retention Time Lock for a minimum of 10 days **AND** enabling two-factor authentication on ExaGrid local user accounts assigned the Admin, Operator, or Security Officer role.

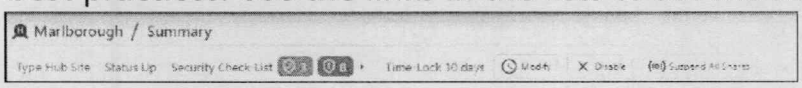
- The ExaGrid resides in your data center and your access protocols limit physical access to the ExaGrid and its data.
- Time-locks are set on deduplicated and retained data. This protects against ransomware and other malicious activity. For details see ***"Retention Time-Lock Overview" on page 25***.
- Two-Factor Authentication can be enabled on a user's account. ExaGrid **HIGHLY** recommends enabling this for all users. For details see ***"Two-Factor Authentication" on page 35***.

Security Alert - Employing **BOTH Retention Time Lock and Two Factor Authentication** are your best defense against ransomware and other malicious activity.

- Users can be assigned roles that limit their access to a specific set of ExaGrid functions. For details see ***"User Roles" on page 29***.

- ExaGrid Appliances can be members of an Active Directory Domain. ExaGrid roles can be mapped to users or groups in their server's Active Directory Domain. For details see ***" Managing Active Directory" on page 38***.
- User Access Policies define the backup users who have access to a share. For details see ***"User Access Policies" on page 59***.
- Network Access Policies that define network access to a share. For details see ***"Network Access Policies" on page 58***.
- Hardware options that employ Encryption at Rest and Boot Protection. For details see ***"Encryption Capable ExaGrid Appliances" on page 89***.

At the top of an ExaGrid Site's Summary page are drop down lists that detail whether the site's security settings meet ExaGrid's recommended best practices. Use the links in the lists to set the site's security settings:



Caution – ExaGrid **HIGHLY** recommends reviewing these security settings on a regular schedule, **including ExaGrid's Retention Time-Lock and Two Factor Authentication**. Doing so ensures that the maximum security settings are applied to your backed up data.

Retention Time-Lock Overview

ExaGrid's Tiered Backup Storage architecture has:

- A high-speed, disk cache that makes up ExaGrid's front-end Landing Zone Tier where the latest backup data resides.
- A separate Retention Tier that contains all deduplicated and retained data.

This proven tiered architecture lends itself to a unique, time-lock ransomware solution where:

> Data is written directly to the network facing ExaGrid Landing Zone. The backed up data is then kept in a "non-network facing" long-term retention tier. As data is put into the Retention Tier, it is deduplicated and stored in a series of objects and metadata. As with other object storage systems, the ExaGrid objects and metadata cannot be modified. This ensures that only new objects are created and only old objects are deleted when their defined retention date is reached.

Because the Retention Tier is not network facing and not accessible to ransomware and other malicious activity, a time-lock can be set on the ExaGrid Retention Tier that blocks deletes for up to 30 days.

This combination of a non-network facing Retention Tier, a definable period of time where delete operations are not performed, and objects that never change, protect ExaGrid's retained data from ransomware and other malicious activity.

If the data in the ExaGrid Landing Zone is deleted or encrypted, the data in the Retention Tier is not affected. As soon as an attack is identified, with a single click you can suspend (lock down) all shares in an ExaGrid Site and begin restoring backup data from the ExaGrid Retention Tier to your primary storage.

Key features of ExaGrid's Time-Lock Retention solution include:

- A Retention Time-Lock policy that can delay delete commands from 0 to 30 days.
- Required security officer approval for changes to time-lock settings.

- Compromised data backed up to the ExaGrid Landing Zone Tier is deduplicated and sent to the Repository Tier but does not delete or change previous backups in the Repository Tier.
- Two-factor Authentication protects against unauthorized access and changes to Retention Time-Lock setting. For details see ***"Two-Factor Authentication" on page 35***.
- Optionally, separate passwords for Administrators on Primary and Secondary (DR) ExaGrid Sites.
- The Retention Tier usually only needs 2% extra capacity per week for the Time-Lock. For example, setting the Time-Lock to 14 days typically will require only 4% of additional Retention Tier capacity.

For details on how to recover from a ransomware or malicious software attack, see ***"Recovering From Malicious Software Attacks, or a Loss of ExaGrid Appliances" on page 100***.

Modifying Retention Time-Locks

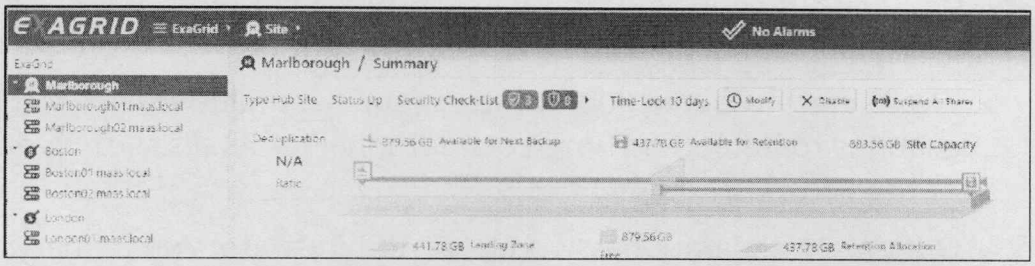
By default, ExaGrid's Retention Time-Locks are set to 10 days. For most customers the default setting will provide more than enough time to detect and then recover from a ransomware or malicious software attack.

Retention Time-Locks can be modified by any user assigned the Admin role. Retention Time-Locks can be manually set from 0 (not recommended) to 30 days.

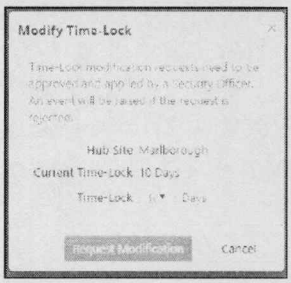
Changes to Retention Time-Locks require the approval of an ExaGrid User assigned the Security Officer role. Current time-locks stay in effect until the Security Officer approves a change. Before modifying Retention Time-Locks, ensure a user with the Security Officer role exists in the site and they are aware that a modification request is coming.

