

# CA Cross-Enterprise Application Performance Management

## Installation Guide

Version 3.0



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

## CA Technologies Product References

This document references the following CA Technologies products and features:

- CA Application Performance Management (CA APM)
- CA Application Performance Management for IBM CICS Transaction Gateway (CA APM for IBM CICS Transaction Gateway)
- CA Application Performance Management for IBM WebSphere MQ (CA APM for IBM WebSphere MQ)
- CA Application Performance Management for SOA (CA APM for SOA)
- CA Chorus™ Software Manager (CA CSM)
- CA Common Services for z/OS (CA Common Services)
- CA Datacom®/DB
- CA Embedded Entitlements Manager (CA EEM)
- CA Insight™ Database Performance Monitor for DB2 for z/OS (CA Insight DPM)
- CA Introscope® (CA Introscope)
- CA NetMaster® Network Management for TCP/IP (CA NetMaster NM for TCP/IP)
- CA Network and Systems Management Database Option for DB2 for z/OS (CA NSM Database Option)
- CA SYSVIEW® Performance Management (CA SYSVIEW)
- CA TCPaccess™ Communications Server for z/OS (CA TCPaccess CS)
- CA TCPaccess™ Telnet Server (CA TCPaccess Telnet Server)

# Contact CA Technologies

## Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At <http://ca.com/support>, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

## Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to [techpubs@ca.com](mailto:techpubs@ca.com).

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at <http://ca.com/docs>.

# Contents

---

## Chapter 1: Overview 9

Audience .....	9
Installation Roadmap .....	10
How the Installation Process Works.....	10

## Chapter 2: About CA Cross-Enterprise Application Performance Management 13

Architecture .....	14
--------------------	----

## Chapter 3: Preparing for Installation 17

System Requirements .....	17
Software Requirements .....	18
Management Module .....	19
Security Prerequisites.....	20
Port and Firewall Requirements .....	21
CA Insight DPM Security Requirements .....	21
CA NetMaster NM for TCP/IP Security Requirements .....	22
CA Common Services Requirements .....	23
Install CA Common Services.....	24
LMP Key Requirements .....	24
Set Up CAICCI for CA Cross-Enterprise APM .....	25
USS Space Requirements .....	25
Additional Prerequisites .....	26
Application Environment Requirements .....	27
Download the Appropriate CA Cross-Enterprise APM Files .....	27
How to Ready the CA SYSVIEW Product Package for Use with CA Cross-Enterprise APM.....	28
CA SYSVIEW Job Steps .....	29
Start XSXS Subtask.....	30
Post-Installation Considerations .....	31
Use Groups to Filter Queue Managers and Queues .....	32
Configure CA Insight DPM for Use with CA Cross-Enterprise APM .....	33
CA Insight DPM Installation Recommendations .....	35
CA Insight DPM Post-Installation Recommendations .....	36
CA Insight Customization .....	36
Set Up Xmanager, Xnet, and Required IQL Queries .....	39
How to Ready the CA NetMaster NM for TCP/IP Product Package for Use with CA Cross-Enterprise APM .....	40

---

CA NetMaster NM for TCP/IP Installation Considerations .....	40
<b>Chapter 4: Installing Your Product Using CA CSM</b> .....	<b>41</b>
How to Install Your Product Using CA CSM .....	41
Access CA CSM Using the Web-Based Interface .....	42
Acquire a New Product .....	43
Install a Product .....	44
Maintain the Installed Products .....	46
Deploy the Product to the Destination System.....	47
Configure the Deployed Product.....	48
<b>Chapter 5: Installing Your Product Using Pax ESD or DVD</b> .....	<b>51</b>
How to Install Your Product Using a Pax File.....	51
USS Environment Setup .....	52
Allocate and Mount a File System .....	53
Acquire the Product Pax Files.....	55
Download Files to a PC Using Pax ESD .....	56
Download Using Batch JCL .....	56
Download Files to Mainframe through a PC .....	59
Create a Product Directory from the Pax File .....	60
Example: JCL File, Unpackage.txt, to Customize .....	61
Copy Installation Files to z/OS Data Sets.....	61
Install the Cross-Enterprise APM Agent .....	63
Clean Up the USS Directory .....	64
Maintain the Cross-Enterprise APM Agent .....	64
Download Maintenance .....	65
SMP/E RECEIVE and APPLY.....	65
<b>Chapter 6: Starting Your Product</b> .....	<b>67</b>
How to Deploy Without CA CSM.....	67
Deploy the Cross-Enterprise APM Agent .....	67
Configure the Cross-Enterprise APM Agent .....	72
Configure and Accept the End User License Agreement .....	74
Configure Network Topology and Firewall Settings.....	75
Configure the Cross-Enterprise_APM_Dynamic.properties File .....	76
Configure the Introscope_Cross-Enterprise_APM.profile File .....	81
Configure Transaction Sampling .....	82
Start the Cross-Enterprise APM Agent .....	84
Confirm the Connectivity .....	84
Stop the Cross-Enterprise APM Agent .....	85

---

Deploy an Updated Version of the Cross-Enterprise APM Agent .....	85
SMP/E ACCEPT .....	86
SMP/E RESTORE .....	86

## **Chapter 7: Integrating CA SYSVIEW and CA Insight DPM With CA APM 87**

How You Integrate CA SYSVIEW and CA Insight DPM With CA APM .....	87
Preparing for Integration Procedure.....	87
Install and Enable the Enterprise Manager Components .....	88
Install and Enable CA APM Java Agent Components .....	90
Install the MQ Tracer (Optional) .....	97
Verify the Installation.....	98

## **Chapter 8: Integrate CA NetMaster NM for TCP/IP with CA Introscope 99**

How You Integrate CA NetMaster NM for TCP/IP with CA Introscope .....	99
Verify File Locations .....	100
Configure EPAgent .....	100
Confirm the Connectivity .....	101
Configure CA NetMaster NM for TCP/IP .....	102
Verify the Integration.....	103
Performance Monitoring Metrics .....	103
Specify the Performance Monitoring Metrics to Send.....	104

## **Appendix A: Recommended Reading 107**

CA APM Core Documentation .....	107
CA SYSVIEW Core Documentation .....	108
CA Insight DPM for DB2 for z/OS Core Documentation .....	109
CA APM for IBM WebSphere MQ Documentation.....	109
CICS Documentation .....	109
CA NetMaster NM for TCP/IP Core Documentation .....	110

## **Index 111**





# Chapter 1: Overview

---

This guide provides the processes and procedures to install and implement the CA Cross-Enterprise APM with CA SYSVIEW, CA Insight DPM, and CA NetMaster NM for TCP/IP.

This section contains the following topics:

[Audience](#) (see page 9)

[Installation Roadmap](#) (see page 10)

[How the Installation Process Works](#) (see page 10)

## Audience

Readers of this book require knowledge in the following areas:

- Job control language (JCL)
- TSO/ISPF
- System z environment and installing software in this environment
- IT environment, enterprise structure, and region structure of your organization.
- Installation and maintenance of the System z Module or a CA Cross-Enterprise APM instance.
- Cross-platform processes to enable CA Cross-Enterprise APM interact with System z.

You work with the following personnel:

- Systems programmer for System z, VTAM, and TCP/IP definitions
- Security administrator, for libraries and started task access authority.
- Storage Management Subsystem (SMS) or storage administrator, for direct-access storage device (DASD) allocations

## Installation Roadmap

Use this roadmap during the installation. This roadmap is not a replacement for the CA SYSVIEW PM, CA Insight DPM for DB2, CA NetMaster NM for TCP/IP, or CA Cross-Enterprise APM installation guides. For more information, see those guides for installation and configuration details of the respective products.

**Note:** If you only require network data, download, install and configure CA NetMaster NM for TCP/IP. You do *not* have to download CA Cross-Enterprise APM, but you must have the CA Cross-Enterprise APM license.

1. Validate software requirements by [preparing for this installation](#) (see page 17).
2. Install CA Common Services (if not already installed).  
**Note:** For more information, see CA Common Services Requirements.
3. [Download the appropriate CA Cross-Enterprise APM files](#) (see page 27).
4. [Install and configure the CA SYSVIEW product package for CA Cross-Enterprise APM](#) (see page 28).
5. [Install and configure the CA Insight DPM product package for CA Cross-Enterprise APM](#) (see page 33).
6. [Install and configure the CA NetMaster NM for TCP/IP product package](#) (see page 40).
7. Install and configure the CA Cross-Enterprise APM component.
8. Integrate the products.
9. Validate that CA SYSVIEW, CA Insight DPM, or CA NetMaster NM for TCP/IP data is available in CA APM Investigator and CA Introscope dashboards.

## How the Installation Process Works

CA Technologies has standardized product installations across all mainframe products. Installation uses the following process:

- Acquisition—Transports the software to your z/OS system.
- Installation using SMP/E—Creates an SMP/E environment and runs the RECEIVE, APPLY, and ACCEPT steps. The software is untailored.
- Deployment—Copies the target libraries to another system or LPAR.
- Configuration—Creates customized load modules, bringing the software to an executable state.

[CA Chorus™ Software Manager \(CA CSM\)](#) - formerly known as CA Mainframe Software Manager™ (CA MSM) - is an intuitive web-based tool that can automate and simplify many CA Technologies product installation activities on z/OS systems. This application also makes obtaining and applying corrective and recommended maintenance easier. A web-based interface enables you to install and maintain your products faster and with less chance of error. As a best practice, we recommend that you install mainframe products and maintenance using CA CSM. Using CA CSM, someone with limited knowledge of JCL and SMP/E can install a product.

**Note:** If you do not have CA CSM, you can download it from the Download Center at <http://ca.com/support>. Follow the installation instructions in the CA Chorus Software Manager documentation bookshelf on the CA Chorus Software Manager product page.

You can also complete the standardized installation process manually using pax files that are downloaded from <http://ca.com/support> or a product DVD.

To install your product, do the following tasks:

1. Prepare for the installation by [confirming that your site meets all installation requirements](#) (see page 17).
2. Verify that you acquired the product using one of the following methods:
  - Download the software from <http://ca.com/support> using CA CSM.
  - Download the software from <http://ca.com/support> using Pax-Enhanced Electronic Software Delivery (Pax ESD).
  - Order a product DVD. To do so, contact your account manager or a CA Technologies Support representative.
3. Perform an SMP/E installation using one of the following methods:
  - If you used CA CSM to acquire the product, start the installation process from the SMP/E Environments tab in CA CSM.
  - If you used Pax ESD to acquire the product, you can install the product in the following ways:
    - Install the product manually.
    - Complete the SMP/E installation using the Add Product option in CA CSM.
  - If you used a DVD, install the product manually.

**Note:** If a CA Recommended Service (CA RS) package is published for your product, install it before continuing with deployment.

4. Deploy the target libraries using one of the following methods:
  - If you are using CA CSM to configure your products, a CA CSM deployment is required.
  - If you are using a manual configuration process, a manual deployment is an optional step.

**Note:** Deployment is considered part of [starting your product](#) (see page 67).

5. Configure your product using CA CSM or manually.

**Note:** Configuration is considered part of [starting your product](#) (see page 67).

# Chapter 2: About CA Cross-Enterprise Application Performance Management

---

CA Cross-Enterprise Application Performance Management (CA Cross-Enterprise APM) is an extension to CA APM that enables mainframe application monitoring and management from a distributed platform interface. This extension allows you to do the following tasks:

- Manage the performance of distributed applications accessing mainframe back end.
- Trace transactions from distributed applications to mainframe Customer Information Control System (CICS) or Information Management System (IMS) transactions.
- Monitor health metrics of critical mainframe components such as your IBM DB2 database subsystems and network resources.

This extension increases end-to-end visibility for quickly isolating transaction performance problems and allows you to leverage performance data from CA SYSVIEW, CA Insight DPM, and CA NetMaster NM for TCP/IP.

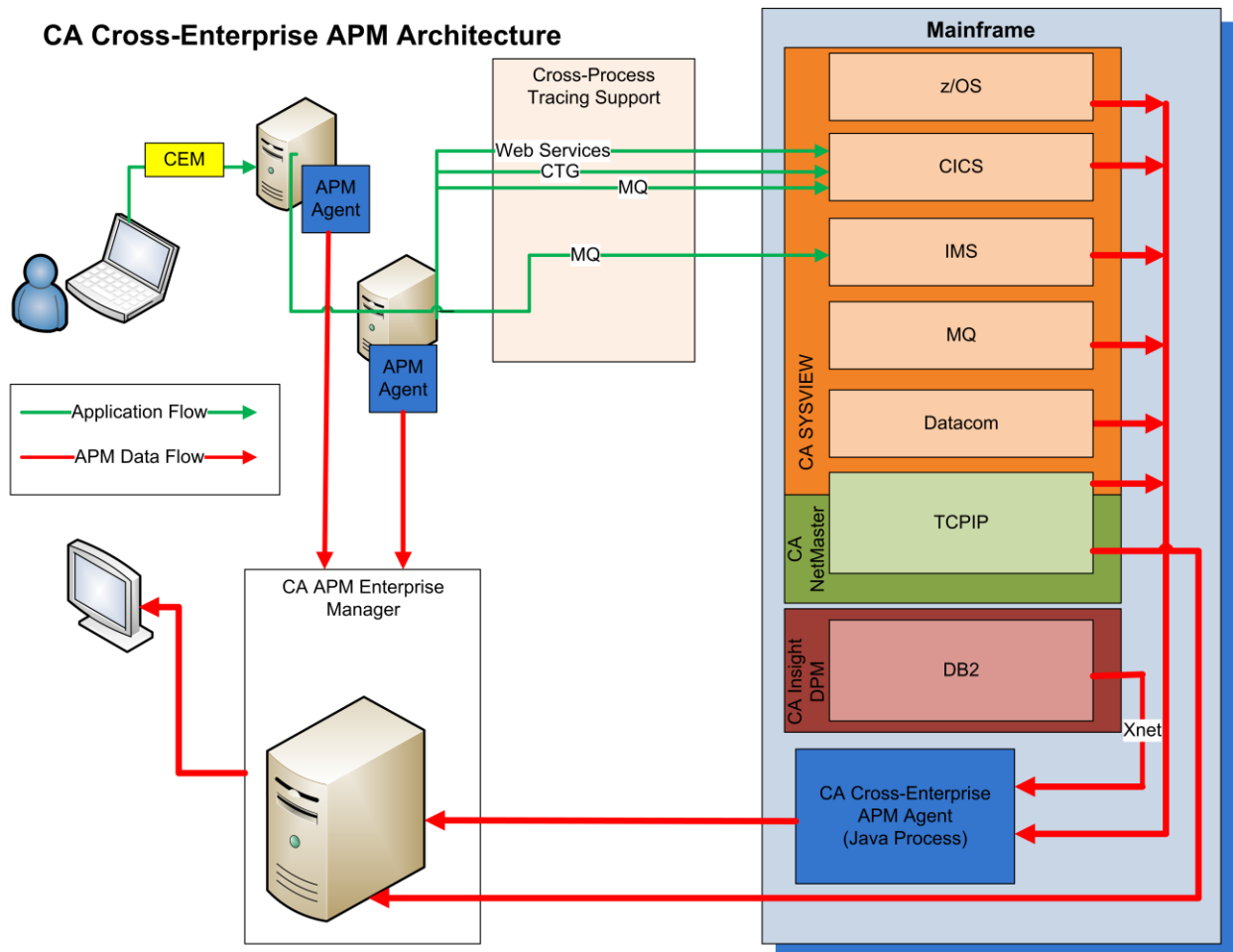
Additionally, it addresses the problems that are associated with applications that span mainframe and distributed environments as these environments have different tools, processes, and teams. Using CA Cross-Enterprise APM, you can bridge all enterprise environments.

