IDS-2200

Intrusion Detection System

IDS 2R2 Release Announcement

August 2019

Formula Consultants Inc.
222 S. Harbor Blvd.
Anaheim, CA 92805

Direct your comments or requests to:

Formula Consultants Incorporated
P. O. Box 544
Anaheim, California 92815
714/778-0123
714/778-6364 (Fax)

Software Version: 2R2

Contents

[Page intentionally left blank.]

General

Formula Consultants Incorporated is pleased to announce that Level 2R2 of IDS-2200 is now available for distribution. IDS-2200 is FCI's Intrusion Detection System used to monitor security events within the Unisys OS2200 environment.

The IDS-2200 level 2R2 product release can be obtained via the FCI Support Center (see Note of Interest number 1). Consistent with FCI policy, this release will be provided at no additional cost to all IDS-2200 users with current maintenance contracts, as well as to users who are still in their initial warranty period.

Product Overview

IDS-2200 can assist businesses facing additional security requirements by providing real-time security monitoring of the OS2200 environment.

IDS-2200 is implemented in several components. When installing these components you decide whether they will communicate amongst themselves using an SSL or non-SSL interface.

IDS Security Agent(s)

Security Agents are installed on the OS 2200 partitions which your site wants to monitor. The Agent runs as a background job under OS 2200, reading different system and product log files, collecting information about security related events.

The Security Agent responds to conditions it detects, and performs Security Response Actions which have been pre-defined by the IDS Admin Client. These actions include, under appropriate conditions, Disabling a UserID, Enabling a UserID and terminating all runs for a given UserID.

IDS Server

The IDS Server component runs on a Windows Server platform. The IDS Server collects data provided by the Agents and maintains it in the IDS Database. The IDS Server stores configuration changes made via the IDS Admin Client. It also provides data to the IDS Events Client upon request.

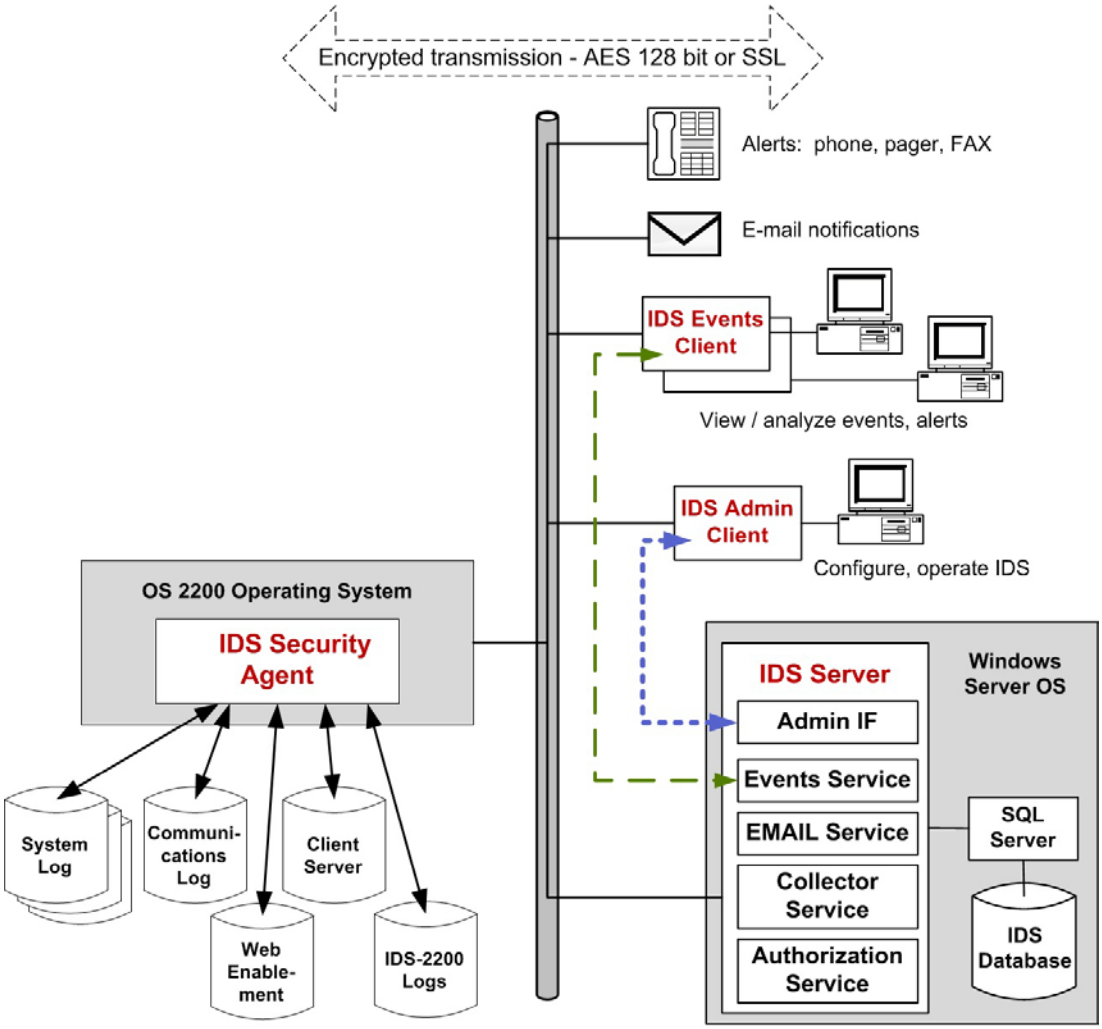
IDS Admin Client(s)