To modify Retention Time-Locks on shares in an ExaGrid Site:

1. Log into the ExaGrid Site as a user who is assigned the Admin role, and the site's summary page is displayed:

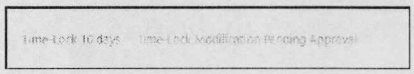


2. At the top of the page, next to the current time-lock setting, click **Modify** and the Modify Time-Lock dialog box is displayed:



3. From the drop down menu select the new time-lock period.

4. Click **Request Modification** and the following message will appear at the top of the Security Officer's default login page:

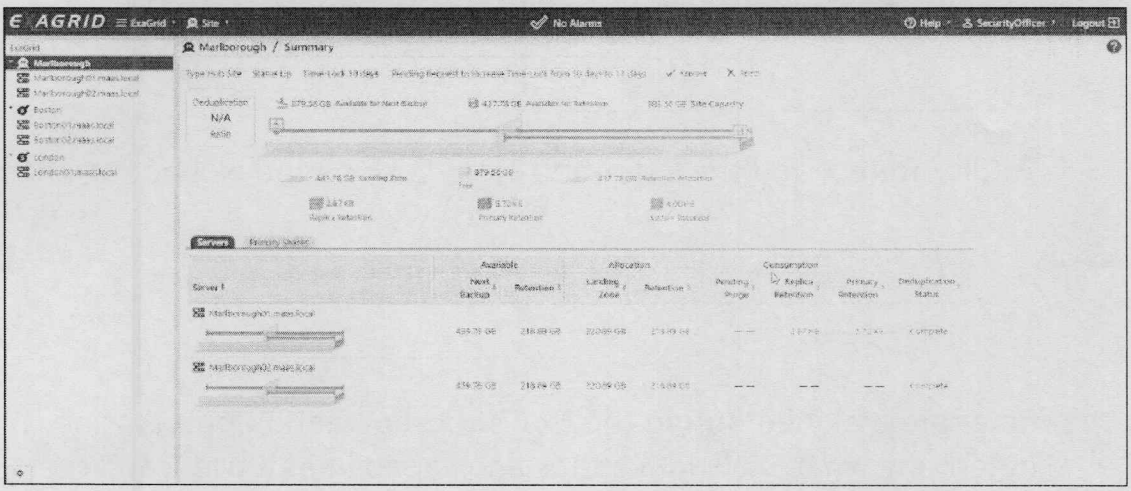


Approving and Rejecting Retention Time-Lock Modifications

It is the responsibility an ExaGrid Site's Local or Active Directory user assigned the Security Officer role to accept or reject modifications to a site's Retention Time-Locks.

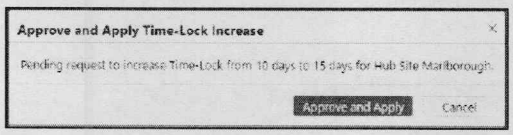
To approve or reject a Retention Time-Lock modification request:

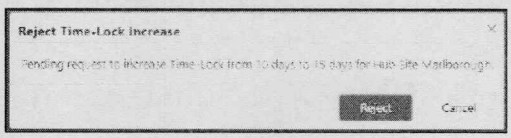
1. Log into the ExaGrid Site as a user who is assigned the Security Officer role, and the site's summary page is displayed:



2. At the top of the page, next to message that details the Time-Lock change request, click either **Approve** or **Reject**.

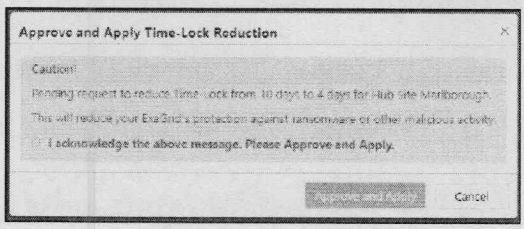
3. If this is a request to increase the Time-Lock period: clicking **Accept** or **Reject** displays a simple confirmation dialog box**:**





4. Click either **Approve and Apply** or **Reject** and the site's Retention Time-Lock is set accordingly.

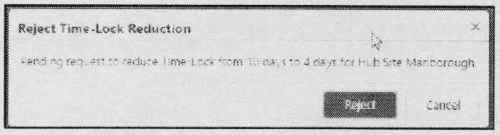
5. If this is a request to decrease the Time-Lock period, if you click **Accept**, a dialog box explaining the risks involved in decreasing the Time-Lock period is displayed:



6. Because of the increased risks involved, you must click the **I Acknowledge...** check box before you click Approve and Apply.

7. Click **Approve and Apply** and the Time-Lock setting for the site is changed.

8. **If t**his is a request to decrease the Time-Lock period, if you click **Reject**, a simple confirmation dialog box is displayed:



9. Click **Reject** and the Retention Time-Lock period will not be changed.

User Roles

Roles are assigned during the ExaGrid user creation process and determine what ExaGrid features and capabilities a user can access. See ***"Creating and Modifying ExaGrid Local Users" on page 31*** for details.

Each ExaGrid comes with one predefined ExaGrid user named Admin that is assigned the Admin role. The Admin role grants complete access to the ExaGrid user interface and can perform all management functions including creating new users.

Note – The Admin user role **CANNOT** approve or deny Retention Time-Lock change requests. Approving and denying such requests is the sole responsibility of the Security Officer role. See ***"Retention Time-Lock Overview" on page 25***.

Domain users, and domain groups can be to mapped an ExaGrid role. See ***" Managing Active Directory" on page 38*** for details.

The following list defines the roles that can be assigned or mapped:

- Admin: Grants full access to all ExaGrid features and can perform all management functions including creation of new users and power management. **As a best practice, only a limited number of users should be assigned this role.**
- Operator: Grants access to typical day-to-day operations such as share creation (but cannot modify or delete shares) without granting operating-system-level access to the entire ExaGrid environment. **As a**

best practice, most users should be assigned this role. Not assigning this role to at least one user will raise an alarm in the ExaGrid Site's security check list.

- Security Officer: Grants approvals or denials to changes to Retention Time-Lock settings. **As a best practice, only one user should be assigned this role.** Not assigning this role to at least one user will raise an alarm in the ExaGrid Site's security check list. See ***"Retention Time-Lock Overview" on page 25***.
- Viewer: Grants access to ExaGrid reports and status information. Users with the Viewer role cannot perform any day-to-day or system-level operations.
- UPS Operator: Grants scripts access to ExaGrid's power management features.
- Backup Only: Grants (backup applications) access to ExaGrid Shares for backup operations. This role does not give access to ExaGrid management functions.

Caution – Attempting to access ExaGrid CIFS shares using the **guest** account from certain versions of Windows will not succeed if your Windows username (domain) matches an ExaGrid user. To access an ExaGrid CIFS share in this case, use your Windows username rather than "guest".

User Role Idle-Timeout Settings

To help prevent unauthorized use of an ExaGrid user account, idle-timeouts are set on user roles. Roles with the greatest access have the shortest idle-timeout periods:

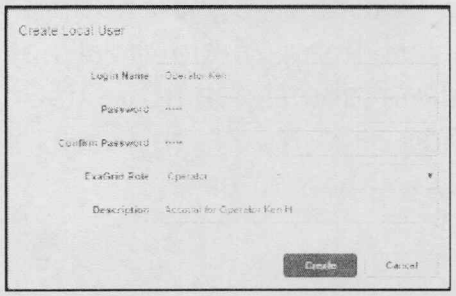
- Security officer, Admin, and Support role time out after fifteen minutes
- Operator role times out after one hour
- Viewer role times out after twelve hours

These timeout settings are not configurable.