This section contains the following topics:

[Architecture](#) (see page 14)

# Architecture

After the installation is complete, CA Cross-Enterprise APM has an architecture that looks like this diagram. The diagram illustrates in general how each component connects to other components. On each z/OS system (Mainframe) that you want CA APM to monitor, you have CA Cross-Enterprise APM Agent, CA SYSVIEW, CA Insight DPM, and CA NetMaster NM for TCP/IP running.



The agent is designed to allow the tracing of transactions across the multiple tiers of an application that invokes transactions on the mainframe. These components are:

- Web Services calls into CICS
- CICS Transaction Gateway (CTG) using channels invoking the CICS transactions
- The WebSphere MQ Series messages sent to CICS or IMS transactions which the mainframe transaction retrieves

On the mainframe, CA Cross-Enterprise APM Agent collects information for analysis from z/OS, CICS, IMS, WebSphere MQ, CA Datacom/DB, and DB2 products components. These collections are done using CA SYSVIEW and CA Insight DPM.

Xnet (Execution Manager Network) provides a communications subsystem that CA Database Management Solutions for DB2 for z/OS shares. Xnet executes as a started task in its own address space between CA Insight DPM and other CA Technologies products, including CA Cross-Enterprise APM and CA SYSVIEW PM. Xnet is required for CA Cross-Enterprise APM to interface with CA Insight DPM to collect DB2 information.

CA NetMaster NM for TCP/IP allows information to be collected for TCP/IP.

**Note:** If you only require TCP/IP network data, you do *not* have to install CA Cross-Enterprise APM but you must have the CA Cross-Enterprise APM license.

All Enterprise Managers (EMs) connect to the APM database to store data for business transactions and application triage maps.

**Note:** For more information, see [Recommended Reading](#) (see page 107) for the documentation that is related to CA Cross-Enterprise APM.





# Chapter 3: Preparing for Installation

---

This section describes what you need to know and do before you install the product.

This section contains the following topics:

[System Requirements](#) (see page 17)

[Software Requirements](#) (see page 18)

[Security Prerequisites](#) (see page 20)

[CA Common Services Requirements](#) (see page 23)

[USS Space Requirements](#) (see page 25)

[Additional Prerequisites](#) (see page 26)

[Application Environment Requirements](#) (see page 27)

[Download the Appropriate CA Cross-Enterprise APM Files](#) (see page 27)

[How to Ready the CA SYSVIEW Product Package for Use with CA Cross-Enterprise APM](#) (see page 28)

[Configure CA Insight DPM for Use with CA Cross-Enterprise APM](#) (see page 33)

[How to Ready the CA NetMaster NM for TCP/IP Product Package for Use with CA Cross-Enterprise APM](#) (see page 40)

## System Requirements

As part of the CA Cross-Enterprise APM solution, you have already installed CA APM.

For the integration between CA APM and CA SYSVIEW, you require the following environment:

- CA APM on a supported operating system
- CA Cross-Enterprise APM and CA SYSVIEW on the same z/OS system

For the integration between CA APM and CA Insight DPM, you require the following environment:

- CA APM on a supported operating system
- CA Cross-Enterprise APM, CA SYSVIEW, and CA Insight DPM on the same z/OS system

For the integration between CA APM and CA NetMaster NM for TCP/IP, you require the following environment:

- CA APM on a supported operating system
- CA Cross-Enterprise APM (You require the license only; you do not have to install the software.)
- CA NetMaster NM for TCP/IP on a z/OS system

## Software Requirements

Before you install CA Cross-Enterprise APM, verify that you have met the following requirements for each component that you plan to enable.

The supported platforms (as applicable):

**Important!** Using CA SYSVIEW Release 13.5 disables certain features. The metrics, typeviews, and dashboards are disabled for z/OS Alerts, z/OS Degradation Delay Analysis, z/OS Workload Manager Service Goals, CICS Alerts, and CICS Degradation Analysis.

Requirement	CA SYSVIEW	CA Insight DPM	CA NetMaster NM for TCP/IP	CA Cross-Enterprise APM
z/OS, JES2, JES3	1.11, 1.12, or 1.13	1.11, 1.12, or 1.13	1.11, 1.12, or 1.13	1.11, 1.12, or 1.13
IMS	10.1, 11.1, or 12.1			
CICS	3.1, 3.2, 4.1, 4.2, or 5.1			
CA Datacom/DB	r11.0, Version 12.0, or Version 14.0			
DB2		8.1, 9.1, or 10.1		
WebSphere MQ for z/OS	6.0, 7.0.1, or 7.1			
CA SYSVIEW PM				Release 13.5 or Release 13.7
CA Insight DPM for DB2 for z/OS (if you plan on retrieving DB2 performance metrics)				r14, r14.5, r15, Version 16.0, or Version 17.0 (all with latest maintenance applied)
CA DB2 Tools Xmanager				Version 14.0 or later
CA DB2 Tools Xnet				Version 14.0 or later
CA NetMaster NM for TCP/IP				Version 12.0 (with maintenance) or Release 12.1
CA APM				Release 9.5
Java				1.5 (31 bit only), 1.6, or 1.7

Requirement	CA SYSVIEW	CA Insight DPM	CA NetMaster NM for TCP/IP	CA Cross-Enterprise APM
UNIX System Services				Enabled

**Note:** The Enterprise Manager can reside on any supported operating system, not only z/OS.

**Note:** The Cross-Enterprise APM Agent must run on the same system (or LPAR) as CA SYSVIEW and CA Insight DPM.

## Management Module

The following information is specific to the Management Module component:

Requirement	Supported Release
CA APM Enterprise Manager	Same release only. The compatible release of Management Module is delivered with the Enterprise Manager. You can enable the module during installation or copy the module from the examples directory afterwards.
CA Introscope Workstation	Same release only.

## Security Prerequisites

Before you install the CA Cross-Enterprise APM, verify these security requirements:

- You can run a batch JCL streams.
- You have READ, WRITE, and ALLOCATE access to the data set prefix or high-level qualifier that is used for the installation.
- You have a user ID with an OMVS segment and UID defined for access to UNIX System Services (USS).
- You have the permission to update and create directories and files in the mount point for the installation.
- If a superuser or a UID(0) rights are not assigned, you require the permission to mount a USS file system.
- If superuser rights are not assigned, you have READ access to the SAF resource SUPERUSER.FILESYS.MOUNT in the UNIXPRIV class.
- The user ID that is assigned to the WILYZOS job has an OMVS segment and UID assigned.
- The WILYZOS user ID has READ access to the high-level qualifier of the installation data set.
- If the WILYZOS user ID does not have superuser rights or is not in the same group ID (GID) as the person installing the software, then CONTROL access to the following SAF resource is required: SUPERUSER.FILESYS in the UNIXPRIV class.
- If the WILYZOS user ID does not have superuser rights, then the ID requires READ access to the SAF resource BPX.CONSOLE in the FACILITY class. Otherwise, the agent issues WTO messages that are prefixed with message ID BPXM023I.
- If PassTicket authentication is required to retrieve metric data from local DB2 subsystems, the WILYZOS user ID must be authorized to generate PassTickets.

**Note:** For more information, see the documentation from your security vendor or see the *IBM z/OS Security Server RACF Security Administrator's Guide*.

Also, configure the Xnet component of CA Database Management Solutions for DB2 for z/OS to accept PassTicket authentication information.

**Note:** If PassTicket support is not configured, specify a valid user ID and password in the agent configuration file. This specification can potentially be a security risk.

## Port and Firewall Requirements

Connectivity is required between the following software and systems:

- The z/OS system on which the Cross-Enterprise APM Agent, CA SYSVIEW, and CA Insight DPM are installed must have connectivity to the CA APM Enterprise Manager.
- The CA APM Enterprise Manager IP address and agent listening port (default 5001) must be opened for connectivity to the z/OS system.
- A TCP listening port (default 15029) provides the connectivity for CA SYSVIEW to send trace information to CA Cross-Enterprise APM.
- (CA NetMaster NM for TCP/IP) CA Introscope EPAgent Network Data Port (default 8000) provides the connectivity between the CA NetMaster NM for TCP/IP region and EPAgent.

## CA Insight DPM Security Requirements

Verify that the following security-related authorizations are in place for the user ID associated with the data collector task:

- The user ID has the appropriate authority to update the exception VSAM data set and the online history VSAM data sets.
- The user ID minimally has TRACE, MONITOR1, and MONITOR2 DB2 privileges.

## CA NetMaster NM for TCP/IP Security Requirements

When you prepare your z/OS task for startup, the following authorities are required on your system:

- If you plan to use ESD to download the product, you require access to UNIX System Services (USS).
- You have READ authority to data sets with a prefix of CAI.\*.
- You have UPDATE authority to the following data sets or libraries:
  - Started task PROCLIB that stores the run-time JCL job, for example, SYS1.PROCLIB
  - SYS1.PARMLIB
  - SYS1.VTAMLST or the library that stores VTAM application definitions and VTAM initialization parameters
  - SYS1.VTAMLIB for terminal mode table definitions
  - Master catalog, a requirement if you intend to define alias entries for data set prefixes
- You have authority to update the following initialization parameter data set members if necessary:
  - SYS1.PARMLIB(IEFSSNxx) to add subsystem IDs
  - SYS1.PARMLIB(IEAAPFxx) to APF-authorize your load libraries
  - SYS1.PARMLIB(CONSOLxx) if your system does not use extended MCS consoles
  - SYS1.PARMLIB(PROGxx) if you want CA Auditor for z/OS or CA Common Inventory Service to know of your products for your auditors
- Ensure that the following conditions are met:
  - The user IDs associated with your started tasks have access to the run-time data sets created by the installation and setup processes (UPDATE authority required).
  - The user ID associated with the product region started task is authorized to issue system commands.
  - The user IDs associated with the product and SOLVE SSI region must have authority to use UNIX System Services.

## CA Common Services Requirements

The following CA Common Services are used with your product:

- CAIRIM
- CAICCI
- CA LMP

**Note:** If other CA Technologies products are installed at your site, some of these services are already installed.

CA Cross-Enterprise APM requires the CA Common Communications Interface (CAICCI) portion of CA Commons Services. CAICCI is used to communicate between the WILYZOS address space and the CA SYSVIEW user address space, SYSVUSER, on the same z/OS host. The CA Event Notification Facility (CAIENF) address space is responsible for starting and initializing CAICCI.

CA Cross-Enterprise APM requires the following components:

- The CAIENF address space must be running.
- The SYSID() statement must be present in the CAIENF/CAICCI parameters.
- CAS9DCM3 must be installed.

CA Cross-Enterprise APM does *not* require that the CCITCP or CCITCPGW address spaces be active, nor does it require that PROTOCOL, NODE, and CONNECT statements be specified. However, other optional functions in base CA SYSVIEW (or other CA Technologies products) require these address spaces and definitions. (For example, the CCITCPGW address space must be active for the Cross-system Resource Monitoring feature of base CA SYSVIEW to operate.)

**Note:** For more information, see the *CA Common Services for z/OS Installation Guide*.

## Install CA Common Services

If you do not have CA Common Services, download and install the software.

**Follow these steps:**

1. Read the CA Common Services cover letter that you have downloaded when you [downloaded the appropriate files](#) (see page 27). This letter shows you where to obtain the documentation if you have not done so already.
2. Install the required software if necessary.
  - a. To validate which, if any, CA Common Services are installed, check which FMIDs are in place. The CA Common Services descriptions, FMIDs, and requirements are located in the *CA Common Services for z/OS Installation Guide*.
  - b. To take advantage of the zIIP enablement of data collection, validate that you have the following CCS levels and fixes:
    - CCS for z/OS r11—FMID CS91000 + PTF RO27636
    - CCS for z/OS r12—FMID CAS9C00 + PTF RO27110
    - CCS for z/OS r14—FMID CAS9E00

## LMP Key Requirements

The CA License Management Program (CA LMP) tracks licensed software in a standardized and automated way. CA LMP uses common real-time enforcement software to validate the user configuration. CA LMP reports on activities that are related to the license, usage, and financials of CA Technologies products.

Your product is licensed with an LMP key. You acquire the LMP key with one of the following methods:

- From your product media
- With Pax ESD
- From <http://ca.com/support>

**Note:** For more information about LMP keys, see the CA Common Services for z/OS documentation.



## Set Up CAICCI for CA Cross-Enterprise APM

Use this procedure if you do not have CAICCI set up.

**Note:** For more information, see the *CA Common Services for z/OS Installation Guide*.

**Follow these steps:**

1. Define the CAICCI SYSID in the CAIENF parameter file or as a separate CCIPARM PDS member concatenated to ENFPARMS, using the following format:

`SYSID(sysid)`

***sysid***

Specifies the CAICCI identifier.

**Limit:** Eight characters

2. Depending on the release of CA Common Services, perform one of the following steps:
  - (r12 or later) Define the CAICCI data collection module (DCM), CAS9DCM3, in your CAIENF parameter file.
  - (r11 SP8) Install CAS9DCM3 into the CAIENF database using the CAS9DB utility.

## USS Space Requirements

Ensure that you have sufficient free space in the USS file system that you are using for Pax ESD to hold the directory that the pax command and its contents create. You need approximately 3.5 times the pax file size in free space.

If you do not have sufficient free space, you receive error message EDC5133I.

## Additional Prerequisites

Gather the following information:

- Know the computer on which your existing Enterprise Manager is installed.
- Identify these directory locations in your CA Introscope Agent environment:
  - Application server home directory — Home directory of your application server.
  - Agent home directory — Installation directory of the CA Introscope Agent for the application server being monitored.
  - Introscope directory — Installation directory for CA Introscope on your Enterprise Manager computer.
  - The directory where *IntroscopeAgent.profile* is located, on each agent where you plan to implement Cross-Enterprise APM.

The agent profile is typically in the top-level directory of the agent installation. The CE APM profile is *Introscope\_Cross-Enterprise\_APM.profile* and is found within <host-location>/Cross-Enterprise\_APM/config/*Introscope\_Cross-Enterprise\_APM.profile*. The CA Introscope Agent profile is *IntroscopeAgent.profile* and is found within <Agent\_Home>\wily\core\config\*IntroscopeAgent.profile*

- Know the components that you plan to install on each computer.