An IDS Admin Client runs on a Windows platform: either the on server or on network accessible workstation. It is used by site administrators to manage the IDS-2200 operating environment. Administrators define Alerts whereby the IDS system will notify staff of security events which reach a threshold to trigger an alert. Administrators also define IDS objects such as the relevant Agents, Users, and Contacts. Further, you use the Admin Client to adjust operating preferences.

IDS Events Client(s)

IDS Events Clients run on Windows platforms and are used by your security analysts to view the information gathered by the OS 2200 Security Agents. Analysts using the ID Events Client can also manually constrain the capabilities of users suspected of unauthorized activity.

The IDS-2200 Product also includes an optional Product Modification Element (PME) for MAPPER. This PME implements enhanced security logging for MAPPER which, in turn, allows IDS-2200 to monitor it.



Release Description

Stability Update and Minor Enhancement Release

IDS-2200 level 2R2 is a stability update release with minor enhancements.

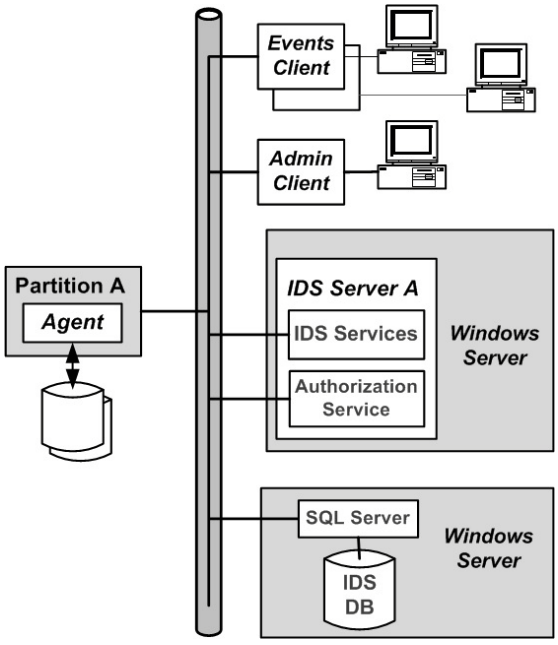
Product Enhancements

IDS Database and SQL Server Remote from IDS Server

Previous levels of IDS required the IDS database and supporting SQL Server to be on the same host as the IDS Server.

IDS 2R2 eliminates this restriction, giving you the flexibility to host the IDS Database and its supporting instance of SQL Server on a host remote from the IDS Server.

This feature requires some additional configuration within the installation process when installing the Windows based components.



Improvements to Installation of Windows Based Components

Bootstrapper Installer

When installing the IDS Windows based components, the IDS installation script continues to install the Windows hosted IDS elements. In IDS 2R2, the entire installation script is wrapped in a "bootstrapper installer."

The bootstrapper installer ensures that the correct version of the .NET framework is installed, improving the reliability of the installation process.

The bootstrapper also transparently installs the C++ redistributable—a Windows component required to support the remote hosting of the instance of SQL Server.

Configuration Requirements during Installation

To support the possibility of the SQL Server being hosted remotely from the IDS Server, it is necessary to unambiguously define the host for the SQL Server. This is handled in some configuration steps within the installation process.

Because the IDS Events Client must access the IDS Database, whenever you are installing the IDS Events Client, you must unambiguously identify the host location for the relevant instance of SQL Server.

Release Notes Available within the Installation

When you reach the end of the installation, the installation script gives you the option to view release notes, which are displayed within the default web browser application.

IDS-2200 Notes Of Interest

Only IDS-2200 Note of Interest (NOI) 1 and above are relevant to level 2R1.

Technical Concerns

Restrictions and Limitations

Your OS 2200 environment must support UCS object module execution. This includes support for extended mode by the Exec as well as installation of the LINK and URTS products.