Creating and Modifying ExaGrid Local Users

To create or modify a new ExaGrid local user:

1. Ensure that you are logged in to the ExaGrid as a user assigned the Admin role.
2. In the navigation tree, click the ExaGrid Site.
3. From the top, main menu, click **Site** and all menu options for the site are displayed.
4. Under **Security**, select **Local Users** and the Manage Local Users page is displayed.
5. If you are modifying an existing user, select the user then click **Modify** and the Modify Local User dialog box is displayed.
6. If you are creating a new user, click **New** and the Create Local User dialog box is displayed:



7. In the spaces provided enter a user name and password. See ***"Valid ExaGrid Local User Name Character Set" on page 32*** and ***"Valid ExaGrid Local User Password Character Set" on page 32***.
8. From the drop down menu select the required role.
9. In the space provided, enter a description of the user.
10. Click **Create or Apply**, and the local user is created or modified.

Valid Local User Names

When creating a new local user for a site, you cannot use a reserved Linux account name.

If you try to create a local user with a reserved Linux account name you will encounter an error stating that the account already exists. For example, the user name **operator** with a **lowercase "o"** is a reserved Linux account name and cannot be used for an ExaGrid Local User.

Valid ExaGrid Local User Name Character Set

Local user names must:

- Not contain more than 32 characters
- Begin with an upper or lower case letter A-Z or a-z

For the rest of the name, you can use any of the following:

- Upper/lower case A-Z
- Numeric 0-9
- . - _ (period, hyphen, underscore)

Valid ExaGrid Local User Password Character Set

Local user passwords cannot contain spaces but can contain any printable, 7-bit ASCII character.

Changing Your Password

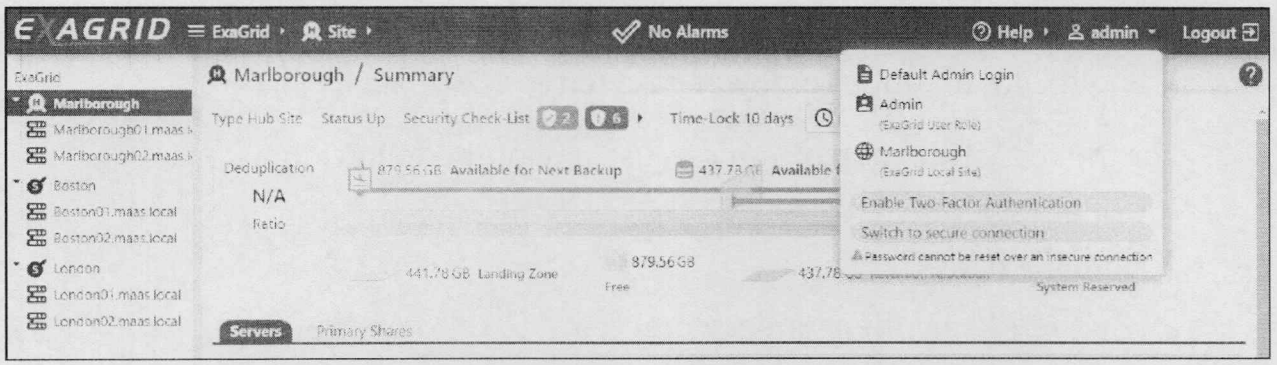
Most users are not assigned a role that allows them to change passwords for other local users. However, all local users can change their own password.

To change your password:

Note – In the following example, the user name is **Admin**.

---

1. In the main menu bar click your user name and a drop down menu is displayed:

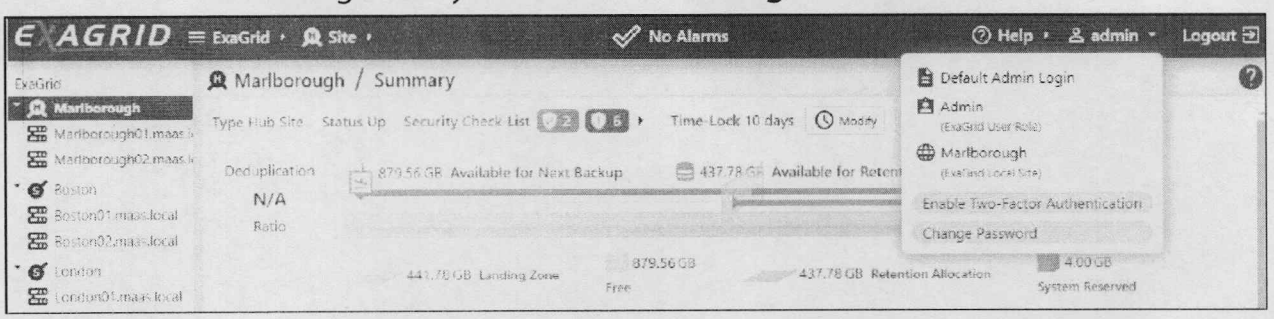


2. If you are not using a **Secure Connection** (not recommended) you must first select **Switch to a secure connection**.

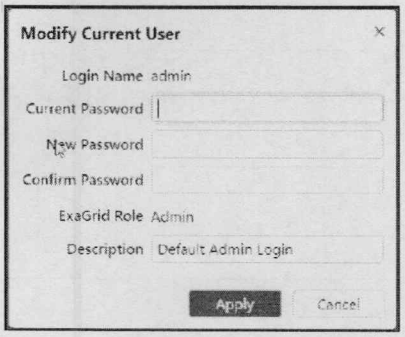
Caution – ExaGrid highly recommends that each user enables two-factor authentication. See ***"Two-Factor Authentication" on page 35***.

---

3. Once a secure connection has been established, the drop down menu will change and you can select **Change Password**:



4. Click **Change Password** and the Modify Current User dialog box is displayed:



5. In the spaces provided enter:

   a. Your current password

   b. The new password

Note – See ***"Valid ExaGrid Local User Password Character Set" on page 32***.

---

   c. The new password again for verification

   d. If needed, update the user description.

6. Click **Apply** and the new password is set.

Two-Factor Authentication

As a best practice, local users and active directory users assigned the following roles should set ExaGrid's two-factor authentication on their account.

- Admin
- Operator
- Security Officer
- Viewer

The following roles cannot use two-factor authentication:

- **The Backup Only role** is meant for backup applications writing to ExaGrid Shares.
- The UPS Operator role is meant for power control scripts.

Note – Two-factor authentication is set on a site-by-site basis. For example, setting two-factor authentication for the Security Officer on a hub site **WILL NOT** set two-factor authentication for the Security Officer on any of the hub's associated spoke sites.

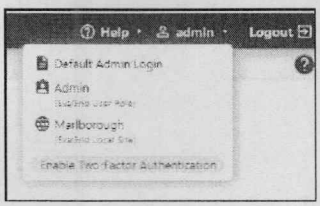
Setting Two-Factor Authentication

Before two-factor authentication can be set, an ExaGrid user must first install a third party two-factor authentication application on the device (cell phone, lap top, etc.) that will be used to authenticate their log in.