**Note:** For more information, see [Install and Enable the Enterprise Manager Components](#) (see page 88) and [Install and Enable Java Agent Components](#) (see page 90).
- Know the proxy host name and proxy server port (if you have to provide this information to access the CA APM software download area on [CA Support](#)). If your proxy server requires authentication, you must have a valid user name and password for the proxy server.
- Verify if a firewall exists between the CA Cross-Enterprise APM extension and Enterprise Manager, open the CA Cross-Enterprise APM Extension port on the firewall. The extension connects to this port.

**Note:** For more information, see [Configure Network Topology and Firewall Settings](#) (see page 74).

## Application Environment Requirements

To access a CICS back end, end-to-end transaction tracing Java applications must use one of the following methods:

- Java to CICS using Web Services
- Java to CTG and then to CICS (using Channels, or with special review COMMAREA, which must allow for decoration)
- Java to MQ and then to CICS

To access an IMS back end, end-to-end transaction tracing Java applications must access MQ and then to IMS.

## Download the Appropriate CA Cross-Enterprise APM Files

**Note:** If you only require network data, download, install and configure CA NetMaster NM for TCP/IP. You do *not* have to download CA Cross-Enterprise APM, but you must have the CA Cross-Enterprise APM license.

The site ID is given access on CA Support Online to the products being installed.

**Follow these steps:**

1. Access CA Support Online and log in, creating a login ID if necessary, using the site ID that is supplied by CA Technologies.
2. Access the CA Cross-Enterprise Application Performance Management solution for which you have license from Download Center. Select the latest gen level.
3. Download all files that are needed for the installation. Listed are the core pax files for the data collectors and collection agent.

CROSS ENTERPRISE APM MEDIA  
CA DB2 TOOLS PK PAX DNLD ONLY  
CA SYSVIEW PRODUCT PACKAGE  
MF NETWK MGM STE PAX DWNLDONLY

## How to Ready the CA SYSVIEW Product Package for Use with CA Cross-Enterprise APM

### CA SYSVIEW is not installed.

Follow the instructions in *CA SYSVIEW Performance Management Installation Guide*.

### CA SYSVIEW is installed.

Verify the status of the CEAPM option, and the DB2 component is enabled, by running the Installation verification program (IVP). Also verify that the CA Insight DPM agent is configured to start.

**Note:** For information about how to run IVP, see [Post Installation Considerations](#) (see page 31).

**Important!** The CA SYSVIEW option CEAPM must be set and enabled for CA Cross-Enterprise APM to work with CA SYSVIEW.

### To set the CEAPM option

1. Modify the GSVIINST macro parameters in SAMPJCL(INSTALL); remove the “NO” before the CEAPM option.

```
, *-----* X
, * CA SYSVIEW Options * X
, *-----* X
OPTIONS=(,      Begin option list      X
NOCAPTURE,      ...option                X
NOCICS,          ...option                X
NODATACOM,       ...option                X
NOIMS,           ...option                X
NOMVS,           ...option                X
NOMQSERIES,      ...option                X
NOTCPIP,         ...option                X
CEAPM,           ...option                X
NOCHORUS         ...option                X
),              End option list          X
```

2. When the installation steps are complete, begin the configuration using the *CA SYSVIEW Performance Management Installation Guide*. If you are configuring CA SYSVIEW only for CA Cross-Enterprise APM, you only have to run a subset of the jobs.

## CA SYSVIEW Job Steps

The job steps and whether they are required to run for this installation are outlined.

**Important!** These options are based on installing the CA SYSVIEW data collectors for use with CA Cross-Enterprise APM only, and not for using CA SYSVIEW as a real-time performance monitor.

Run?	Job/Procedure	SAMPLIB	Purpose
Yes	INST0005	None	Creates a set of run-time libraries when SMPHLQ is coded.
Yes	INST0010	None	Contains the system information utility, GSVUTIL.
Yes	INST0011	GSVXGSVX	Copies the System Configuration Options member to the system parmlib.
No	INST0013	MVSMAPI	Assembles the MVS DSECT maps.
Yes	INST0020	ASMJES	Assembles and links the JES configuration module.
No	INST0021	JESMAPI	Assembles the JES DSECT maps.
Yes	INST0030	CAPINDEX	Initializes the Event Capture index data set.
No	INST0031	None	Defines the CA GSS IMOD library.
No	INST0032	None	Loads and compiles the IMOD source modules into the CA GSS IMOD library.
No	INST0040	LOGRADTT	Allocates log stream Audit.
No	INST0041	LOGRPLOT	Allocates log stream Plot.
No	INST0042	LOGRXLOG	Allocates log stream Xlog.
No	INST0043	LOGRSMFD	Allocates log stream SMFD.
No	INST0044	LOGRCICS	Allocates log stream CICS.
No	INST0045	LOGRIMTR	Allocates log stream IMS.
No	INST0046	LOGRMQHR	Allocates log stream MQ.
No	INST0050	CNVTSECU	Converts the security data set.
No	INST0051	CNVTPROF	Converts the profile data set.
Yes (if you have CICS)	INST0060	CSDUTIL	Defines the CICS CSD objects.

Run?	Job/Procedure	SAMPLIB	Purpose
Yes (if you have CICS)	INST0061	None	Link edits the CICS object members to create a load module to format the CICS internal trace table entries.
Yes	INST0100	DYNMINST	Dynamically installs the SVC, subsystem, and APF load libraries.
Optional	INST0110	None	Copies the sample members to specific libraries for future use.
Yes	USRM0001	None	Contains USERMOD to assemble and link the default subsystem ID (SSID).

## Start XSXS Subtask

The XSXS (XSystem eXternal Server) subtask in the CA SYSVIEW user address space (SYSVUSER) provides the following functions:

- Interfaces with CAICCI.
- Performs the SYSVUSER portion of the communication between the SYSVUSER address space and the WILYZOS address space.

Verify that the XSXS subtask in the SYSVUSER address space is started. The CA SYSVIEW ASADMIN command display lists the subtasks and the status for each of the tasks in each of the address spaces in CA SYSVIEW. If the XSXS task is not listed as ACTIVE, start the XSXS subtask by issuing an S (START) line command next to the XSXS task.

Also, make a permanent change to ensure that the XSYS task starts up automatically when CA SYSVIEW starts. To accomplish this change, add a START XSXS command to the SYSVUSER parmlib member.

**Note:** For more information, see the *CA SYSVIEW Performance Management Installation Guide*.

## Post-Installation Considerations

The installation verification program (IVP) can be executed when the installation is completed and CA Cross-Enterprise APM is started. IVP can also be executed any time that you want to verify your installation.

IVP provides the following programs:

- GSVUTIL  
Provides functions that let you review the settings of your installation parameters.
- GSVXBAT  
Executes in batch any valid CA Cross-Enterprise APM command so that you can exercise components in CA Cross-Enterprise APM.

### To verify your installation using the program GSVUTIL:

1. Submit member IVP00001.

The resulting IVP report provides the installation settings for the following functions:

- z/OS system
- Subsystem
- Supervisor call (SVC) table
- Authorized Program Facility (APF) list
- SYSVIEW LMP keys

2. Review the report and verify your settings.

### To verify your installation using the program GSVXBAT:

1. Submit member IVP00002.

The output from the CA Cross-Enterprise APM command is returned to the SYSPRINT ddname where the settings can be verified.

2. Review for messages in the SYSPRINT output.

Whether commands return data depends on the installed or active components.

For example, the IMSLIST command display is empty when IMS is inactive.

**Note:** For a sample job, see the SAMPLIB member EXECBAT. For more information about the GSVXBAT program, see the *Administration Guide*.

## Use Groups to Filter Queue Managers and Queues

A way to reduce waste in processing power is to filter out unnecessary data before it reaches the Cross-Enterprise APM Agent. Include or exclude queue managers for the WILYQM group and queues for the WILYQUE group definition.

CA SYSVIEW automatically includes definitions for the WILYQM and WILYQUE groups. We recommend that you add members to these groups so that the agent receives only those queues that are related to the applications in use.

By default, CA SYSVIEW includes all queue managers and queues except for the temporary queues.

**Note:** You may find that you do not need all that data.

CA SYSVIEW automatically filters out the temporary queues, such as PERMDYN and TEMPDYN. You do not have to exclude these queues specifically from the group definitions.

Add a queue manager or queue to the group by adding a separate member key/value pair on a separate line.

### Group Definitions

```
sysvhlq.CNM4BPRM(GROUPS)
```

```
DEFINE WILYQM
    TYPE      MQQMGR
    DESC      'Wily monitored queue managers'
    MEMBER    =
```

```
DEFINE WILYQUE
    TYPE      MQQUEUE
    DESC      'Wily monitored queues'
    MEMBER    =
```

### Example: Filter Queue Managers and Queues

This example shows how to exclude and include queue managers and queues in the group definitions. The modified group definitions exclude the XYZ queue manager and include the ABC queue.

```
DEFINE WILYQM
    TYPE      MQQMGR
    DESC      'Wily monitored queue managers'
    MEMBER    =
    EXCLUDE   XYZ
```



```
DEFINE WILYQUE
  TYPE      MQQUEUE
  DESC      'Wily monitored queues'
  MEMBER    =
  MEMBER    ABC
```

## Configure CA Insight DPM for Use with CA Cross-Enterprise APM

### Recommendations:

1. To allow uninterrupted monitoring of the DB2 subsystem, set up the data collector and PC tasks as started tasks that start automatically upon initial program load (IPL).
2. After the started tasks are defined, set the dispatching priority for the data collector task as follows:
  - Just below the IRLM dispatching priority
  - Above the DB2 address spaces and DB2 applications

The dispatching priority must be high enough to minimize the chance of lost DB2 trace data.

3. Create an OBID translation file during the installation process. CA Insight DPM uses this file to translate pageset, index, and table OBIDs into the actual object names. This file collects data that is more meaningful to your business. This practice allows CA Insight DPM online displays to show object names rather than DBID or OBID numbers.

4. The data collector must have enough trace buffer space to collect trace data. Otherwise, the buffers overflow and trace data is lost.

Two sets of buffers are involved:

- Buffers that are located in common service area (CSA)  
DB2 (instrumentation facility interface (IFI) or service trace exit) uses these buffers to pass trace data to the data collector.
- Buffers residing in the data collector private area  
These buffers flush the CSA buffers and process the records.

The following data collector SYSPARM options control these buffers:

#### **SRVBUFSZ and SRVBUFNUM**

Control the size of the CSA trace buffers.

#### **PRVBUFNUM and PRVMAXSZ**

Control the size of the private area buffers.

Set your parameters based on the following information:

- Type of DB2 subsystem being monitored
- Expected trace workload (such as the volume of trace data)
- Current system paging rate

Higher buffer sizes reduce the chance of lost trace data but increase the demand on real, common, and virtual storage.

On higher-volume systems, we recommend the following settings (to start with a CSA buffer allocation of 4 MB):

- SRVBUFSZ=8
- SRVBUFNUM=128
- PRVBUFNUM=128
- PRVMAXSZ=4096

On a low-volume system, use the following default values:

- SRVBUFSZ=8
- SRVBUFNUM=8
- PRVBUFNUM=12
- PRVMAXSZ=1024

**Note:** You can use the INS IFI command from the user interface to determine the current CSA (IFI monitor size) and private buffer sizes in use. This command also shows the number of trace records that have been lost due to unavailable buffers. If records are being lost and the dispatching priority of the data collector is appropriate, increase these values to reduce the number of lost records.

5. CA Insight DPM has a limited number of displays to combine data from members of a data-sharing group. If the data collector is monitoring a data-sharing DB2 subsystem, we recommend enabling the data-sharing option.

## CA Insight DPM Installation Recommendations

1. We recommend installing the optional history component. The history component lets you view past application and subsystem performance data, which is collected and stored in VSAM history files.
2. If you install the history component, consider the following recommendations:
  - To avoid needing to redefine history and copy history files, pay attention to how the file is allocated (size and secondary extents) during the installation process:
  - Verify that the file is properly sized (primary allocation) for the amount of data to be collected.
- Note:** For information about working with the Online History component, see the *CA Insight DPM System Reference Guide*. You can find out how to adjust allocations for the Online History data sets, and use tables and formulas to estimate the proper history file size.
3. We recommend not defining history files with a secondary extents specification. When the history file is initialized, CA Insight DPM initializes the entire file. This initialization causes the data set to extend into as many extents as possible. Use secondary extents only if you cannot allocate enough space in a primary allocation.
4. Filter the history data (using the HISTORY-ACCT=FILTER SYSPARM option) when implementing history on systems that generate a high volume of accounting records. Filtering the records lets you specify which history records to keep in the history file for subsequent online viewing and which records to discard. Storing all records on a high-volume system can cause the data on the history file to wrap too quickly and generate an unnecessary CPU overhead. You can enable filtering in the HISTORY-ACCT SYSPARM option and customize the FILTERAC IQL request to generate a simple IQL WHERE clause that ignores unwanted records. We recommend using a WHERE clause similar to the following example:

```
WHERE TOTAL-TIME-DB2 > .5
```

This clause causes CA Insight DPM to store records that have an “in DB2”

## CA Insight DPM Post-Installation Recommendations

You can create a common exception data set or a unique exception data set for each data collector. We recommend sharing a single common exception data set between all data collector tasks. In the common exception data set, you can define the following exceptions:

- Define unique exceptions by DB2 subsystem name, if needed. Only those DB2 subsystems that qualify by name use these exceptions.
- Define customized exceptions for production systems as opposed to test or development systems.

Thus, in the common file, you can customize exceptions by subsystem name or type.

## CA Insight Customization

If you are installing CA Insight, review the product customization member and execute the following customization tasks:

- Specify CA Insight customization parameters in the installation JCL (IDB2SYS), and submit for execution. Output from this step includes:
  - JCL to run the program call (PC) task as a batch job or started task
  - New SOURCE library containing common customized members
  - The user interface profile data set
  - Common exception definition data
  - Customized SOURCE members to set up and run the VTAM user interface
  - Customized CLIST members for executing CA Insight tasks
  - Default SECURITY profile data set

**Note:** When migrating from a previous release, you are prompted for information from the previous release so that the information can be migrated.

**Note:** The post installation processing does not describe the installation of GSS or the archive tables. For more information about completing these tasks after the IDB2SYS member is created, see the *CA Insight System Reference Guide*.

- Execute the CA Insight DB2-specific installation task.

The task customizes a data collector for the DB2 subsystem. Each DB2 subsystem has one data collector task.

- Review the *CA Insight System Reference Guide* for more information about:
  - Product authorization
  - Installing components as started tasks
  - Scheduling high-level and detailed DB2 reports using system management facility (SMF) data
  - Managing data collector DASD output
  - Implementing the CICS monitoring facility
  - Implementing data sharing
  - Using the data collector (online and batch)
  - Operating the program call (PC) owner
  - Installing optional components:
    - Global Subsystem (GSS)
    - VTAM User Interface
    - Remote Access Facility (RAF)
    - NATURAL for DB2 Support
    - System Condition Monitor (SCM)
    - Shadow catalog tables for EXPLAIN
  - Controlling CA Insight commands, DB2 IFCIDs, and data through the CA Insight security
  - Using online history
  - Archiving DB2 performance data
  - Integrating with CA NSM Database Option
  - Starting program call (PC) owner tasks per z/OS image.

