IDS-2200

Intrusion Detection System

IDS 2R1 Release Announcement

March 2019

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

Copyright Notice

Formula Consultants Incorporated reserves the right to revise or modify the contents of this document. Contact Formula Consultants to verify that you have the most current revision of this document.

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: 2R1

Contents

[Page intentionally left blank.]

General

Formula Consultants Incorporated is pleased to announce that Level 2R1 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 2R1 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.

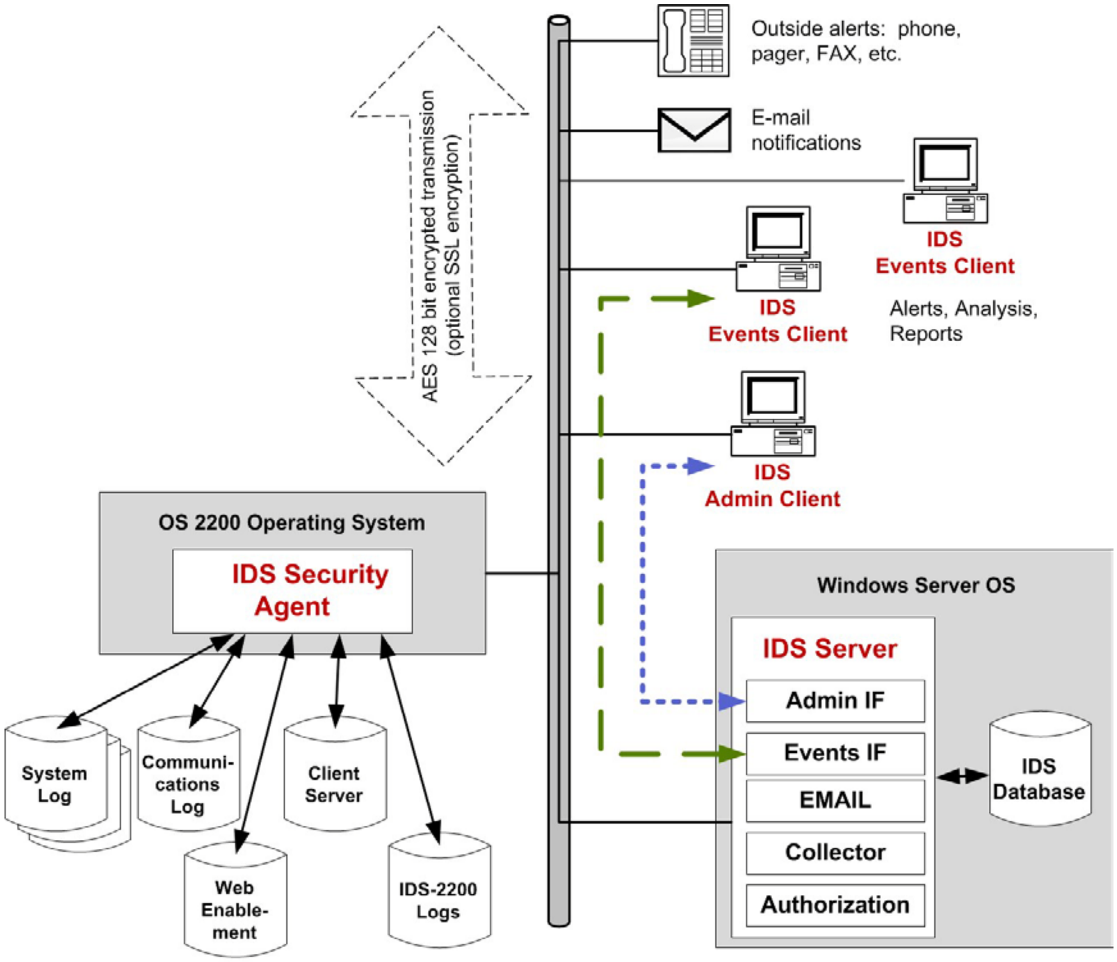
IDS Admin Client(s)

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 2R1 is a stability update and minor enhancement release.