To set Two-Factor Authentication:

1. In the upper right-hand corner of the ExaGrid user interface, find the user account name you are currently logged in to. For example, in the following screen capture we are using the user named **admin.**

2. Click on the user account name.



3. From the drop down menu, select **Enable Two-Factor Authentication** and the Two-Factor Authentication dialog box opens:



4. If supported by your authentication application, scan the QR Code. For other applications you can manually enter the **Key** provided in the dialog box.

5. Your authentication application will generate a code on the device you use for authentication.

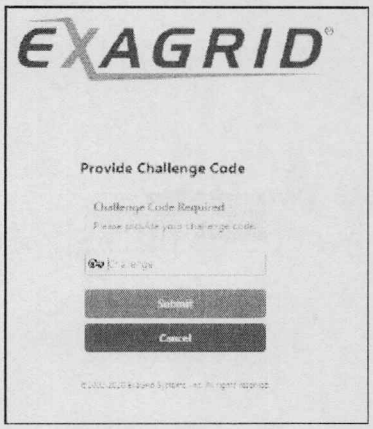
6. Enter the code in the Two-Factor Authentication dialog box's **Code** text box.

7. Click **Register**, and a list of recovery codes is displayed. These codes can be used (once each) to recover from the loss of the soft token.

8. Click **Download** and the list of recovery codes can be downloaded for safe keeping.

9. Click **Close** and two-factor authentication is enabled on the user account.

Going forward, use the two-factor authentication application on your device of choice to obtain a code. This code must be entered into the ExaGrid Challenge Code screen. For example:



Enter the code in the space provided then click **Submit**.

Managing Active Directory

Active Directory membership is defined at the ExaGrid Site level. All ExaGrid Appliances in a multi-server ExaGrid Site must belong to the same Active Directory Domain. All ExaGrid Sites in a multi-site ExaGrid environment do not have to belong to the same Active Directory Domain.

Note – Active Directory trusts can be used to give a user access to an ExaGrid site in a different domain.

Once the ExaGrid Appliances in an ExaGrid Site are added to a domain, users and groups in that domain can be mapped into ExaGrid roles. When a user or group is mapped into a role, they will have access to all ExaGrid features associated with that role.

Active directory users and groups with mapped roles can be added to a share's User Access Policy. See ***"Share Access Policies" on page 42*** for details.

ExaGrid User Interface Access Using Active Directory Credentials

Microsoft supports a wide range of characters in Active Directory usernames and passwords. However ExaGrid's user interface login is currently limited to:

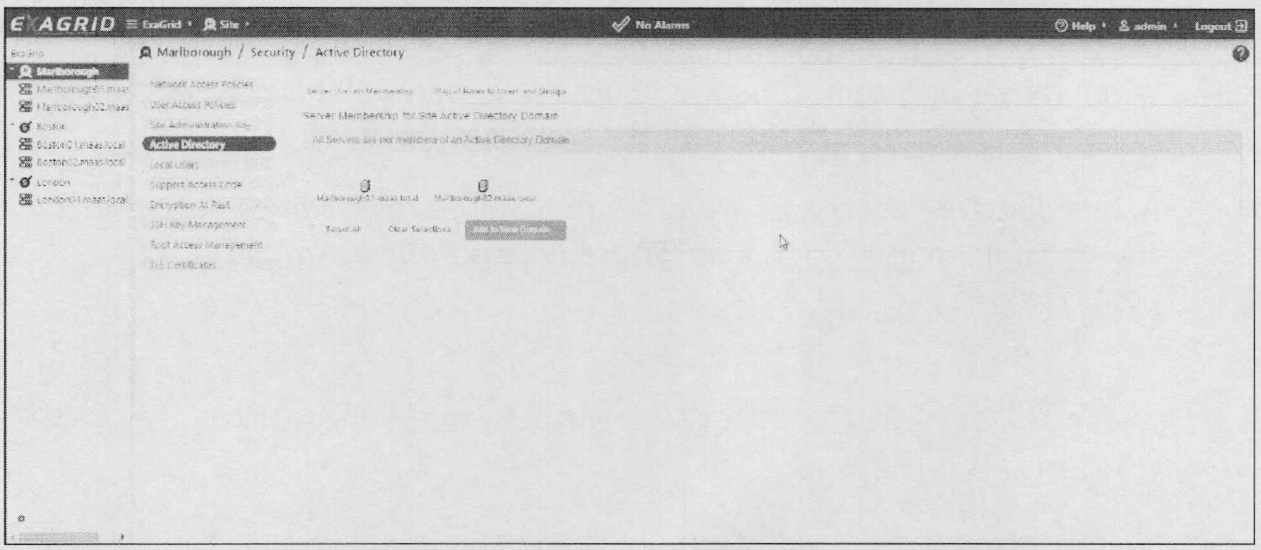
Active Directory usernames and passwords that contain any printable, 7-bit ASCII character including spaces. See***"Mapping an Active Directory User or Group to an ExaGrid Role" on page 40***.

Adding ExaGrid Appliances to An Active Directory Domain

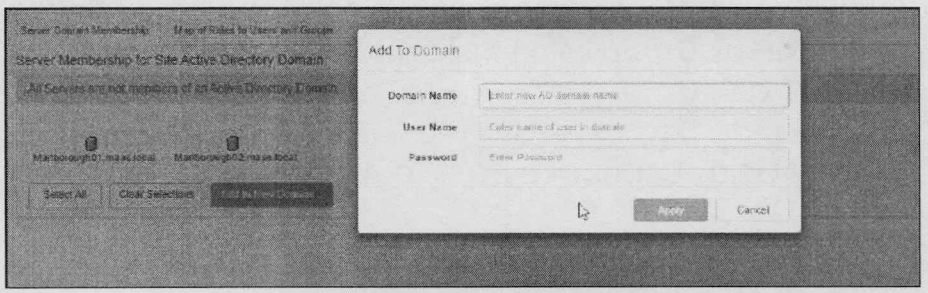
To add ExaGrid Appliances to an Active Directory Domain:

Note – You must be logged in through Hyper Text Transfer Secure (**HTTPS**) Protocol otherwise the Manage Active Directory page will be view only.

1. Log into a user account that has the Admin role.
2. In the left-hand navigation tree, select the ExaGrid Site that contains the ExaGrid Appliances to be added to the Active Directory Domain.
3. From the top, main menu select **Site** and all menu options for the site are displayed.
4. Under **Security**, select **Active Directory** and the Server Domain Membership tab for Active Directory is displayed:



5. Click **Select All.**
6. Click **Add to New Domain** and the Add to Domain dialog box is displayed:



7. In the spaces provided enter the Domain Name, the domain User Name, and the domain Password for the specified user. The User and Password must have sufficient permissions to "Join a computer to a domain" or the operation will fail.

8. Click **Apply** and the selected ExaGrid Appliances in the ExaGrid Site are added to the specified domain.

Mapping an Active Directory User or Group to an ExaGrid Role

Note – If a suitable Domain User or Group containing Users that need access to the ExaGrid does not exist, it must first be created using standard Active Directory management tools.