- Review the *CA Database Management Solutions for DB2 for z/OS Best Practices Guide* for more information about:
  - Starting data collector and PC tasks automatically at IPL.
  - Assigning appropriate authorizations for the user ID associated with the data collector task.
  - Setting the dispatching priority to avoid lost trace data.
  - Creating an OBID table translation file.
  - Allocating adequate trace collection buffer space.
  - Using one exception data set for all data collector tasks.
  - Enabling the data sharing option for data collectors
  - Adjusting the default REGION parameter value
- Review the migration considerations.

We highly recommend that you read the CA Insight installation and upgrade considerations, and known issues in the *Release Notes* for information you should know as you plan your installation.

If you install the online history component, you should only change the primary allocation as needed when allocating the online history files. The maximum data set size supported by data-in-virtual (DIV) data sets is 4 GB or approximately 5825 cylinders.

Secondary extents should not be specified as the data set initialization routine will keep extending the data set until space allocations fails. If you are allocating the data set using an SMS class that supports extended addressability (EA), ensure the allocation attributes will honor the primary allocation with no secondary extents. Otherwise, unused space may be allocated and wasted.

**Note:** For more information about estimating space calculations, see the *CA Insight System Reference Guide*.

## Set Up Xmanager, Xnet, and Required IQL Queries

To retrieve metric data from one or more DB2 subsystems on a single LPAR, install and configure CA Insight DPM on the same LPAR running Cross-Enterprise APM Agent. As part of the installation and configuration of this software, also install and configure the Xmanager and Xnet components.

**Note:** For the available guides to help in this task, see the [CA Insight DPM core documentation set](#) (see page 109).

Specify the **XNETAGT=YES** CA Insight DPM data collector initialization parameter for each DB2 subsystem in your configuration. The data collector initialization parameters reside in the *insight\_hlq.SOURCE(DDCPRMS)* member.

CA Insight DPM includes many Insight Query Language (IQL) queries that can be used to gather information about either itself or the DB2 subsystems currently being monitored. The Cross-Enterprise APM Agent uses several of these IQL queries through the Xmanager/Xnet interface to gather metric data. Specifically, the following IQL queries must be available and started in each CA Insight DPM instance that the Cross-Enterprise APM Agent monitors:

- DSQPARMS
- DSQAPMSS

The DSQAPMSS IQL query is included since CA Insight DPM Version 17.0. Earlier releases have the following PTF requirements:

- Version 16.0 requires RO52880 and RO52881.
- r15 requires RO52873 and RO52874.
- r14.5 requires RO52871 and RO52872.
- r14 requires RO52869 and RO52870.

If multiple CA Insight DPM instances are monitoring the same DB2 subsystem, each instance must have these IQL queries started for the Cross-Enterprise APM Agent to retrieve metrics.

## How to Ready the CA NetMaster NM for TCP/IP Product Package for Use with CA Cross-Enterprise APM

### CA NetMaster NM for TCP/IP is not installed.

Follow the instructions in *CA NetMaster Network Management for TCP/IP Installation Guide*.

### CA NetMaster NM for TCP/IP is installed and configured.

Verify that the following parameter is in *dsnpref.rname*.TESTEXEC(RUNSYSIN). *dsnpref* is the data set prefix, and *rname* is the CA NetMaster NM for TCP/IP region name.

**PPREF='PROD=APM'**

Includes the CA Cross-Enterprise APM feature in the region.

If the parameter is missing, add the parameter in RUNSYSIN.

## CA NetMaster NM for TCP/IP Installation Considerations

To install CA NetMaster NM for TCP/IP, use the *CA NetMaster Network Management for TCP/IP Installation Guide*. The guide contains the information to install the full product. If you are installing CA NetMaster NM for TCP/IP only for CA Cross-Enterprise APM, note the following considerations:

- With only the CA Cross-Enterprise APM license, CA NetMaster NM for TCP/IP does *not* support CA TCPaccess Telnet Server and CA TCPaccess CS.
- You do *not* have to install WebCenter.
- You do *not* use the SOLVE Subsystem Interface (SSI) task as the Program-to-Program Interface (PPI) provider.
- If you configure the product manually, you do *not* have to submit the V02ASMOD job to assemble the VTAM MODE table.
- You do *not* have to grant the CA NetMaster NM for TCP/IP region permission to issue the z/OS operator VARY commands.
- You do *not* have to perform IPsec-related tasks.



# Chapter 4: Installing Your Product Using CA CSM

---

**Note:** If you only want to integrate CA APM with CA NetMaster NM for TCP/IP, you do *not* have to perform these tasks to install CA Cross-Enterprise APM.

## How to Install Your Product Using CA CSM

As a system programmer, your responsibilities include acquiring, installing, maintaining, deploying, and configuring CA Technologies mainframe products on your system.

CA CSM is an application that simplifies and unifies the management of your CA Technologies mainframe products on z/OS systems. As products adopt the CA CSM services, you can install your products in a common way according to industry best practices.

This scenario describes the steps for a system programmer to acquire, install, deploy, and configure products and maintenance. Not all tasks may apply to your organization. For example, you may decide not to deploy and configure products. In this case, do not perform the product deployment task and the product configuration task.

Before you use this scenario, you must have CA CSM installed at your site. If you do not have CA CSM installed, you can download it from the Download Center at <http://ca.com/support>. This web page also contains links to the complete documentation for CA CSM.

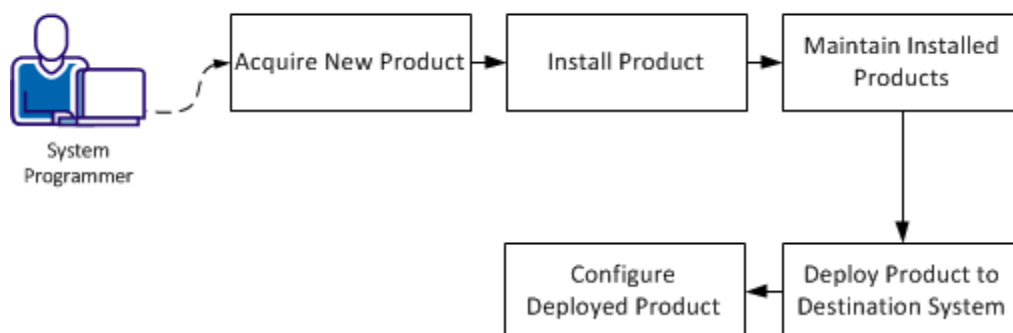
You [access CA CSM](#) (see page 42) from a web browser.

**Note:** This scenario applies to the latest version of CA CSM. If you are using an earlier version, see the appropriate bookshelf on the CA Chorus Software Manager product page.

This scenario is a high-level overview of steps that you perform using CA CSM. For more detailed information, use the online help that is included in CA CSM.

You perform the following tasks to install products and manage them on your system:

### How to Install Your Product Using CA CSM



1. [Acquire a new product](#) (see page 43).
2. [Install the product](#) (see page 44).
3. [Maintain the installed products](#) (see page 46).
4. [Deploy the product to the destination system](#) (see page 47).
5. [Configure the deployed product](#) (see page 48).

## Access CA CSM Using the Web-Based Interface

You access CA CSM using the web-based interface.

You need the URL of CA CSM from the CA CSM administrator.

### Follow these steps:

1. Start your web browser, and enter the access URL.

The login page appears.

**Note:** If the Notice and Consent Banner appears, read and confirm the provided information.

2. Enter your z/OS login user name and password.

The initial page appears. If you log in for the first time, you are prompted to define your account on [the CA Support Online website](#).

**Note:** For more information about the interface, click the online help link at the top right corner of the page.

3. Click New.

You are prompted for the credentials to use on [the CA Support Online website](#).

4. Specify the credentials, click OK, and then click Next.

You are prompted to review your user settings.

**Note:** These settings are available on the User Settings page.

5. Change the settings or keep the defaults, and then click Finish.

A dialog opens, which shows the progress of the configuration task. You can click Show Results to view the details of the actions in a finished task.

**Important!** If your site uses proxies, review your proxy credentials on the User Settings, Software Acquisition page.

## Acquire a New Product

Acquisition allows you to download products and product maintenance from the CA Support Online website at <http://ca.com/support> to a USS directory structure on your system. The products to which your site is entitled and the releases available are displayed in the Available Products section on the Products page.

You perform the following high-level tasks to acquire a product using CA CSM:

1. Set up a CA Support Online account at <http://ca.com/support>.

To use CA CSM to acquire or download a product, you must have a CA Support Online account. If you do not have an account, create one on <http://ca.com/support>.

2. Determine the CA CSM URL for your site.

To [access CA CSM](#) (see page 42), you require its URL. You can get the URL from your site CA CSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA CSM account with your credentials that you use to access <http://ca.com/support>. This account enables you to download product packages.

3. Log in to CA CSM and go to the Products page to locate the product that you want to acquire.

After you log in to CA CSM, you can see the products to which your organization is entitled on the Products tab.

If you cannot find the product that you want to acquire, update the product list. CA CSM refreshes the product list through <http://ca.com/support> using the site IDs associated with your credentials.

4. Download the product installation packages.

After you find your product in the product list, you can download the product installation packages.

CA CSM downloads (acquires) the packages (including any maintenance packages) from the CA Support Online website.

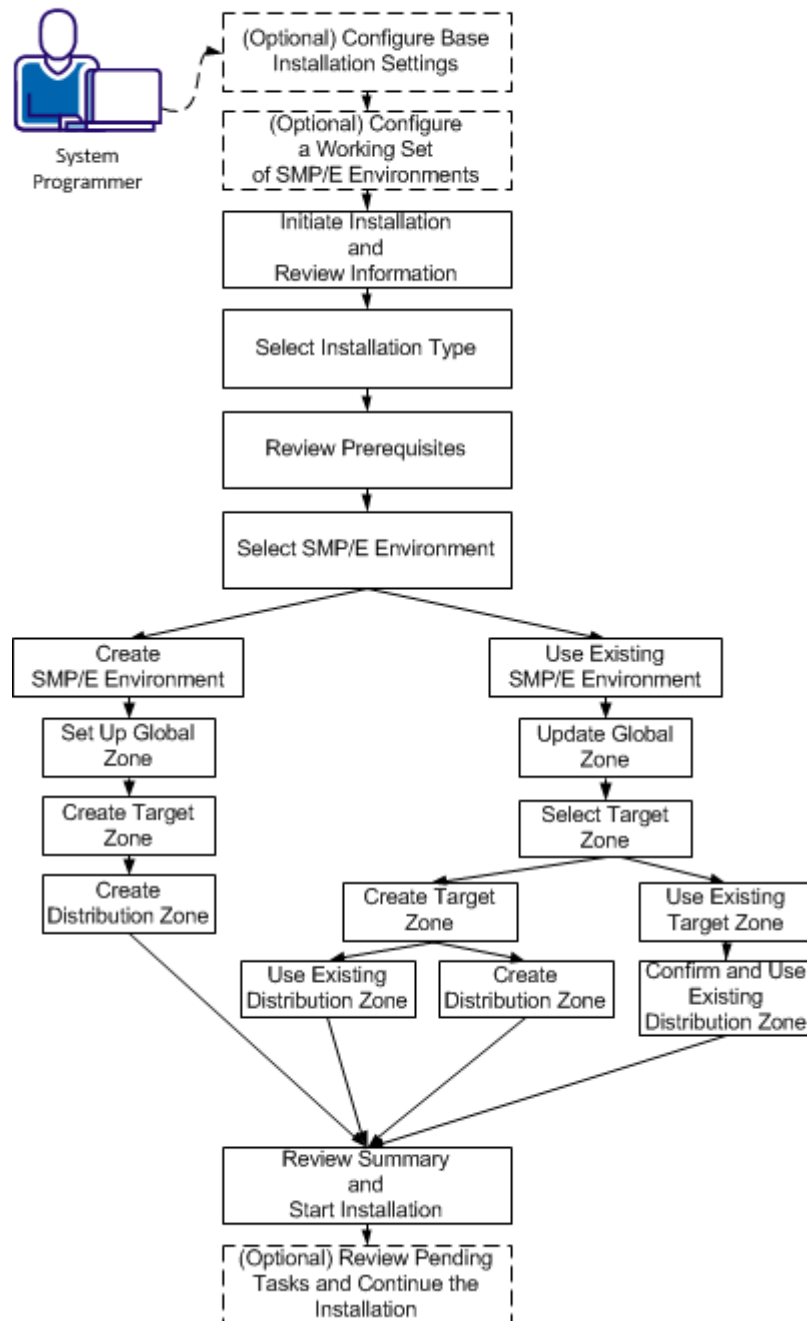
After the acquisition process completes, the product is ready for you to install or apply maintenance.

## Install a Product

CA CSM simplifies and manages SMP/E installation tasks. You can browse and install a product that you acquired and that is available in the product list on the Products page. You can also install the maintenance for the products that are currently installed in a managed SMP/E environment on the driving system.

You perform the following high-level tasks to install a product using CA CSM:

### How to Install a Product



1. (Optional) On the Settings tab, click Software Installation under System Settings, and configure base installation settings.
2. (Optional) Click the SMP/E Environments tab, and configure a working set of SMP/E environments.
3. Click the Products tab and select a product that you want to install. Start the installation wizard and review product information.
4. Select an installation type.
5. Review installation prerequisites if any are presented.
6. Take *one* of the following steps to select an SMP/E environment:
  - Create an SMP/E environment:
    - a. Set up the global zone.
    - b. Create a target zone.
    - c. Create a distribution zone.
  - Use an existing SMP/E environment from your working set:
    - a. Update the global zone.
    - b. Set up the target zone: Create a target zone or use an existing target zone.
    - c. Set up the distribution zone: Create a distribution zone or use an existing distribution zone.
7. Review the installation summary and start the installation.
8. (Optional) Review pending tasks for the SMP/E environment where you are installing your product. Continue the installation, if applicable.

CA CSM installs the product.

After the installation process completes, check for and install available product maintenance. The product is ready for you to deploy. Sometimes, there are other steps to perform manually outside of CA CSM before continuing.

## Maintain the Installed Products

You can migrate existing SMP/E environments into CA CSM to maintain all your installed products in a unified way from a single web-based interface.

You can use CA CSM to maintain a CA Technologies product.

You perform the following high-level tasks to maintain a product using CA CSM:

1. Verify that CA CSM recognizes the SMP/E environment where your product is installed. If not, migrate the SMP/E environment to CA CSM.

During the migration, CA CSM stores information about the SMP/E environment in the database.

2. From the Product tab, download the latest maintenance for the installed product releases.

If you cannot find the required release, perform the following steps to download the maintenance:

- a. Add the release manually.
- b. Update the release.

3. Apply the maintenance.

CA CSM applies the maintenance to your product.

After the maintenance process completes, the product is ready for you to deploy to systems that are defined in the system registry.

