

# *IDS-2200*

*Intrusion Detection System*

IDS Level 1R1

Release Announcement

May 2008

Formula Consultants Inc.



**CONFIDENTIAL AND PROPRIETARY PROPERTY.**

*Subject to certain restrictions and non-disclosure requirements of Formula Consultants Incorporated.*

### ***Copyright Notice***

Copyright © 2008 by Formula Consultants Incorporated, P.O. Box 544, Anaheim, California 92815.

No part of this material may be reproduced in any form without permission in writing from Formula Consultants Incorporated.

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: 1R1

# Contents

<b>IDS-2200 LEVEL 1R1 RELEASE ANNOUNCEMENT</b>	<b>1</b>
<b>General</b>	<b>1</b>
<b>Product Overview</b>	<b>1</b>
<b>Release Description</b>	<b>2</b>
<b>Minor Enhancements</b>	<b>2</b>
<b>IDS-2200 Notes Of Interest</b>	<b>2</b>
<b>Restrictions and Limitations</b>	<b>3</b>
<b>Compatibility and Migration</b>	<b>3</b>
<b>Previous Level Support</b>	<b>3</b>
<b>Documentation</b>	<b>3</b>
<b>FCI Website</b>	<b>3</b>
<b>FCI Support Center</b>	<b>4</b>
<b>Corrections</b>	<b>4</b>
<b>Ordering Instructions</b>	<b>5</b>
General Releases	5
Ordering the Software	5
<b>PRODUCT ORDER FORM</b>	<b>6</b>

[ Page intentionally left blank. ]

# IDS-2200 Level 1R1 Release Announcement

---

## General

### ***New Intrusion Detection System Now Available***

Formula Consultants Incorporated is pleased to announce that Level 1R1 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 1R1 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 installs as a Security Agent or agents assigned to monitor major functional areas of your OS2200 operating environment. IDS also has one or more Client component(s), installed on a PC, with which administrators review information gathered by the Security Agents.

- The IDS Security Agent runs as a background job reading different system and product log files. The Security Agent collects information about security related events for any IDS-2200 Clients which are connected.
- The IDS Security Agent uses and connects to COMAPI. The Security Agent listens on a site-defined port for a valid IDS Client with which it can connect.

- The IDS Security Agent optionally encrypts communications with IDS clients using its own AES encryption or the Unisys CIPHER-API encryption product.
- The IDS Security Agent responds to conditions it detects, and performs Security Response Actions on behalf of the IDS Client. The actions to be taken are configured by an authorized administrator. Actions include, Disabling a UserID, Enabling a UserID and terminating all runs for a given UserID.
- 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

### Initial Software Release

IDS-2200 level 1R1 is an initial software release. This initial release provides security monitoring for the EXEC System log file along with optional security monitoring for CPCComm, SILAS, WebTS and CMS1100.

When an optional PME (provided) is applied to MAPPER, IDS 1R1 can also monitor certain security related events in MAPPER.

---

## Minor Enhancements

None

---

## IDS-2200 Notes Of Interest

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

---

## Restrictions and Limitations

Your 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.

---

## Compatibility and Migration

Release 1R1 is generated under CP OS2200 11.

---

## Previous Level Support

There are no prior levels of IDS-2200.

---

## Documentation

Documents provided with release 1R1 includes:

*IDS-2200 1R1 Security Agent Installation and Administrator Guide*

*IDS-2200 1R1 Client Installation and Administrator Guide*

*IDS-2200 Level 1R1 Release Announcement*

*IDS-2200 Quick Start Notes*

*OS2200 Release Tape Creation Instructions*

---

## FCI Website

You may obtain general information about Formula Consultants, Inc. and its products at our website at [www.formula.com](http://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

Effective with the release of IDS-2200 1R1, 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, that 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/ <i>version</i>	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

### General Releases

The OS2200 Software is included on the CD and is available in four different release tape formats, each in their own directory. The directory formats are:

DVD, DDP, FLIT and VTH.

Some sites will require a cartridge tape for a successful installation.

If **all** of the following are **true** for your site, please request the OS2200 components of IDS on cartridge tape.

- You are **not** running on a Dorado 300 series or above.
- You **do not** have DDP-FJT 5R5C (CP OS2200 9.0) or higher installed. It does not have to be running, it merely must be installed.
- You **do not** have FLIT 12R3 (CP OS2200 9.0) or higher installed.
- You **do not** have the Unisys VTH EXEC feature installed.
- You **do not** use or have RSS configured to run through the Internet, **and** your firewall **does not** allow you to send and receive on your port 102, with FCI's IP address.

### Ordering the Software

To order your site's copy of IDS-2200 Level 1R1, contact a sales representative at Formula Consultants Inc. at **714-778-0123**

*or* 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**

*or* Order IDS-2200 1R1 electronically by addressing your e-mail to:

**sales@formula.com**

*or* Order IDS-2200 level 1R1 through the Formula Consultants website at:

**www.formula.com**

# Product Order Form

PRODUCT: IDS-2200 Level 1R1

CUSTOMER: \_\_\_\_\_

DELIVERY ADDRESS: \_\_\_\_\_

CITY, STATE: \_\_\_\_\_

ZIP CODE: \_\_\_\_\_

CONTACT: \_\_\_\_\_

TELEPHONE NUMBER: \_\_\_\_\_

LAST IDS-2200 LEVEL RECEIVED: \_\_\_\_\_

MEDIA - All tapes will be unlabeled.

## Standard Media

- 18-track cartridge     
  36-track cartridge     
  DVD  
 Electronic via RSS and the FCI Support Center

*Use SYSS\$LIB\$\*IDS.NEW-RELEASE/RSS-SCRIPT to copy to local tape.*

## Non-Standard Media

IDS-2200 can also be delivered on non-standard media (such as a 9840 A/B cartridge) supplied to FCI by the customer, provided FCI has compatible equipment. Please contact FCI to confirm the availability of the specific non-standard media you are requesting.

## Corrections

Please indicate the media FCI should use when sending your site minor corrections. Indicating diskette will mean you have the capability of uploading ASCII files from a PC to the mainframe.

- 5 ¼" diskette     
  360K     
  1.2 mg  
 18-track cartridge     
  36-track cartridge  
 Electronic via RSS and the FCI Support Center