To map an Active Directory User or Group to an ExaGrid role:

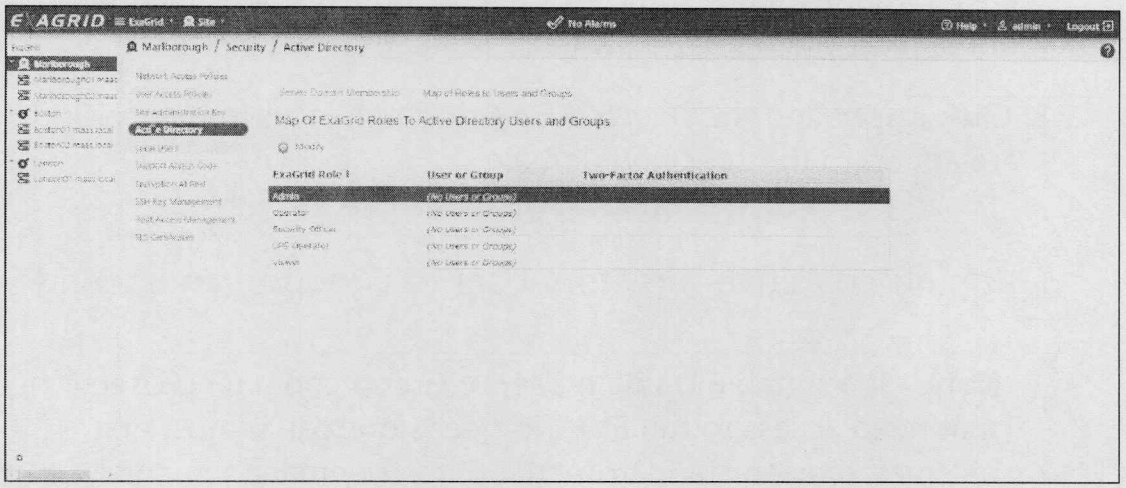
1. Log into a user account that has the Admin role.

2. In the left-hand navigation tree, select the ExaGrid Site that contains the ExaGrid role to be mapped into an Active Directory Group or user.

3. From the top, main menu click **Site** and all menu options for the site are displayed.

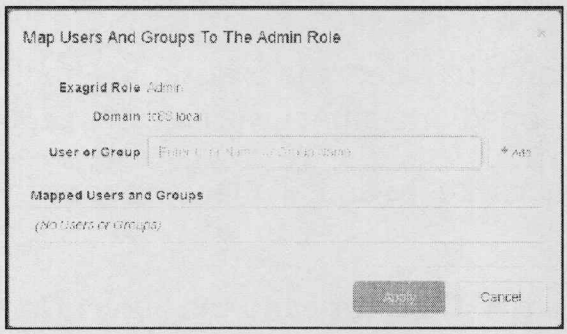
4. Under **Security**, select **Active Directory** and the Server Domain Membership tab for the Manage Active Directory is displayed.

5. Click the **Map of Roles to Users and Groups** tab and a table is displayed that lists how roles are mapped into users or groups is displayed:



6. Select the role to be mapped into a user or group.

7. Click **Modify** and the Map Users and Groups to Role dialog box is displayed:



8. In the space provided, enter the user or group name to map to the selected role.

9. Click **Apply** and the user or group is mapped to the ExaGrid role. The specified user or any user in the group can access the ExaGrid with this role using their Domain credentials.

Share Access Policies

Policies that define share access are created at the ExaGrid Site level. Depending on the share type, you must create at least one:

- User Access Policy that defines the backup application users who have access to a share.
- Network Access Policy that defines network access to a share.

Note – Veeam Shares do not require a Network Access Policy.

A single User and Network Access Policy can be used by multiple shares.

For details see ***"Share Access Policies" on page 58***.

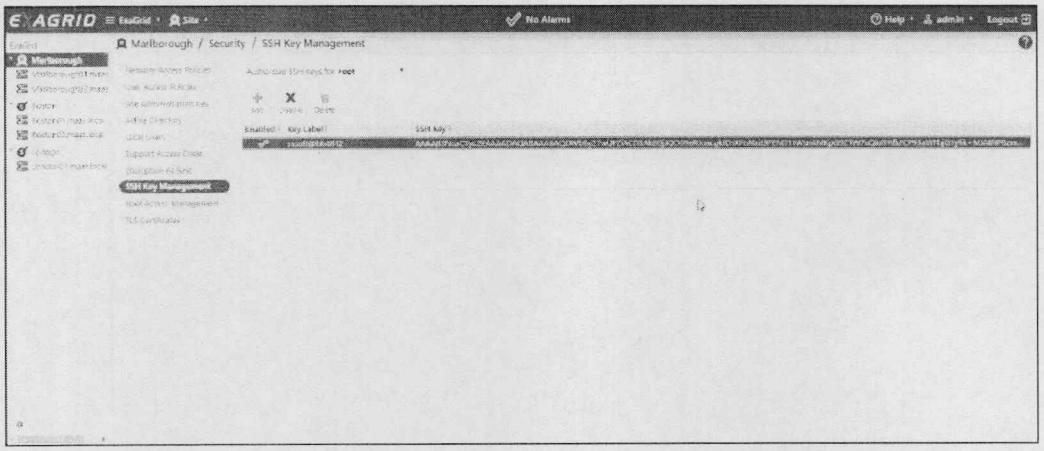
Managing SSH Keys

SSH keys are used by:

- ExaGrid Support logging in as the **root** user.
- Veeam agents logging in as a backup user to access ExaGrid-Veeam data mover shares.

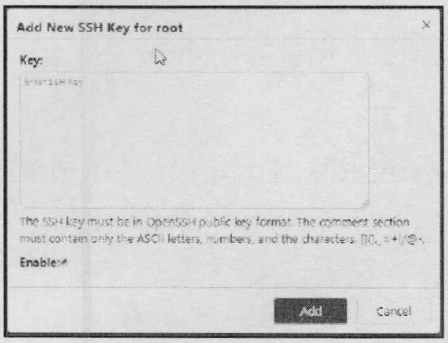
To manage SSH Keys:

1. Log in to the ExaGrid as a user assigned the Admin role.
2. From the navigation tree, select an ExaGrid site.
3. In the to main menu, select **Site**, and all menu options for the site are displayed.
4. Under **Security**, select **SSH Key Management** and the SSH Key Management page is displayed:



5. From the **Authorize SSH Keys For:** drop down menu, select a user.

6. Click **Add** and the Add SSH Key dialog box for the selected user is displayed:.



7. In the space provided, enter or paste the SSH Key.

8. Click **Add** and the key is added for the user.

Support Accounts

The ExaGrid support account is a role-based account created at installation with a user name of **support** and a password set to a unique code called the Support Access Code.