## Deploy the Product to the Destination System

Deployment is a process of copying SMP/E target libraries to a destination system. The destination system could be the local z/OS system, a remote z/OS system, or a sysplex. You identify the destination system, deployed data set names, and the transport mechanism as part of the deployment process. Deploying a product makes it available for configuration.

**Important!** Before you deploy a product, set up the destination systems and remote credentials in the system registry.

You perform the following high-level tasks to deploy your products using CA CSM:

1. On the Deployments tab, set up methodologies.

**Note:** You can also set up methodologies when creating a deployment, or use existing methodologies, if you have set up any previously. If you do so, you can skip this step.

2. Start the New Deployment wizard to create a deployment. Complete each of the steps in the wizard. The wizard guides you through choosing deployment settings for your site. At any point, you can save your work and come back to it later.

3. Deploy:
  - a. Take a snapshot of the deployment.
  - b. Transmit the deployment to a destination system.
  - c. Deploy (unpack) to the mainframe environment.CA CSM deploys the product to the destination system.

After the deployment process completes, the product is ready for you to configure.

## Configure the Deployed Product

Configuration copies the deployed libraries to run-time libraries and customizes the product for your site to bring it to an executable state. You can configure CA Technologies products that you have already acquired, installed, and deployed using CA CSM. You cannot use CA CSM to configure a product unless you have already used CA CSM to deploy the product.

You perform the following high-level tasks to configure your products using CA CSM:

1. Select a configurable deployment on the Deployments tab to view details and products for that deployment.
2. Select a product in the deployment and start the Configuration wizard to create a configuration. Complete each of the steps in the wizard. The wizard has multiple levels of detailed instructions and guides you through choosing configuration settings for your site. At any point, you can save your work and come back to it later. Configurations where you have partially completed the steps in the wizard are listed on the Configurations tab. The steps in the wizard include the following:
  - a. Define a configuration name and select a system for the configuration.
  - b. Select configuration functions and options.
  - c. Define system preferences.
  - d. Create target settings.
  - e. Select and edit resources.
3. Build the configuration. The last step of the Configuration wizard lets you build the configuration. If needed, you can edit the configuration and can build the configuration again. Building the configuration closes the wizard and creates a configuration with all your settings.
4. (Optional) Validate the configuration. Validation verifies access to resources that are going to be used when you implement the configuration.



5. Implement the configuration. You implement a configuration to make your deployed software fully functional. Implementation executes on the destination system, applying the variables, resources, and operations that are defined in the configuration.

CA CSM configures the product.

After the configuration process completes, the product is ready for you to use.



# Chapter 5: Installing Your Product Using Pax ESD or DVD

---

This section contains the following topics:

[How to Install Your Product Using a Pax File](#) (see page 51)

[Allocate and Mount a File System](#) (see page 53)

[Acquire the Product Pax Files](#) (see page 55)

[Create a Product Directory from the Pax File](#) (see page 60)

[Copy Installation Files to z/OS Data Sets](#) (see page 61)

[Install the Cross-Enterprise APM Agent](#) (see page 63)

[Clean Up the USS Directory](#) (see page 64)

[Maintain the Cross-Enterprise APM Agent](#) (see page 64)

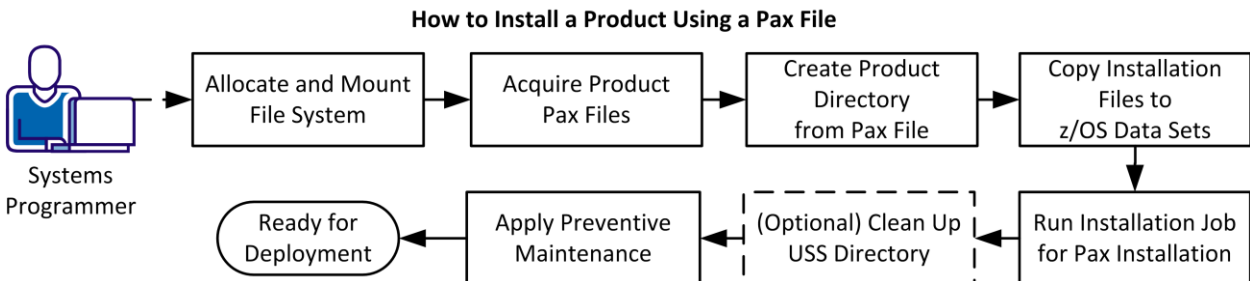
**Note:** If you only want to integrate CA APM with CA NetMaster NM for TCP/IP, you do *not* have to perform these tasks to install CA Cross-Enterprise APM.

## How to Install Your Product Using a Pax File

As a system programmer, your responsibilities include installing products on your mainframe system. With this option, you acquire a product pax file from <http://ca.com/support> or from a product DVD.

The DVD contains a folder that includes the pax file for the product. Product updates may have occurred after you acquired the product DVD. The files on the online site always have the most current product updates. To determine if you have the latest updates, go to <http://ca.com/support> and click Download Center.

You perform the following tasks to install a product with a pax file:



1. [Allocate and mount the file system](#) (see page 53).
2. [Acquire the product pax files](#) (see page 55).

3. [Create a product directory from the pax file](#) (see page 60).
4. [Copy the installation files to z/OS data sets](#) (see page 61).
5. [Run the installation job for a pax installation](#) (see page 63).
6. (Optional) [Clean up the USS directory](#) (see page 64).
7. [Apply preventive maintenance](#) (see page 64).

## USS Environment Setup

You need a UNIX System Services (USS) directory and a file system with adequate space to perform the following tasks:

- Receive product pax files from <http://ca.com/support>.
- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.

We recommend that you allocate and mount a file system that is dedicated to Pax ESD. The amount of space that you need for the file system depends on the following variables:

- The size of the pax files that you intend to download.
- Whether you plan to keep the pax files after unpacking them. We do not recommend this practice.

We recommend that you use one directory for downloading and unpacking pax files. Reusing the same directory minimizes USS setup. You need to complete the USS setup only one time. You reuse the same directory for subsequent downloads. Alternatively, you can create a directory for each pax download.

**Important!** Downloading pax files for the SMP/E installation as part of the Pax ESD process requires write authority to the UNIX System Services (USS) directories that are used for the Pax ESD process. In the file system that contains the Pax ESD directories, you also need free space approximately 3.5 times the pax file size to download the pax file and unpack its contents. For example, to download and unpack a 14 MB pax file, you need approximately 49 MB of free space in the file system hosting your Pax ESD directory.

## Allocate and Mount a File System

The product installation process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system that is dedicated to the product acquisition and create the directory in this file system.

You can use the zSeries File System (zFS) or hierarchical file system (HFS) for product downloads.

This procedure describes how to perform the following tasks:

- Allocate a zFS or an HFS.
- Create a mount point in an existing maintenance USS directory of your choice.
- Mount the file system on the newly created mount point.

**Note:** You must have either SUPERUSER authority, or the required SAF profile setting to allow you to issue the USS mount command for the file system.

- Optionally, permit write access to anyone in the same group as the person who created the directory.

**Important!** USS commands are case-sensitive.

### Follow these steps:

1. Allocate the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
//DEFINE EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//AMSDUMP DD SYSOUT=*
//SYSIN DD *
  DEFINE CLUSTER ( +
    NAME(your_zFS_data_set_name) +
    STORAGECLASS(class) +
    LINEAR +
    CYL(primary secondary) +
    SHAREOPTIONS(3,3) +
  )
/*
//FORMAT EXEC PGM=IOEAGFMT,REGION=0M,
// PARM=(' -aggregate your_zFS_data_set_name -compat')
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
//CEEDUMP DD SYSOUT=*
/*
```

- On an HFS, use the following sample:

```
//ALCHFS EXEC PGM=IEFBR14
//CAPAX DD DSN=yourHFS_data_set_name,
// DISP=(NEW,CATLG,DELETE),UNIT=3390,
// DSN TYPE=HFS,SPACE=(CYL,(primary,secondary,1))
```

The file system is allocated.

**Note:** Ensure that the zFS or HFS data set name that you use conforms to your data set naming conventions for USS file systems. If the allocation of the file system data set fails, it is because of environmental settings not allowing for the allocation. On an HFS, try using the ISPF 3.2 Data Set Utility to allocate your HFS data set.

2. Create a mount point for the file system. This example shows how to create a /CA/CAPAX directory in an existing directory, /u/maint. From the TSO OMVS shell, enter the following commands:

```
cd /u/maint/
mkdir CA
cd CA
mkdir CAPAX
```

**Note:** This document refers to this structure as *yourUSSpaxdirectory*.

The mount point is created.

3. Mount the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
MOUNT FILESYSTEM('your_zFS_data_set_name')
MOUNTPOINT('yourUSSpaxdirectory')
TYPE(ZFS) MODE(RDWR)
PARM(AGGREGROW)
```

- On an HFS, use the following sample:

```
MOUNT FILESYSTEM('your_HFS_data_set_name')
MOUNTPOINT('yourUSSpaxdirectory')
TYPE(HFS) MODE(RDWR)
```

The file system is mounted.

4. (Optional) Set security permissions for the directory. You can use the chmod command to let other users access the Pax ESD directory and its files. For example, to allow write access to the Pax ESD directory for other users in your USS group, from the TSO OMVS shell, enter the following command:

```
chmod -R 775 /yourUSSpaxdirectory/
```

Write access is granted.

**Note:** For more information about the chmod command, see the IBM *z/OS UNIX System Services User Guide* (SA22-7802).

## Acquire the Product Pax Files

To begin the CA Technologies product installation procedure, copy the product pax file into the USS directory that you set up.

**Important!** Downloading pax files for the SMP/E installation as part of the Pax ESD process requires write authority to the UNIX System Services (USS) directories that are used for the Pax ESD process. Also, you must have available USS file space before you start the procedures in this guide.

Use one of the following methods:

- [Download the product pax file from http://ca.com/support to your PC](http://ca.com/support) (see page 56), and then upload it to your USS file system.  
  
If you download a zip file, you must unzip it before uploading to your USS file system.
- [Download the pax files from http://ca.com/support directly to your USS file system](http://ca.com/support) (see page 56).
- [Download the pax file from the product DVD to your PC, and then upload the pax files to your USS file system.](#) (see page 59)

This section includes the following information:

- A sample batch job to download a product pax file from the CA Support Online FTP server directly to a USS directory on your z/OS system
- Sample commands to upload a pax file from your PC to a USS directory on your z/OS system

**Important!** The FTP procedures vary due to local firewall and other security settings. Consult your local network administrators to determine the appropriate FTP procedure to use at your site.

Ensure that sufficient free space is available in the USS file system that you are using to hold the product pax file. If you do not have sufficient free space, error messages similar to the following appear:

```
EZA1490I Error writing to data set  
EZA2606W File I/O error 133
```

When the download finishes, the pax file size in your USS directory matches the value in the Size column for the corresponding pax file on the CA Technologies Products Download window.

## Download Files to a PC Using Pax ESD

You can download product installation files from <http://ca.com/support> to your PC.

### Follow these steps:

1. Log in to <http://ca.com/support>, and click Download Center.  
The Download Center web page appears.
2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and gen level (if applicable), and click Go.  
The CA Product Download window appears.
3. Download an entire CA Technologies product software package or individual pax files to your PC. If you download a zip file, you must unzip it before continuing.

**Note:** For traditional installation downloads, see the *Traditional ESD User Guide*. For information about download methods, see the Download Methods and Locations article. Go to <http://ca.com/support>, log in, and click Download Center. Links to the guide and the article appear under the Download Help heading.

## Download Using Batch JCL

You download a pax file from <http://ca.com/support> by running batch JCL on the mainframe. Use the sample JCL attached to the PDF file as [CAtoMainframe.txt](#) (see page 58) to perform the download.

**Important!** The PDF version of this guide includes sample JCL jobs that you can copy directly to the mainframe. To access these jobs, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click a file to view a sample JCL. We recommend that you use the latest version of Adobe Reader for viewing PDF files.

**Note:** We recommend that you follow the preferred download method as described on <http://ca.com/support>. This JCL procedure is our preferred download method for users who do not use CA CSM. We also include the procedure to download to the mainframe through a PC in the next section.

### Follow these steps:

1. Replace *ACCOUNTNO* with a valid JOB statement.  
The job points to your profile.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.  
The job points to your email address.
3. Replace *YourEmailAddress* with your email address.  
The job points to your email address.



4. Replace *yourUSSpaxdirectory* with the name of the USS directory that you use for Pax ESD downloads.

The job points to your USS directory.

5. Locate the product component to download on the CA Support Product Download window.

You have identified the product component to download.

6. Click Download for the applicable file.

**Note:** For multiple downloads, add files to a cart.

The Download Method window opens.

7. Click FTP Request.

The Review Download Requests window displays any files that you have requested to download.

**Note:** We send you an email when the file is ready to download or a link appears in this window when the file is available.

8. Select one of the following methods:

**Preferred FTP**

Uses CA Technologies worldwide content delivery network (CDN). If you cannot download using this method, review the security restrictions for servers that company employees can download from that are outside your corporate network.

**Host Name:** ftp://ftpdnloads.ca.com

**Alternate FTP**

Uses the original download servers that are based on Long Island, New York.

**Host Name:** ftp://scftpd.ca.com for product files and download cart files and ftp://ftp.ca.com for individual solution files.

Both methods display the host, user name, password, and FTP location, which you then can copy into the sample JCL.

**Note:** The following links provide details regarding FTP: the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

**Important!** If your FTP commands are incorrect, it is possible for this job to fail and still return a zero condition code. Read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

After you run the JCL job, the pax file resides in the mainframe USS directory that you supplied.

## Example: CAtoMainframe.txt, JCL

The following text appears in the attached CAtoMainframe.txt JCL file:

```
//GETPAX JOB (ACCOUNTNO),'FTP GET PAX ESD PACKAGE',
//          MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to download a pax file directly from *
/* CA Support Online to a USS directory on your z/OS system.      *
/*                                                                *
/* When editing the JCL ensure that you do not have sequence numbers *
/* turned on.                                                    *
/*                                                                *
/* This job must be customized as follows:                        *
/* 1. Supply a valid JOB statement.                              *
/* 2. The SYSTCPD and SYSFTPD JCL DD statements in this JCL may be *
/*    optional at your site. Remove the statements that are not  *
/*    required. For the required statements, update the data set  *
/*    names with the correct site-specific data set names.       *
/* 3. Replace "Host" based on the type of download method.       *
/* 4. Replace "YourEmailAddress" with your email address.        *
/* 5. Replace "yourUSSpaxdirectory" with the name of the USS      *
/*    directory used on your system for Pax ESD downloads.       *
/* 6. Replace "FTP Location" with the complete path              *
/*    and name of the pax file obtained from the FTP location   *
/*    of the product download page.                              *
//*****
//GETPAX EXEC PGM=FTP,PARM='(EXIT',REGION=0M
//SYSTCPD DD DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSFTPD DD DSN=yourFTP.DATA.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//OUTPUT DD SYSOUT=*
//INPUT DD *
Host
anonymous YourEmailAddress
lcd yourUSSpaxdirectory
binary
get FTP_location
quit
```

## Download Files to Mainframe through a PC

You download the product installation files to your PC and transfer them to your USS system.