Requirements for Windows-Hosted Components

Table 1-1. System Requirements for IDS Client Components

Component	Requirement
Operating System	Windows 7 Professional (64-bit) or later
Processor	X64 Architecture processor 3.0 GHz or faster 4 cores minimum
Memory	4GB Minimum
.NET Framework	.Net 4.71 is required for IDS Client components
Storage: Hard Drive	1.5GB for client components: system, logs, and reports

Table 1-2. System Requirements for IDS Server Host

Component	Recommended
Operating System	Windows Server 2012 R2 (Standard or Datacenter)
Processor	X64 Architecture processor 3.3 GHz or faster For SQL Server and IDS database, 2 processors, 16 cores are recommended
Memory	32GB minimum
SQL Server	SQL Server Enterprise 2016
.NET Framework	.Net 4.6 is required for SQL Server 2016; .Net 4.71 is required for IDS Services
Storage: Hard Drive	2GB/ week of disk space is required for the IDS Database; the equivalent amount of space is required for archived data
Storage: (Optional) offline storage for events archival	DVD writer minimum. Blu-Ray writer recommended.

Compatibility and Migration for OS 2200 Component

The IDS Security Agent for release 2R2 is generated under **CP OS2200 16.0** and tested under both **CP OS2200 16.0** and **CP OS2200 15.0**.

Previous Level Support

The prior level of IDS-2200 was 2R1. IDS-2200 2R1 will be supported until 12/31/2020.

Documentation

The complete set of IDS-2200 manuals includes:

- *IDS-2200 2R2 Release Announcement*
- *IDS-2200 2R2 Security Agent Installation and Administrator Guide,* FP-101107-005
- *IDS 2R2 Installation and Configuration Guide for Windows Platforms*, FP-101108-003
- *IDS 2R2 Admin Client User Guide*, FP-101109-003
- *IDS 2R2 Events Client User Guide*, FP-101110-003
- *IDS 2R2 Splunk Integration Guide,* FP-101111-001
- *IDS 2R2 Quick Start Notes*
- *FCI Products Release Tape Recreation Instructions*

FCI Website

You may obtain general information about Formula Consultants, Inc. and its products at our website at www.formula.com. After you register with the site and receive a userid and password, you can also download PCRs and Notes of Interest. Product documentation in PDF format is also available (Adobe Acrobat™ Reader required).

FCI Support Center

The FCI Support Center (FCISC) is available for use. The FCISC is a 2200 host server software system that is accessible by using the standard UNISYS Remote Site Support (RSS) product. It allows you to send and receive data electronically to and from FCI. Refer to the *IDS-2200 Security Agent Installation and Administrator Guide* for more information.

Corrections

File 13 on your release tape contains PCRs, if any, which have been generated against this release, as of the date your tape was created. Include any of these corrections applicable to your site with the first build from this tape. IDS-2200 elements are a combination of basic and UCS elements so the PCRs are organized by IDS-2200 processor type (basic mode or UCS). These elements can be @ADDed following an @COMUS to enter the corrections into your local COMUS database. Examine the file to determine which elements should be added to your build.

The elements README, CHGNUM-ALL, and IDS-NOIS are informational only and should not be @ADDed to your COMUS database.

The possible elements in File 13 are:

README	explanation and cutoff date/time
ADD/SGS	changes for the 'additional SGS' build prompt
BASE/*version*	changes to IDS-2200 elements
CHGNUM-ALL	list of all change numbers
IDS-NOIS	all relevant Notes of Interest

where:

version can be BASIC or UCS depending on the associated IDS-2200 element. The CHG numbers generated by COMUS must be entered at the 'New Change number' build prompt. These numbers can be entered individually, or @ADD the CHGNUM elements that apply to your build.

If you add UCS corrections, the UCOB and/or UC compilers must be installed. Another method of including UCS corrections is to copy updated object modules contained in this file. This is done by answering the build prompt, 'Any replacement Object Modules to be included', and specifying the filename into which the modules were copied.

File 13 of your release tape also contains Notes of Interest in the element called IDS-NOIS. Notes of Interest are field bulletins which we recommend reading prior to generating or installing IDS-2200.

Ordering Instructions

To obtain a copy of IDS-2200 level 2R2, please download it from the Formula Consultants support website at:

www.formula.com/support/logon.asp

or Order IDS-2200 2R2 electronically by addressing your e-mail to:

IDS@formula.com

or To order your site's copy of IDS-2200 Level 2R2 Security Agent on DVD and IDS-2200 IDS Server, IDS Admin Client and IDS Events Client CD's, please complete the attached Product Order Form and fax it to 714-778-6364, or mail your order to:

Formula Consultants Incorporated
P.O. Box 544
Anaheim, CA 92815
Attn: Product Sales

General Releases

MEDIA: The IDS-2200 level 2R2 Security Agent DVD and IDS-2200 IDS Windows Server, IDS Admin Client and IDS Events Client CD's are available for download on the FCI support web site.

Product Order Form

PRODUCT: **IDS-2200 Level 2R2**

CUSTOMER: _____

DELIVERY ADDRESS: _____

_____

CITY, STATE: _____

ZIP CODE: _____

CONTACT: _____

TELEPHONE NUMBER: _____

LAST IDS-2200 LEVEL RECEIVED: _____