Note – The ExaGrid Support role cannot be mapped to an Active Directory Group.

The **support** user password can be changed from either the:

- Local User page - When you manually change the **support** user's password on the Local User's page the **root** user's password will also be changed. See ***"Creating and Modifying ExaGrid Local Users" on page 31***.
- Support Access Code page - When you generate a new access code, the generated code becomes the new password for both the **support** user AND for the **root user**. This is typically used to give ExaGrid Support representatives temporary root access to ExaGrid Appliances. Once the support representative has completed their tasks, a new password can be generated and they will no longer have access to root.

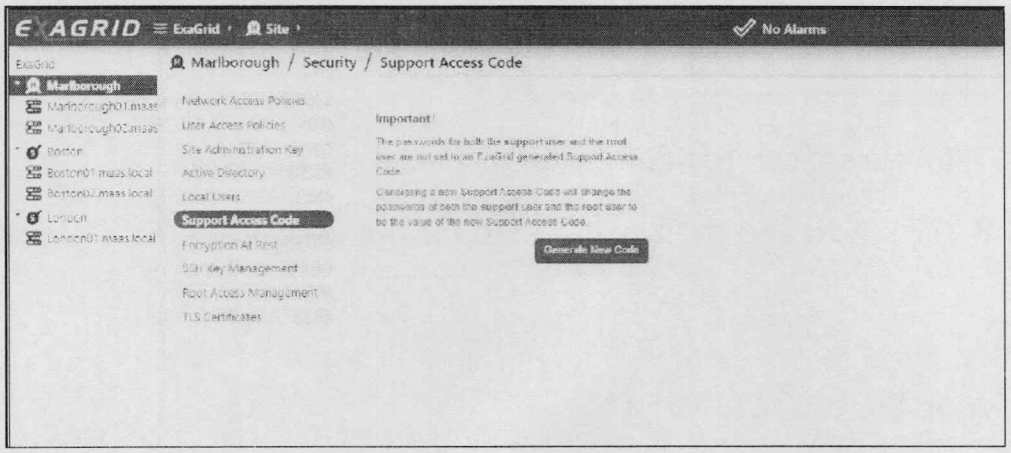
To generate a new support access code:

1. Log in to the ExaGrid as a user assigned the Admin role.

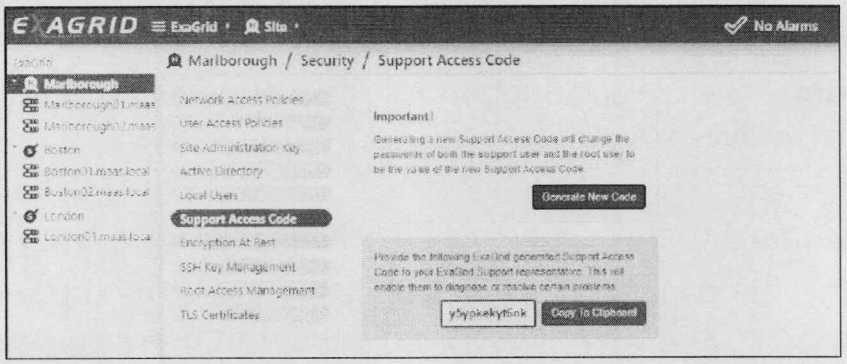
2. From the navigation tree, select an ExaGrid site.

3. In the top, main menu, click **Site**, and all menu options for the site are displayed.

4. Under **Security**, select **Support Access Code** and the Support Access Code page is displayed



5. Click **Generate New Code** and a new **support** user password and **root** user password will be created:



6. You can copy the new code to the clipboard and paste it in to a message or file as needed.

Support Gateway

The Support Gateway provides your ExaGrid Support Engineer with a gateway to access a selected ExaGrid Appliance.

Before initializing the support gateway, you must first obtain a registration code from your ExaGrid Support Engineer. Once the code is received, it will automatically time out if not used within 20 minutes.

To initialize a support gateway:

1. Log in to the ExaGrid as a user assigned the Admin role.
2. From the navigation tree, select the ExaGrid Site that has the ExaGrid Appliance your ExaGrid Support Engineer will access.
3. In the to main menu, select **Site**, and all menu options for the site are displayed.
4. Under **Configuration**, select **Support Gateway** and the Initialize Support Gateway page is displayed.
5. From the list of ExaGrid Appliances, select the ExaGrid Appliance your ExaGrid Support Engineer can access.
6. Click **Initialize** and the Initialize Support Gateway dialog box for the selected ExaGrid Appliance is displayed.
7. In the space provided, enter your company name.
8. In the space provided, enter the registration code you obtained from your ExaGrid Support Engineer.
9. If you must use a HTTP proxy to access the Internet, then in the spaces provided, enter the host name and port number.
10. Click **Apply** to save the configuration, or **Cancel** to exit without saving.

Root Access Management

You can use a combination of passwords and SSH keys to control access to the **root** user account for ExaGrid Appliances in a site. Three options are provided for managing root access:

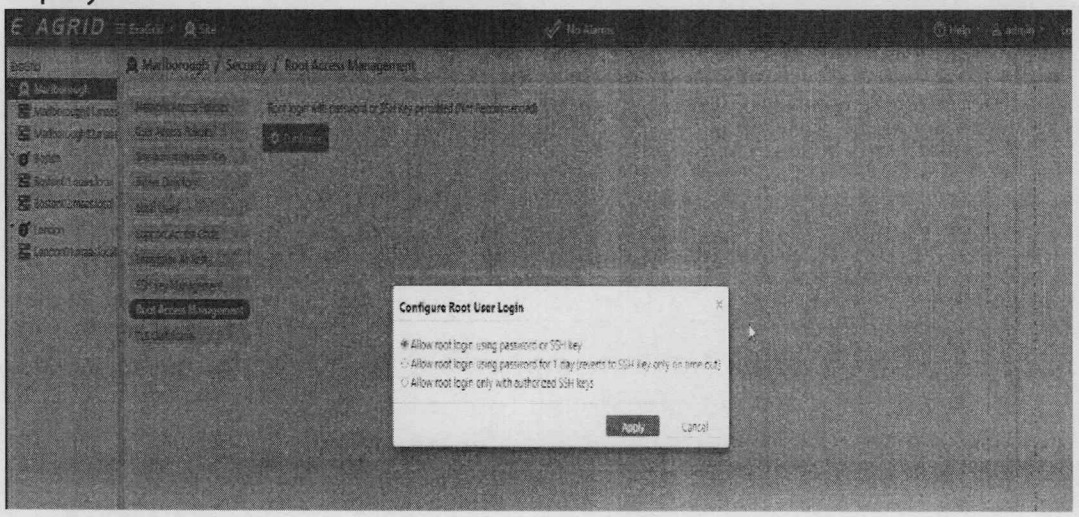
- Allow root log in using authorized SSH keys only (Recommended)
- Allow root log in using a password for one day (reverts to **SSH Key only** on time out)
- Allow root log in using a password or SSH key (Not recommended)

Note – To disable root access entirely, select the **Allow root log in using authorized SSH keys only** option and then ensure an SSH key has **NOT** been uploaded to the SSH Key Management page. See ***"Managing SSH Keys" on page 43***.