**Follow these steps:**

1. Download the product file to your PC using one of the following methods:
  - [Pax ESD](#) (see page 56). If you downloaded a zip file, first unzip the file to use the product pax files.
  - DVD. Copy the entire product software package (or individual pax files) to your PC.

The pax file resides on your PC.

**Note:** Do *not* change the format of the pax.Z.

2. Open a Windows command prompt.

The command prompt appears.

3. Customize and enter the following FTP commands:

```
FTP mainframe
userid
password
bin
lcd C:\PC\folder\for\thePAXfile
cd /yourUSSpaxdirectory/
put paxfile.pax.Z
quit
exit
```

***mainframe***

Specifies the z/OS system IP address or DNS name.

***userid***

Specifies your z/OS user ID.

***password***

Specifies your z/OS password.

***C:\PC\folder\for\thePAXfile***

Specifies the location of the pax file on your PC.

**Note:** If you specify a location that has blanks or special characters in the path name, enclose that value in double quotation marks.

***yourUSSpaxdirectory***

Specifies the name of the USS directory that you use for Pax ESD downloads.

***paxfile.pax.Z***

Specifies the name of the pax file to upload.

The pax file is transferred to the mainframe.

## Create a Product Directory from the Pax File

The pax command performs the following actions:

- Extracts the files and directories that are packaged within the pax file.
- Creates a USS directory in the same directory structure where the pax file resides.
- Automatically generates a product and level-specific directory name.

Set the current working directory to the directory containing the pax file, and create a directory in your USS directory by entering the following command:

```
pax -rvf pax-filename
```

Use the sample JCL that is attached to the PDF file as [Unpackage.txt](#) (see page 61) to extract the product pax file into a product installation directory.

**Important!** The PDF version of this guide includes sample JCL jobs that you can copy directly to the mainframe. To access these jobs, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click a file to view a sample JCL. We recommend that you use the latest version of Adobe Reader for viewing PDF files.

**Follow these steps:**

1. Replace *ACCOUNTNO* with a valid JOB statement.
2. Replace *yourUSSpaxdirectory* with the name of the USS directory that you use for product downloads.

The job points to your specific directory.

3. Replace *paxfile.pax.Z* with the name of the pax file.

The job points to your specific pax file.

4. Submit the job.

The job creates the product directory.

**Note:** If the PARM= statement exceeds 71 characters, uncomment and use the second form of UNPAXDIR instead. This sample job uses an X in column 72 to continue the PARM= parameters to a second line.

## Example: JCL File, Unpackage.txt, to Customize

The following text appears in the attached Unpackage.txt JCL file:

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX PAX ESD PACKAGE',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to invoke the pax command to create *
/* the product-specific installation directory. *
/* *
/* This job must be customized as follows: *
/* 1. Supply a valid JOB statement. *
/* 2. Replace "yourUSSpaxdirectory" with the name of the USS *
/* directory used on your system for Pax ESD downloads. *
/* 3. Replace "paxfile.pax.Z" with the name of the pax file. *
/* NOTE: If you continue the PARM= statement on a second line, make *
/* sure the 'X' continuation character is in column 72. *
//*****
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSpaxdirectory/; pax -rvf paxfile.pax.Z'
/*UNPAXDIR EXEC PGM=BPXBATCH,
/* PARM='sh cd /yourUSSpaxdirectory/; pax X
/* -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

## Copy Installation Files to z/OS Data Sets

Use this procedure to invoke the SMP/E GIMUNZIP utility to create MVS data sets from the files in the product-specific directory.

The file UNZIPJCL in the product directory contains a sample job to GIMUNZIP the installation package. You edit and submit the UNZIPJCL job to create z/OS data sets.

**Follow these steps:**

1. Locate and read the product readme file or installation notes, if applicable, which resides in the product-specific directory that the pax command created. This file contains the product-specific details that you require to complete the installation procedure.

You have identified the product-specific installation details.

2. Use ISPF EDIT or TSO ISHELL to edit the UNZIPJCL sample job. You can perform this step in one of the following ways:
  - Use ISPF EDIT. Specify the full path name of the UNZIPJCL file.
  - Use TSO ISHELL. Navigate to the UNZIPJCL file and use the E line command to edit the file.

The job is edited.

3. Change the SMPDIR DD PATH to the product-specific directory created by the pax command.

Your view is of the product-specific directory.

4. If ICSF is not active, perform the following steps:
  - a. Change the SMPJHOME DD PATH to your Java runtime directory. This directory varies from system to system.
  - b. Perform one of the following steps:
    - Change the SMPCPATH DD PATH to your SMP/E Java application classes directory, typically /usr/lpp/smp/classes/.
    - Change HASH=YES to HASH=NO on the GIMUNZIP parameter.

One of the following occurs: ICSF is active or you are using Java.

5. Change all occurrences of *yourHLQ* to the high-level qualifier (HLQ) for z/OS data sets that the installation process uses. We suggest that you use a unique HLQ for each expanded pax file to identify uniquely the package. Do *not* use the same value for *yourHLQ* as you use for the SMP/E RELFILES.

All occurrences of *yourHLQ* are set to your high-level qualifier for z/OS data sets.

6. Submit the UNZIPJCL job.

The UNZIPJCL job completes with a zero return code. Messages GIM69158I and GIM48101I in the output and IKJ56228I in the JES log are acceptable.

GIMUNZIP creates z/OS data sets with the high-level qualifier that you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed.

**Note:** For more information, see the IBM *SMP/E for z/OS Reference (SA22-7772)*.

## Install the Cross-Enterprise APM Agent

To install the agent, customize and submit the installation jobs.

**Follow these steps:**

1. Customize the sample batch JCL in the *yourHLQ.CAI.SAMPJCL(SMPALLOC)* member as instructed.
2. Submit the batch job.

The job allocates and mounts the z/FS file system and MVS data sets required for the installation. The MVS data sets are named using the high-level qualifier (*smp*) specified in the JCL. The zFS file system is mounted on the mount point, */root/C7C4950/*, using the root name that is specified in the JCL. The default value for *root* is */usr/lpp/CAI*.

3. Carefully read the CA Technologies End User License Agreement (EULA) in the *yourHLQ.CAI.SMPMCS* data set in SMP/E HOLDDATA.
4. Customize the sample batch JCL in the *yourHLQ.CAI.SAMPJCL(SMPINSDA)* member as instructed.
5. Bypass the SMP/E HOLDDATA that contains the CA Technologies EULA.

This agreement confirms that you have read, understood, and will comply with all the terms and conditions that are outlined in the EULA.

6. Submit the batch job to SMP/E receive, apply, and accept the CA Cross-Enterprise APM base product into the following locations:
  - SMP/E target library *smp.C7C4JCL*
  - SMP/E target paths */root/C7C4950/C7C4HFS/* and */root/C7C4950/C7C4JAR/*
7. After you have finished installing the extension, deploy it.

**Note:** For more information, see [Deploy the Cross-Enterprise APM Agent](#) (see page 67).

## Clean Up the USS Directory

**Important!** This procedure is optional. Do not use this procedure until you complete the entire installation process.

To free file system disk space for subsequent downloads after downloading and processing the pax files for your CA Technologies product, we recommend removing the files from your USS directory and deleting unnecessary MVS data sets. You can delete the following items:

- Pax file
- Product-specific directory that the pax command created and all of the files in it
- SMP/E RELFILES, SMPMCS, and HOLDDATA MVS data sets

These data sets have the HLQ that you assigned in the UNZIPJCL job.

**Note:** Retain non-SMP/E installation data sets such as *yourHLQ*.INSTALL.NOTES for future reference.

### Follow these steps:

1. Navigate to your Pax ESD USS directory.

Your view is of the applicable USS directory.

2. Delete the pax file by entering the following command:

```
rm paxfile
```

***paxfile***

Specifies the name of the CA Technologies pax file that you downloaded.

The pax file is deleted.

3. Delete the product-specific directory by entering the following command:

```
rm -r product-specific_directory
```

***product-specific\_directory***

Specifies the product-specific directory that the pax command created.

The product-specific directory is deleted.

**Note:** You can also use TSO ISHELL to navigate to the pax file and product-specific directory, and delete them using the D line command.

## Maintain the Cross-Enterprise APM Agent

CA Cross-Enterprise APM is maintained using SMP/E.



## Download Maintenance

Download SMP/E maintenance from CA Support online.

## SMP/E RECEIVE and APPLY

SMP/E receive and apply the downloaded maintenance into SMP/E target paths */root/C7C4950/C7C4HFS/* and */root/C7C4950/C7C4JAR/*, using standard SMP/E batch JCL.

**Note:** This step does not alter the deployed run-time path */root/C7C4950/Cross-Enterprise\_APM/*.



# Chapter 6: Starting Your Product

---

This section describes what you need to do to start CA Cross-Enterprise APM.

This section contains the following topics:

[How to Deploy Without CA CSM](#) (see page 67)

[Configure the Cross-Enterprise APM Agent](#) (see page 72)

[Start the Cross-Enterprise APM Agent](#) (see page 84)

[Confirm the Connectivity](#) (see page 84)

[Stop the Cross-Enterprise APM Agent](#) (see page 85)

[Deploy an Updated Version of the Cross-Enterprise APM Agent](#) (see page 85)

**Note:** If you only want to integrate with CA NetMaster NM for TCP/IP, you do *not* have to perform these tasks.

## How to Deploy Without CA CSM

The topics in this section describe the manual tasks you perform if you are not deploying your product using CA CSM.

### Deploy the Cross-Enterprise APM Agent

After you have installed the extension using the method that you prefer, deploy it.

**Follow these steps:**

1. Using ISPF View, customize the sample batch JCL in member *smp.C7C4JCL(COPYSAMP)* as instructed in the sample JCL.

**Note:** Before you continue with the next step, be aware that your customized job *smp.C7C4JCL(COPYSAMP)* is not saved. Back it up if it is necessary.

2. Submit the batch job.

The job makes a copy of data set *smp.C7C4JCL* that you customize for your site.

This customized data set is named *custom.JCL*, using the high-level qualifier (*custom*) specified in the JCL. Additionally, the contents of SMP/E Target data set, *smp.C7C4JCL*, are copied into the customizable data set *custom.JCL*, which includes these members:

- COPYSAMP
- DEPLOY

- START
  - STDENV
  - STOP
  - WILYZOS
3. Customize the sample batch JCL member in *custom.JCL(DEPLOY)* as instructed in the sample JCL.
  4. Submit the batch job.

The job deploys (copies) the contents of your installed SMP/E target paths */root/C7C4950/C7C4HFS* and */root/C7C4950/C7C4JAR* into the run-time path */root/C7C4950/Cross-Enterprise\_APM/*.
  5. Customize the sample Cross-Enterprise APM startup JCL PROC in the *custom.JCL(WILYZOS)* member as instructed inside that JCL, specifying your */root/C7C4950 z/FS* file system mount point.
  6. Copy the member into a standard PROCLIB defined on your system, such as *SYS1.PROCLIB*.
  7. Edit these variables in *custom.JCL(STDENV)*:
    - Set the *SA\_INSTALL* variable to the actual Cross-Enterprise\_APM installation path.
    - Set the *SYSVIEWPATH* variable to the actual path of the CA SYSVIEW release-specific directory.
    - Set the *IRRACFPATH* variable to the actual path of the directory containing the *IRRacf.jar* file (PassTicket support).
    - Set the *JAVA\_HOME* variable to the installation path of the JRE.
    - Set the *LIBPATH* variable to include the directory containing the *libIRRacf.so* library (PassTicket support).
    - Set the *TZ="EST5EDT"* export the TZ environment variable which specifies the time zone.
  8. Save the member to apply the changes.

## Cross-Enterprise APM Files

The following list shows all the extracted files:

### **STDENV**

Is the shell script containing the main configuration variables for running the agent procedure.

**Location:** *custom.JCL*

### **WILYZOS**

Contains the job control language that starts and stops the agent.

**Location:** *custom.JCL*

### **WILYZOS.sh**

Is the script used to start or stop the agent.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/*

**Note:** This shell script is necessary only if you run the agent from USS. We recommend that you run the agent from the JCL.

### **Cross-Enterprise\_APM\_Dynamic.properties**

Configures CA Cross-Enterprise APM properties.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/config*

### **Introscope\_Cross-Enterprise\_APM.profile**

Specifies CA Introscope information. This agent configuration file provides all the required properties to connect and communicate to Enterprise Manager.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/config*

**Cross-Enterprise\_APMMetrics.xml**

(Internal use only) Is the configuration file that includes the list of metrics to be collected from CA SYSVIEW and the commands to get them.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/data*

**EULA.txt**

Contains the End User License Agreement that you read and agree to.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/data*

**EULAInstructions.txt**

Contains the instructions that are printed to the log when the product is started but the EULA has not yet been accepted. The instructions tell how to accept the EULA.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/data*

**InsightMetrics.xml**

(Internal use only) Includes the list of metrics to be collected from CA Insight DPM and the queries that are used to retrieve them.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/data*

**IntroscopeCAPIConfig.xml**

(Internal use only) Is a required agent file.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/data*

**SMFRecords255C27.conf**

(Internal use only) Is the SMF Records Definition file.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/data*

**SMFSend255C27.reqs**

(Internal use only) Is the SMF Send Metrics Requests file.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/data*

**XnetErrors.xml**

(Internal use only) Is the configuration file that defines actions to take in response to error conditions.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/data*

**com.wily.introscope.ext.sysview.agent\_<version>.jar**

Contains the CA Introscope agent plug-in for CA SYSVIEW.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/ext*

**Agent.jar**

Contains required library files.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/lib*

**AgentShim.jar**

Contains required library files.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/lib*

**castor-1.0.4.jar**

Contains required library files.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/lib*

**commons-logging-1.0.4.jar**

Contains required library files.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/lib*

**Cross-Enterprise\_APM.jar**

Contains required library files.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/lib*

**log4j-1.2.14.jar**

Contains required library files.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/lib*

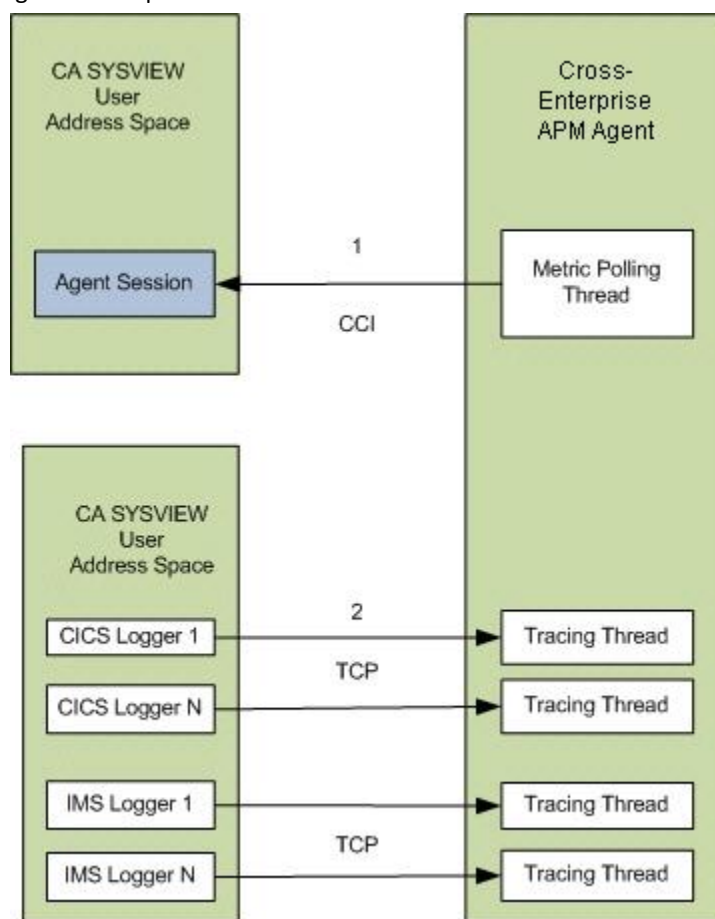
**Cross-Enterprise\_APM.log**

Is the log file.

