Tel:
0208 502 7344

Website:
www.groupcall.com

XVault Security

XVault Version

This user guide applies to Groupcall XVault version 1.2.3 (2011-08)

Version Control

	Date	Author	Notes
1	2012-04-20	Becky Thornton	Created as a standalone guide

Contents

XVault Data Security

While Groupcall XVault is designed to operate securely and requires authentication to access web servers and the management console, it is advised that additional configuration is made in the operating environment to ensure full platform-level security.

The XVault Database

The XVault database should be located on a physically secure server that is appropriately configured to prevent unintended access. Each system accessing the database requires a separate SQL user account with a strong password. Systems reading data from the XVault database should be constrained to a specific view or set of views per accessing system.

Groupcall recommends that the SQL platform or underlying system is encrypted in order to protect data.

The XVault Application

The server on which the XVault application is installed on should be physically secured and appropriately configured to prevent unintended access. XVault only permits incoming connections to its Web Services interface and to its web-based management console[1]. XVault will make outgoing connections to https://dashboard.groupcall.com/ and to any SIF Zone Integration Server that it is configured to contact.

Although the XVault application does not store any sensitive data locally (only into the XVault Database), Groupcall recommends that the server or underlying system is encrypted to prevent unintended release of the SQL server credentials or SIF SSL private keys.

SSL Encryption

The XVault application runs on top of Apache Tomcat, the current version of Apache Tomcat is 7.0. To enable SSL encryption for the web service and management console it is necessary only to apply the appropriate SSL configuration instructions to Apache Tomcat and restart it.

Non-SIF Message Security

For XVault Zones that are configured without the use of SIF Transport (Non-SIF zones) XVault and the source Xporter installation broker their messages via an SSL connection to Groupcall Dashboard. The collection template assigned to a Zone in XVault is authoritative regarding which objects will or will not be retrieved from the source SIF Agent.

[1] Except when using SIF push-mode; this requires XVault to open an additional listener for SIF push messages.

SIF Message Security

All SIF Agents, including XVault, connect to a SIF Zone Integration Server; in live environments this is an SSL connection. A Zone Integration Server (ZIS) partitions school data sources into multiple SIF Zones – each Zone being isolated. A single school SIF Agent connects to each zone and XVault connects to all Zones it has been configured with.

Each Agent in each Zone is allowed to request certain SIF Data Objects; this enforces the collection of data to only those objects supported by data agreement. This configuration denies any data objects configured for collection in the XVault collection template that are not allowed by the Zone, providing an additional tier of data access control and highlighting any requests for data that are outside of the SIF Data Objects permitted.