Product Enhancements

Product Installation for Windows-Hosted Components

The installation for components hosted on Windows platforms is consolidated into a single installation script with options for selecting one or more components to install. These components are: the IDS Server, the IDS Admin Client, and the IDS Events Client.

IDS Server Component

The IDS Server is supported on a hardware platform running Windows Server 2012 R2 with SQL Server 2016 Enterprise.

IDS Admin Client

The IDS 2R1 Admin Client can run on the Windows Server 2012 R2 as well as on Windows 7 workstations connected through the network.

IDS Events Client

The IDS 2R1 Events Client can run on the Windows Server 2012 R2 as well as Windows 7 workstations connected through the network.

IDS Security Agent Support of CP OS2200 15.0 release (EXEC 49R1)

The IDS 2R1 Security Agent background run has been enhanced to be able to read the new system log file format released in EXEC level 49R1 of CP OS2200 release 15.0. The IDS-2200 Security Agent will read both the old system log file format as well as the new format, which was introduced to support the Unisys Daylight Savings Time adapt.

IDS 2R1 Security Agent New Parameter

The IDS Security Agent background run has been enhanced to implement the SECLEV parameter.

SECLEV Sets the Security Level for each of the IDS background run Commands and Processes. The format of the SECLEV parameter is:

SECLEV *Command Level*

Where:

Level	Description
1	Basic Console Mode
2	Limited Console Mode
3	Full Console Mode
4	Display Console Mode
5	Response Console Mode
6	Inter-Process Command (internal)
7	System Console
8	Batch Parameter only.

IDS 2R1 Security Agent New Flags

The IDS Security Agent background run has been enhanced to implement the new flags of MSGI, TUMSGS and TUMTXT.

MSGI Sets the message interval in minutes between communications errors with CompAPI or CPComm when one or the other is down. The default is one minute.

```
SET MSGI 1
```

TUMSGS Determines if a termination message is sent to a demand run prior to it being terminated by IDS as a result of a Termination Action defined in an Alert. The default is zero indicating that no message is sent. A value of one will send the defined message to the demand run before it is terminated.

```
SET TUMSGS 1
```

TUMTXT Sets the optional Terminate User Message text that the IDS background run optionally sends to a user demand session before the demand session is terminated. The sending of the message is dependent on the new flag TUMSGS. The text message is a string of characters up to 70 characters in length. Any spaces must be represented as underscores

```
SET TUMTXT Run_has_been_terminated_by_IDS_due_to_security_errors
```

IDS 2R1 PME for MAPPER 47R1

The IDS-2200 Security Agent has been enhanced to provide a new Product Modification Elements (PME) for MAPPER level 47R1. The PME name for MAPPER Level 47R1 is MAPPER47. This PME is installed in SYS$LIB$*IDS-2.

Option to Enable SSL Sessions

Optionally, the IDS Security Agent and the IDS Windows 2008 Server can be configured for SSL sessions in their communications with each other. Note that if you have multiple agents, those agents and their servers must either be all SSL enabled or all non-SSL enabled. Further, when you install IDS Server and IDS Client components, they must all be configured with the same encryption protocol.

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	
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 2R1 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 1R2. IDS-2200 1R2 will be supported until **12/31/2019**.

Documentation

The complete set of IDS-2200 manuals includes:

- *IDS-2200 2R1 Release Announcement*
- *IDS-2200 2R1 Security Agent Installation and Administrator Guide,* FP-101107-004
- *IDS 2R1 Installation and Configuration Guide for Windows Platforms*, FP-101108-002
- *IDS 2R1 Admin Client User Guide*, FP-101109-002
- *IDS 2R1 Events Client User Guide*, FP-101110-002
- *IDS 2R1 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 2R1, please download it from the Formula Consultants support website at:

www.formula.com/support/logon.asp

or Order IDS-2200 2R1 electronically by addressing your e-mail to:

IDS@formula.com

or To order your site's copy of IDS-2200 Level 2R1 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 2R1 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 2R1**

CUSTOMER: ____________________

DELIVERY ADDRESS: ____________________

____

CITY, STATE: ____________________

ZIP CODE: ____________________

CONTACT: ____________________

TELEPHONE NUMBER: ____________________

LAST IDS-2200 LEVEL RECEIVED: ____________________