**Location:** */root/C7C4950/Cross-Enterprise\_APM/logs*

## Configure the Cross-Enterprise APM Agent

This diagram provides a high-level overview of the Cross-Enterprise APM Agent configuration steps.



### Before you begin

Before you begin configuring the Cross-Enterprise APM Agent, verify that you have [Set Up CAICCI for CA Cross-Enterprise APM](#) (see page 25).

### Follow these steps:

1. Collect the metrics from CA SYSVIEW by configuring the Cross-Enterprise APM Agent. Establish a session with the CA SYSVIEW user address space by setting these configurations:
  - a. Configure the SYSVIEWPATH statement in *custom.JCL(STDENV)*. Point the statement to the zFS directory that is created during the CA SYSVIEW SMP/E process, for example:

```
SYSVIEWPATH=/usr/lpp/sysview/cnm4d70
```



**Note:** Your directory varies according to the CA SYSVIEW release. Verify that the file being referenced in STDENV resides at the path you provide here.

- b. Configure the Cross-Enterprise\_APM\_Dynamic.properties file:

```
SYSVIEW.connection.jobname=
```

**Note:** The jobname parameter is not required because the agent discovers the CA SYSVIEW user address space running on the same system. This parameter is required only if you run multiple copies of CA SYSVIEW and multiple user address spaces.

**Note:** For more information about setting the Cross-Enterprise\_APM\_Dynamic.properties configurations, see [Configure the Cross-Enterprise APM Dynamic.properties File](#) (see page 76).

2. Configure CA SYSVIEW to send the trace information to Cross-Enterprise APM.
  - a. Establish a TCP listener to which the CA SYSVIEW CICS and IMS loggers connect. The configuration is set by editing this property in the Introscope\_Cross-Enterprise\_APM.profile file:

```
ppz.smf.socket.port=15029
```

- b. Connect the CICS logger and IMS logger tasks in the CA SYSVIEW server to the Cross-Enterprise APM TCP listener on the specified port. Edit the following properties in the CA SYSVIEW data members:

```
sysvhlq.CNM4BPRM(CICSLOGR)
```

```
Wily-Introscope-PortList CICSWILY
```

```
sysvhlq.CNM4BPRM(GROUPS)
```

```
DEFINE CICSWILY
```

```
    TYPE    PORTLIST
```

```
    DESC    'Wily Agent Listener Port '
```

```
    MEMBERS 15029
```

```
sysvhlq.CNM4BPRM(IMSLOGR)
```

```
Wily-Introscope-PortList IMSWILY
```

```
sysvhlq.CNM4BPRM(GROUPS)
```

```
DEFINE IMSWILY
```

```
    TYPE    PORTLIST
```

```
    DESC    'Wily Agent Listener Port '
```

```
    MEMBERS 15029
```

**Note:** For more information about setting the Introscope\_Cross-Enterprise\_APM.profile configurations, see [Configure the Introscope Cross-Enterprise APM.profile File](#) (see page 81).

**Note:** After you configure these settings, read and accept the End User License Agreement. For more information, see [Configure and accept the End User License Agreement](#) (see page 74).

## Configure and Accept the End User License Agreement

Read and accept the end user license agreement.

**Important!** If you do not acknowledge the license agreement, error message WILY004E displays.

**Follow these steps:**

1. Open the EULA.txt file at `/root/C7C4950/Cross-Enterprise_APM/data`, and read the terms.
2. After you have agreed to the terms, open the `Cross-Enterprise_APM_Dynamic.properties` file at `/root/C7C4950/Cross-Enterprise_APM/config` and set the following property:  
  
`CA.Cross-Enterprise.APM.I.Read.And.Accept.End.User.License.Agreement = yes`
3. Save the file.

The accepted agreement is applied after the agent is restarted.

## Configure Network Topology and Firewall Settings

Open firewall ports between CA Cross-Enterprise APM and the Enterprise Manager to allow them to communicate. To allow the bi-direction communication between all appropriate Enterprise Managers and the Cross-Enterprise APM Agent, update the firewall in both directions.

In a clustered environment, an Enterprise Manager serves as a Manager of Managers (MOM), managing the other Enterprise Managers in the cluster (named Collectors). For load-balancing, the Introscope agents that connect to the MOM are redirected to a Collector with the lightest weight-adjusted load in the cluster. If an agent is disconnected later from the Collector, the agent reconnects to the MOM and can be assigned to a different Collector. In this MOM environment, configure the Cross-Enterprise APM Agent to connect directly to MOM or directly specify an Enterprise Manager.

### Follow these steps:

1. Open the `Introscope_Cross-Enterprise_APM.profile` file at `/root/C7C4950/Cross-Enterprise_APM/config`:
  - Edit the `introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=hostname` property to the server name or IP address of the Enterprise Manager (or MOM).
  - Edit the `introscope.agent.enterprisemanager.transport.tcp.port.DEFAULT=5001` property if you want to use an Enterprise Manager connection port other than the 5001 default port.

**Note:** If the Cross-Enterprise APM Agent connects to a MOM with load balancing, then the connection port to this MOM and all defined collectors must be opened. The Enterprise Manager connection port for the collector is defined in the `<agent-collector>` element of the `loadbalancing.xml` file on the MOM Enterprise Manager host. For more information about configuring load balancing, see the *CA APM Configuration and Administration Guide*. For more information about how to download this document, see the recommended reading.

2. Save the changes.

To apply a change, [start](#) (see page 84) or restart the Cross-Enterprise APM Agent.

## Configure the Cross-Enterprise\_APM\_Dynamic.properties File

The Cross-Enterprise\_APM\_Dynamic.properties file is the main configuration file, in that it allows you to specify these settings for CA Cross-Enterprise APM:

- Top worst performing transactions to retain
- Regular expression pattern to filter which CICS regions to monitor
- Regular expression pattern to filter which transaction groups to monitor
- Regular expression pattern to filter which queue managers to monitor
- Regular expression pattern to filter which queues to monitor
- Regular expression pattern to filter which IMS subsystems to monitor
- Regular expression pattern to filter which IMS transaction groups to monitor
- Regular expression pattern to filter which CA Datacom/DB address spaces to monitor
- Regular expression pattern to filter which TCP/IP stacks to monitor
- Option to turn off collection of z/OS metrics
- Option to turn off collection of CA SYSVIEW metrics
- The format of the URL for the transaction trace click-through feature
- The frequency for which static metrics are reported
- The metric update interval for retrieving CA SYSVIEW metrics
- The parameters that are required to connect to a specific CA SYSVIEW
- The configuration options to turn off z/OS metric collection or metric collection completely
- The configuration options to allow distinct collection intervals for each metric category

- The following configuration properties must be properly set to collect metrics from one or more CA Insight DPM instances running on the local system:

#### Insight.metrics.collect

Determines whether metrics are collected from any CA Insight DPM instance running on the local system.

- **no** indicates that DB2-specific metrics are not collected.
- **yes** indicates that the Cross-Enterprise APM Agent attempts to contact the configured XNET agent subtask of CA Insight DPM and retrieve DB2-specific metrics.

#### Insight.connection.port

Specifies the TCP/IP port that the local Xnet agent subtask of CA Insight DPM uses to listen for query requests. This Xnet agent subtask must be enabled and configured for the Cross-Enterprise APM Agent to collect DB2-specific metrics. The value corresponds to the PORT parameter for Xnet. CA APM uses this property with the Insight.connection.hostname property to connect to Xnet.

#### Insight.passticket.support

Determines whether to use PassTickets when sending authentication information to the Xnet agent subtask of CA Insight DPM. To use the PassTicket authentication, you require the following conditions:

- Your active z/OS security manager must be properly configured to allow for the PassTicket creation.
- The user account that is used to start the Cross-Enterprise APM Agent must have the proper permissions to create the PassTickets.
- The Xnet agent subtask must be configured to allow for the PassTicket authentication.

**Important!** When setting up PassTicket support for CA APM, be sure to complete the security product configuration and enable Xnet PassTicket support before setting this property to "yes". If Xnet PassTicket support is not enabled and CA APM generates a PassTicket, the connection request fails. After some number of failed attempts, the security product will suspend that user ID.

If this property is set to "yes", PassTickets are used for the authentication instead of user passwords. If this property is set to "no", specify a valid user password in the Insight.password configuration property.

#### Insight.passticket.appl

If the Insight.passticket.support property is set to "yes", use this property to specify the application name for the generation of PassTicket authentication tokens. The Xnet agent subtask of CA Insight DPM must be configured to use this application name by specifying the same value in the PASSNAME() configuration parameter.

### Insight.username

Specifies the user name sent to the Xnet agent subtask of CA Insight DPM for authentication. This property must always be specified, regardless of whether PassTicket support is enabled.

### Insight.password

Specifies the user password sent to the Xnet agent subtask of CA Insight DPM for authentication. If PassTicket support is not enabled, this property must be specified. If PassTicket support is enabled, this property is blank. For security reasons, always use the PassTicket authentication to avoid storing unencrypted passwords in the configuration file.

### Insight.DB2.subsystem.name.list

Specifies which local DB2 instances the Cross-Enterprise APM Agent monitors. A connection is established to each data collector instance of CA Insight DPM that is monitoring a DB2 subsystem in this comma-separated list. To collect metrics from all local CA Insight DPM data collector instances that are monitoring DB2 subsystems, specify the "\*" wildcard character for this value of this property.

- The remaining configuration properties in the `Cross-Enterprise_APM_Dynamic.properties` file that begin with the “Insight” prefix have default values that function properly for most installations.

The following “Insight” configuration properties influence the collection performance of metrics from local DB2 subsystems:

#### `Insight.DB2.subsystem.refresh.interval`

Specifies how often the Cross-Enterprise APM Agent performs the following tasks:

- Refresh the list of accessible DB2 subsystems.
- Submit status queries to each subsystem.

The default value is adequate for most situations, but this value can be changed if necessary.

**Default:** Half the value of the `Insight.update.interval` parameter

#### `Insight.DB2.subsystem.refresh.threads`

Specifies how many operating system threads are used to process the tasks that are defined to run during the DB2 subsystem refresh interval. If you want the DB2 subsystem refresh interval to execute more quickly, increase the value. The increased value allows multiple tasks to execute simultaneously (at the cost of increased CPU consumption during the refresh interval).

**Default:** 1, which means a single thread is used to issue status queries to each configured DB2 subsystem

#### `Insight.update.interval`

Specifies how often the Cross-Enterprise APM Agent retrieves updated metric values from each configured DB2 subsystem. The value can be increased, which decreases the rate configured DB2 subsystems have to process metric value queries.

**Default:** Value of the `SYSVIEW.update.interval` property

#### `Insight.update.threads`

Specifies how many operating system threads are used to process the metric value queries for each configured DB2 subsystem. If you want the metric update interval to execute more quickly, increase the value. The increased value allows multiple queries to execute simultaneously (at the cost of increased CPU consumption during the metric update interval).

**Default:** 1, which means the same thread is used to process sequentially each configured DB2 subsystem query

The properties file contains explicit detail, examples, and lists the configuration options available to help you determine what best suits your environment.

**Follow these steps:**

1. Open the `Cross-Enterprise_APM_Dynamic.properties` file, which is at `/root/C7C4950/Cross-Enterprise_APM/config`.
2. Edit and save the text file.

The changes will be applied after the agent picks them up dynamically.



## Configure the Introscope\_Cross-Enterprise\_APM.profile File

The *Introscope\_Cross-Enterprise\_APM.profile* file is where the agent configuration required to communicate to Enterprise Manager and CA SYSVIEW agent are made.

Introscope\_Cross-Enterprise\_APM.profile is a standard CA Introscope agent configuration file that provides all required properties to connect and communicate to Enterprise Manager. Any update in the file requires that you restart the Cross-Enterprise APM Agent.

The following properties identify the Enterprise Manager instance:

```
introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=em_hostname  
introscope.agent.enterprisemanager.transport.tcp.port.DEFAULT=em_port_number
```

In addition to other settings, you can set these CA SYSVIEW-related properties in this configuration file:

- Turn sampling on or off, and set the sampling interval.
- Set the buffer size for the socket receive in kilobytes.
- Disable or enable the ability to acquire metrics.
- *Specify the TCP/IP port so the SMF records can be obtained from CA SYSVIEW.*
- Set the agent antiflood threshold, which specifies the number of traces that are sent to Enterprise Manager by the Cross-Enterprise APM Agent.
- Specify the amount of detail that is logged and the output location.
- *If there are multiple IP stacks with different security permissions, specify the specific IP stack to bind the agent to.*

The properties file contains explicit detail, examples, and lists the configuration options available to help you when configuring settings for your environment.

### Follow these steps:

1. Open the *Introscope\_Cross-Enterprise\_APM.profile* file, which is at `/root/C7C4950/Cross-Enterprise_APM/config`.
2. Edit and save the text file.

## Configure Transaction Sampling

Transaction sampling enables CA Introscope agents to take a transaction trace occasionally without having an explicit transaction trace session running. The sampling does not apply any filtering and wakes up on a timer to take the sample. The samples are visible from the Workstation.

**Important!** The sampled traces are only visible from the Workstation Investigator metric tree traces tab. The traces do not show in the Transaction Trace Viewer of a transaction trace session.

Trace samples that are taken from a front-end agent automatically attempt to generate correlated cross-process back-end transaction traces. These back-end traces that correlate with front-end samples have the trace type, Normal. When running a transaction trace session, the high volume of back-end transaction trace sessions can hit the antiflood limit. The front-end samples may not have correlated traces. When the antiflood limit is hit, the worst performing (by duration) transaction traces get preferential delivery. Therefore, if a back-end transaction trace is missing during a high volume period, it is not likely to be the source of a problem.

The Cross-Enterprise APM Agent can be configured to take independent transaction samples that originated at front-end applications that a Cross-Enterprise APM tracer monitors using a communication method into CICS or IMS (the back ends). Samples generated directly from the agent do not always have correlated front-end traces because they are taken at random intervals independent of the front-end samples.