To manage **root** user access:

1. Log in to the ExaGrid as a user assigned the Admin role.
2. From the navigation tree, select an ExaGrid site.
3. In the top, main menu, click **Site**, and all menu options for the site are displayed.
4. Under **Security**, select **Root Access Management** and the Root Access Management page is displayed.

5. Click **Configure** and the Configure Root User Login dialog box is displayed:



6. Make your selection as needed.

7. Click **Apply** and **root** user access will be configured.

Using Server Message Block (SMB) Signing

SMB Signing is a feature that allows communications to be digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity. This security mechanism in the SMB protocol helps avoid issues like tampering of packets and "man in the middle" attacks. SMB signing does not encrypt data.

In addition, SMB signing augments the ExaGrid Share Network Access Policy and User Access Policy to control who and what has access to data on ExaGrid Shares.

To use SMB signing with your ExaGrid's CIFS Shares you must enable SMB signing on your Microsoft® Windows® backup servers through either:

- Enabling the Local Security Policy for the Microsoft network client: Digitally signed communications (always).
- Setting up a security policy that includes the enabled Microsoft network client: Digitally signed communications (always) on a Windows domain through the use of Group Policy Objects (GPO), and applying it to the backup server.

To ensure these changes are fully in place, restart your backup server.

Caution – Backups must not be running while you are enabling SMB signing.

Caution – Once SMB signing is enabled, you must specify credentials on your backup application and on the ExaGrid System. Not doing so will cause your backups to fail.

Determine which Windows account (NOT the local system account) or domain account credentials you will specify in your backup application and on the ExaGrid System.

If the ExaGrid Site is not part of an Active Directory Domain, enable and define local security credentials on your ExaGrid System:

1. In the left-hand navigation tree, click the ExaGrid Site name.
2. From the top, main menu, click **Site**, and all menu options for the site are displayed.
3. Under **Security**, select **Local Users.**
4. Create a local user with the **Backup Only Role.**

   The local user credentials you specify on the ExaGrid System must match an existing local or domain user account. Domain accounts must be entered without the domain information.
5. Create a **User Access Policy** specifying the local user (when the ExaGrid Site is not added to an Active Directory Domain) or the Active Directory Domain user(s) or group(s).
6. Assign the User Access Policy in the ExaGrid share configuration.

ExaGrid Shares

ExaGrid Shares are mount points to which your backup application backs up data.

There are two basic types of ExaGrid Shares:

- **Primary Shares:** Mount points created on ExaGrid Appliances to which your backup application can write.
- **InstantDR Shares:** Replicas of Primary Shares.

Primary Shares

There are four types of Primary Shares:

1. Backup Application Specific Shares
2. Pooled Shares
3. Universal Backup Shares
4. Utility Shares

Backup Application Specific Shares

Application specific shares are tailored to specific backup applications. ExaGrid provides detailed step-by-step instructions on how to use your backup application with these shares:

1. In the ExaGrid top, main menu, click **Help**.
2. From the drop down menu, select the **Online Library**. The Online library is displayed.
3. Expand the option that applies to your backup application.
4. Scroll down until you see the guide that applies to your application.
5. Right mouse click on the link to the guide and save or print it as needed.

To create an application specific share, see ***"Creating Shares" on page 62***.

Pooled Shares

Pooled Shares are available to, and recommended for, selected backup applications. i.e. Veritas NetBackup (OpenStorage).

A Pooled Share can use the storage resources of all ExaGrid Appliances in an ExaGrid Site.

For details on whether your backup application can be used with an ExaGrid Pooled Share, consult the ExaGrid backup application document for your backup application. A copy of the guide can be found in the ExaGrid Online Library in the ExaGrid user interface.

Universal Backup Shares

ExaGrid Universal Backup Shares are designed to accommodate those backup applications that do not have an ExaGrid Share designed specifically for their use.

Universal Backup Shares are deduplicated and can be replicated and migrated like application specific ExaGrid Shares.

ExaGrid has qualified a number of backup applications for use with the Universal backup Share. Best practices for the qualified applications can be found in your ExaGrid's Online Library.

In addition, ExaGrid is continually qualifying backup applications for the Universal Backup Share. The ExaGrid web site (www.exagrid.com) will have the most up-to-date list of applications qualified for use with the Universal Backup Share.

In most cases, if your backup application has not yet been qualified by ExaGrid for use with the Universal Backup Share; the application will work with the Universal Backup Share provided you follow these simple guidelines:

Note – ExaGrid Support may have limited expertise in applications not qualified by ExaGrid.

---

1. Create an ExaGrid Universal Backup Share. ***"Creating Shares" on page 62***

2. Write backups to the ExaGrid Universal Backup Share as recommended by the application's best practices for writing to disk,

3. In addition to following your backup application's best practices, if supported by your backup application, ensure that:

- Compression is **OFF**
- Encryption is **OFF**
- Multiplexing is **OFF**
- Deduplication is **OFF**
- Concurrent write operations should not exceed 20. ExaGrid recommends to initially limit concurrent writes to four or five. Over time, increase concurrent writes until you reach a number that maximizes the performance of your backups. Each backup application, due to its particular pattern it writes will experience different levels of performance.

4. Run a series of test backups and restores to monitor deduplication ratios and performance and make adjustments as needed.When testing your backups look for:

- Errors or warnings in the ExaGrid Event Viewer

- Unusual deduplication ratios
- Unusual deduplication rates
- A sudden increase in backup durations when the retention period for your first backups is reached.
- Restores from backups at the other edge of your retention period that take an excessive amount of time.

Note – Your ExaGrid Appliances do not employ real-time reporting. When monitoring backup results it can take up to fifteen (15) minutes for a report to be updated.

The Universal Backup Share is not suitable for all backup applications. This includes backup applications that:

- Create file and folder names that do NOT use UTF-8 encoding.
- Archive data into many small, individual files
- Backup data into many small, individual files
- Overwrite large amounts of backup data sent previously to the ExaGrid Universal Backup Share. Overwriting a small amount of "metadata" – e.g. control files, catalogs, etc. – should perform acceptably.
- Treat the ExaGrid Universal Share as primary storage

Utility Shares

Utility Shares are designed to accommodate any data type. Data can be copied manually, through a script, or from an application to a Utility Share.

Caution – Utility Shares are not protected by ExaGrid's Retention Time-Lock settings and can be vulnerable to ransomware and other malicious activity. See ***"Retention Time-Lock Overview" on page 25***

When you create a Utility Share you must allocate a specific amount of storage space to the Utility Share. The space allocated is taken proportionately from the host ExaGrid Appliance's Landing Zone Tier and Retention Tier.

- Data in Utility Shares is not deduplicated and can not be replicated to another ExaGrid Site.
- You can only create one Utility Share per ExaGrid Appliance.
- When you create a Utility Share, the amount of available Landing Zone Tier and Retention Tier reported in Summary Reports will be automatically adjusted.
- No more than twenty percent (20%) of an ExaGrid Appliance's space can be allocated to a Utility Share.
- The maximum allowable size of a Utility Share is 13 TB

Caution – When allocating space, you must consider the impact of the space allocation on your backup Landing Zone Tier as well as your Retention Tier. It is possible to allocate space for a Utility Share such that it interferes with your ExaGrid Appliance's ability to accept and retain backups from other backup applications.

To create a Utility Share, see ***"Creating Shares" on page 62***

InstantDR™ Shares

InstantDR Shares are replicas of primary shares that are reside on one or more ExaGrid Site. InstantDR shares can be used to:

- Recover replicated data after a disaster scenario. In multi-site ExaGrid environments, backup data in ExaGrid Shares that are set to replicate to other sites, can be recovered.
- Test recovery of replicated data. You can use InstantDR shares to prove that the data replicated to other ExaGrid Sites is recoverable.
- Perform remote tape copy operations. Instant DR shares can also be used to make a tape copy of data that has been replicated to other ExaGrid Sites. For details, see the ExaGrid guide that describes how to use your backup application. A copy of your backup application guide can be found in the Online Library.
- Can be used with Veritas' OpenStorage Technology to achieve:
  - Seamless integration with ExaGrid

- Unified control and tracking of all copies of data from the Veritas application's interface -- including copies replicated to other ExaGrid Sites and tape copies.
- Simplified disaster recovery, as Veritas OpenStorage is already aware of all copies of data and individually tracks retention periods for each copy
- Fast recovery times due to the combination of Veritas' and ExaGrid InstantDR capability
- Short backup window, by load balancing across Veritas media servers into the ExaGrid environment.
- Flexibility to retain different amounts of backup data at a local site versus an off-site disaster recovery location, by better utilizing the unique ExaGrid architecture.

To see how InstantDR shares are added to replicas, see ***"Creating Replicas and InstantDR Shares" on page 68***.

Share Protection

Shares, and the data they contain, are protected in multiple ways:

- The ExaGrid Appliances and the data backed up to it are in your data center.
- Time-locks can be set on deduplicated and retained data. This protects against ransomware and other malicious activity. For details see ***"Retention Time-Lock Overview" on page 25***.
- Two-Factor Authentication can be enabled on a user's account. ExaGrid **HIGHLY** recommends enabling this for all users. For details see ***"Two-Factor Authentication" on page 35***.

Security Alert - Employing **BOTH Retention Time Lock and Two Factor Authentication** are your best defense against ransomware and other malicious activity.

- ExaGrid Appliances can be members of an Active Directory Domain. ExaGrid Roles can be assigned to groups in their server's Active Directory Domain, thereby limiting access to an ExaGrid Appliance and the ExaGrid Shares it hosts. For details see ***" Managing Active Directory" on page 38***

- User Access Policies that define the backup application users who have access to a share. For details see ***"User Access Policies" on page 59***.
- Network Access Policies that define network access to a share. For details see ***"Network Access Policies" on page 58***.
- Large-scale deletes can indicate malware activity. A **Delete Monitor** provides, on a share by share basis, a definable threshold for raising an alarm when data is deleted from a share. The threshold is defined during share creation and can be adjusted as needed. The default threshold setting is 50 percent of a share's data in a 24 hour period. See ***"Creating Shares" on page 62***.
- Multi-site configurations provide an additional level of data security. Copies of backup files can be kept on a second site. In case of a catastrophic event where one site has been damaged or destroyed, copies of backups on the second site can be used to rebuild your backups.
- ExaGrid provides a hardware option that employs Encryption at Rest and Boot Protection. See ***"Encryption Capable ExaGrid Appliances" on page 89*** for details.

Share Migration

Over time, your backup requirements will change. Because of these changes, it might be necessary to expand your ExaGrid environment and/or add and move shares from one ExaGrid Appliance to another. To help you balance your backup load, the ExaGrid System allows you to move primary shares from one ExaGrid Appliance to another. This process is known as Migration.

If it becomes necessary to migrate an ExaGrid Share, contact your ExaGrid Support Representative and they will perform the migration.

Once a share has been migrated, it is treated as a new share. If the share is set to replicate to other sites, its replication history will be restarted and its replication reports will begin anew.

Note – Once a share has been migrated, backup jobs writing to the share need to be reconfigured to write to the share's new location. However, Veritas backup jobs using the ExaGrid OpenStorage (OST) plugin do not need to be reconfigured.

See the "***Using .... With ExaGrid***" guide for your specific backup application for more details.

Share Access Policies

Policies that define share access are created at the ExaGrid Site level. Depending on the share type, you must create at least one:

- User Access Policy that defines the backup application users who have access to a share.
- Network Access Policy that defines network access to a share.

Note – Veeam Shares do not require a Network Access Policy.

A single User and Network Access Policy can be used by multiple shares.

Network Access Policies

Network Access Policies provide the necessary networking information (IP address or name) for a backup application's server to access a share. A single Network Access Policy can contain multiple addresses and be used by multiple shares.

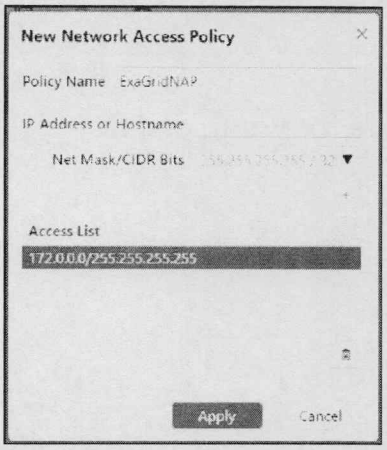
Modifying a Network Access Policy will change access to all the shares that use the policy.

To create a Network Access Policy:

1. In the left-hand navigation tree, select the ExaGrid Site on which the you want to create the Network Access Policy.

2. In the top, main menu, click **Site** and all menu options for the site are displayed.

3. Under **Security,** select **Network Access Policy** and the Network Access Policy dialog box is displayed:



4. In the space provided, enter the Network Access Policy name.

5. In the space provided, enter the IP address of the backup server(s) that will access and backup to this share.

6. Select a subnet mask for the IP address.

7. Click the + plus and the IP/subnet mask pair are entered into the Access list.

8. If a backup server uses multiple IP addresses, or if more than one backup server will write to the share, repeat this process for all servers involved.

9. Click **Apply** and the Network Access Policy is created.

User Access Policies

User access policies allow you to control which users can access a share. A single User Access Policy can be used by multiple ExaGrid Shares.

Modifying a User Access Policy changes access for all shares that use it.

If the servers in the ExaGrid Site are members of an Active Directory Domain, share access control can be expanded to include users and groups who are also members of the Active Directory Domain.