**Follow these steps:**

1. Configure each front-end agent making the following edits to the IntroscopeAgent.profile file in the <Agent\_Home>\core\config directory. This configuration controls the front-end sampling and the generation of correlated back-end traces that go with them.

**introscope.agent.transactiontracer.sampling.enabled**

Enables or disables the transaction sampling. If this parameter is set to false, the other parameters are ignored.

**Default:** true

**introscope.agent.transactiontracer.sampling.interval.seconds**

Specifies when the transaction sample is captured.

**Default:** 120 seconds

**Limits:** 1 second through 300 seconds (5 minutes)

**introscope.agent.transactiontracer.sampling.perinterval.count**

Specifies the number of samples that are captured in a transaction sampling interval.

**Default:** 15

**Limits:** 1 through 1000

2. Configure the Cross-Enterprise APM Agent by opening the Introscope\_Cross-Enterprise\_APM.profile file, at /root/C7C4950/Cross-Enterprise\_APM/config. This configuration generates back-end samples independent of any front-end samples being taken. These samples are the only back-end samples that are labeled as the trace type, Sampled.

**introscope.sysview.agent.transactiontracer.sampling.enabled**

Enables or disables the transaction sampling. If this parameter is set to false, the other parameters are ignored.

**Default:** true

**introscope.sysview.agent.transactiontracer.sampling.interval.seconds**

Specifies when the transaction sample is captured.

**Default:** 120 seconds

**Limits:** 1 second up to 300 seconds (5 minutes)

**introscope.sysview.agent.transactiontracer.sampling.perinterval.count**

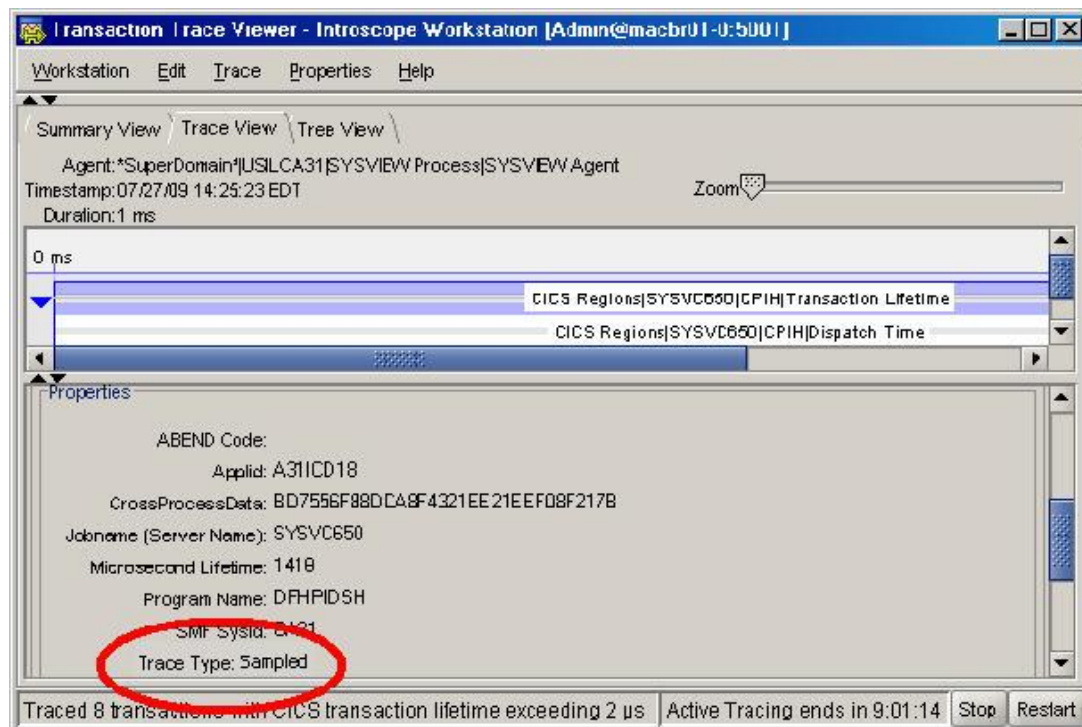
Specifies the number of samples that are captured in a transaction sampling interval.

**Limits:** 1 to 1000

**Default:** 15

After you start or restart the Cross-Enterprise APM Agent, the new settings are applied.

Any transaction trace types that you receive have *Sampled* in the Trace Type:



## Start the Cross-Enterprise APM Agent

Issue the following MVS operator command to start the Cross-Enterprise APM Agent:

```
MVS S WILYZOS
```

or

```
MVS S WILYZOS,ACTION=START
```

## Confirm the Connectivity

Verify the connection between the Cross-Enterprise APM Agent and the Enterprise Manager hosts in both directions by using the *ping* command.

## Stop the Cross-Enterprise APM Agent

To stop the Cross-Enterprise APM Agent, issue *one* of the following MVS operator commands:

- MVS S WILYZOS,ACTION=STOP
- MVS P WILYZOS

## Deploy an Updated Version of the Cross-Enterprise APM Agent

While SMP/E is used to install the extension, deployment is required to create the executable runtime path. Likewise, SMP/E is used to maintain or update the agent, deployment is required to update the executable runtime path. If you update the agent, deploy it using the steps in this topic.

### Follow these steps:

1. Shut down CA Cross-Enterprise APM Agent by issuing the following MVS operator command:

```
MVS P WILYZOS
```

2. Submit the *custom.JCL(DEPLOY)* batch job.

The job deploys or copies the contents of your installed SMP/E target paths */root/C7C4950/C7C4HFS* and */root/C7C4950/C7C4JAR* into the runtime path */root/C7C4950/Cross-Enterprise\_APM/*.

3. Restart CA Cross-Enterprise APM Agent by issuing the following MVS operator command:

```
MVS S WILYZOS
```

**Note:** After initial deployment, subsequent executions of the *custom.JCL(DEPLOY)* job to deploy any maintenance does not alter the */root/C7C4950/Cross-Enterprise\_APM/config* runtime path. The path contains configurable files that you have customized. If these files require maintenance, that maintenance contains *HOLDDATA*. The *HOLDDATA* instructs you on how to update these files manually to deploy that maintenance.

## SMP/E ACCEPT

You can permanently SMP/E accept the maintenance that has been applied.

**Important!** The accepted maintenance cannot be undone.

If the deployed maintenance is good, accept the applied maintenance into the SMP/E Distribution libraries *smp.ASYWHFS* and *smp.ASYWJAR*, using either CA CSM or batch JCL.

## SMP/E RESTORE

You can reject the maintenance that has been applied but not accepted, using SMP/E RESTORE.

If the deployed maintenance is bad, restore the SMP/E Target paths */root/C7C4950/C7C4HFS* and */root/C7C4950/C7C4JAR*, using either CA CSM or batch JCL.

You then [deploy \(copy\) the restored Target paths](#) (see page 85) */root/C7C4950/C7C4HFS* and */root/C7C4950/C7C4JAR* into the runtime path */root/C7C4950/Cross-Enterprise\_APM/*.

# Chapter 7: Integrating CA SYSVIEW and CA Insight DPM With CA APM

---

This section contains the following topics:

[How You Integrate CA SYSVIEW and CA Insight DPM With CA APM](#) (see page 87)

## How You Integrate CA SYSVIEW and CA Insight DPM With CA APM

As an application administrator, you want CA APM to see performance data from CA SYSVIEW and CA Insight DPM. You have already installed the products and CA Cross-Enterprise APM in your environment. To enable the visibility, you configure the integration between the products.

**Follow these steps:**

1. [Verify that your environment is prepared, and that all preparing for integration tasks and requirements have been met](#) (see page 87).
2. [Install and enable the Enterprise Manager components](#) (see page 88).
3. [Install and enable the Java agent components](#) (see page 90).
4. (Optional) [Install the MQ Tracer](#) (see page 97) on the front-end Java application.
5. [Verify the installation](#) (see page 98).

## Preparing for Integration Procedure

Before you perform the integration, familiarize yourself with the various installers.

**Note:** For more information about Enterprise Manager and Workstation installers, see the *CA APM Installation and Upgrade Guide*. For more information about the Java agent installer, see the *CA APM Java Agent Implementation Guide*.

**More information:**

[Additional Prerequisites](#) (see page 26)

[Configure Network Topology and Firewall Settings](#) (see page 75)

## Install and Enable the Enterprise Manager Components

While you install Enterprise Manager, the installation panel, Select Monitoring Options displays a full set of monitoring options that you can select and enable. To enable and install the required components, select the CA Cross-Enterprise Application Performance Management option.

For the installation instruction for CE APM Enterprise Manager, see the *CA APM Introscope Manager* documentation.

Perform the following steps to enable the CA Cross-Enterprise APM monitoring option subsequent to the initial installation of Enterprise Manager.

### Follow these steps:

1. Copy the contents from the `<EM_Home>\examples\Cross-Enterprise_APM` directory to the respective directories within the `<EM_Home>` directory.
2. Verify that the files are in the following directories:

```
<EM_Home>\config\modules\Cross-Enterprise_APM_SYSVIEW_Management_Module.jar
<EM_Home>\config\modules\Cross-Enterprise_APM_DB2zOS_Management_Module.jar
<EM_Home>\config\modules\NetMasterAgent_Management_Module.jar
<EM_Home>\ext\ddtv\Cross-Enterprise_APM_SYSVIEW.typeviewers.xml
<EM_Home>\ext\ddtv\Cross-Enterprise_APM_SYSVIEWMQObjects-typeviews.xml
<EM_Home>\ext\ddtv\NetMasterAgent_typeviewers.xml
<EM_Home>\product\enterprisemanager\features\com.wily.introscope.ext.sysview.
em.extensions.feature_<version>\feature.xml
<EM_Home>\product\enterprisemanager\plugins\
com.wily.introscope.ext.sysview.common_<version>.jar
<EM_Home>\product\enterprisemanager\plugins\
com.wily.introscope.ext.sysview.em_<version>.jar
<EM_Home>\scripts\Cross-Enterprise_APM_SYSVIEW.js
<EM_Home>\scripts\Cross-Enterprise_APM_Insight.js
<EM_Home>\scripts\Cross-Enterprise_APM_SYSVIEWMQQueueManagerAggregation.js
<EM_Home>\scripts\Cross-Enterprise_APM_SYSVIEWMQQueuesAggregation.js
<EM_Home>\ws-plugins\com.wily.introscope.ext.sysview.common.nll_<version>.jar
<EM_Home>\ws-plugins\com.wily.introscope.ext.sysview.common_<version>.jar
<EM_Home>\ws-plugins\
com.wily.introscope.ext.sysview.workstation_<version>.jar
<EM_Home>\ws-plugins\features\
com.wily.introscope.ext.sysview.workstation.extensions.feature_<version>\
feature.xml
```

3. Restart the Introscope Enterprise Manager.



## Enterprise Manager Component Files

The following table lists all the Enterprise Manager component files for the Cross-Enterprise APM.

File	Directory structure	Description
Cross-Enterprise_APM_SYSVIEW_Management_Module.jar	\config\modules	Management modules and dashboards
Cross-Enterprise_APM_DB2zOS_Management_Module.jar	\config\modules	Management modules and dashboards
Cross-Enterprise_APM_SYSVIEW.typeviewers.xml	\ext\ddtv	Tab views that appear in the CA Introscope Workstation
Cross-Enterprise_APM_SYSVIEW MQObjects-typeviews.xml	\ext\ddtv	Tab views that appear in the CA Introscope Workstation
Cross-Enterprise_APM_SYSVIEW.js	\scripts	JavaScripts for calculated metrics
Cross-Enterprise_APM_Insight.js	\scripts	<i>JavaScripts for calculated metrics</i>
Cross-Enterprise_APM_SYSVIEW MQQueueManagerAggregation.js	\scripts	JavaScripts for calculated metrics
Cross-Enterprise_APM_SYSVIEW MQQueuesAggregation.js	\scripts	JavaScripts for calculated metrics
feature.xml	\product\enterprisemanager\features\com.wily.introscope.ext.sysview.em.extensions.feature_<version>	CA EEM plug-ins for the tracer filter
com.wily.introscope.ext.sysview.common_<version>.jar	\product\enterprisemanager\plugins	Enterprise Manager plug-ins for the tracer filter
com.wily.introscope.ext.sysview.em_<version>.jar	\product\enterprisemanager\plugins	Enterprise Manager plug-ins for the tracer filter
feature.xml	\ws-plugins\features\com.wily.introscope.ext.sysview.workstation.extensions.feature_<version>	Workstation plug-ins for tracer filter
com.wily.introscope.ext.sysview.common.nl1_<version>.jar	\ws-plugins	Workstation plug-ins for tracer filter
com.wily.introscope.ext.sysview.common_<version>.jar	\ws-plugins	Workstation plug-ins for tracer filter

File	Directory structure	Description
com.wily.introscope.ext.sysview. workstation_<version>.jar	\ws-plugins	Workstation plug-ins for tracer filter

## Uninstall CE APM Components from Enterprise Manager

To uninstall CE APM components from Enterprise Manager, the following steps are necessary.

**Note:** For additional information refer to the *CA APM Installation Guide*.

**Follow these steps:**

1. Stop the Enterprise Manager if it is running.
2. Remove all the CA Cross-Enterprise APM-related files from the <EM\_Home> directory which are listed under Enterprise Manager Component Files.

## Install and Enable CA APM Java Agent Components

The following steps are necessary to install CA APM Java Agent files.

**Follow these steps:**

1. If the CTG, http, and Webservices tracers are not selected at installation time, copy the jar files from <Agent\_Home>\wily\examples\Cross-Enterprise\_APM\ext to <Agent\_Home>\wily\core\ext.
2. Select and run the Java agent installer for your environment.

**Note:** For more information, see the *CA APM Java Agent Implementation Guide*.

After you run the installer, verify that these files are in the following directories:

- <Agent\_Home>\wily\examples\Cross-Enterprise\_APM\ext\com.wily.introscope.ext.sysview.agent\_<version>.jar
- <Agent\_Home>\wily\examples\Cross-Enterprise\_APM\ext\ctg-tracer.jar
- <Agent\_Home>\wily\examples\Cross-Enterprise\_APM\ext\WS-SYSVIEW-Tracer.jar
- <Agent\_Home>\wily\examples\Cross-Enterprise\_APM\ext\http-tracer.jar

3. Enable the CTG CA SYSVIEW tracer:
  - a. Copy the `ext\com.wily.introscope.ext.sysview.agent_<version>.jar` and `ext\ctg-tracer.jar` files from the `<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext` directory to the existing `<Agent_Home>\wily\core\ext` directory of the Introscope agent.
  - b. Verify that the `ctg-tracer.jar` and `com.wily.introscope.ext.sysview.agent_<version>.jar` files are located in the `<Agent_Home>\wily\core\ext` directory.
  - c. Verify that the `CTG_ECI_Tracer_For_Sysview.pbd` file is in the `<Agent_Home>\wily\core\config` directory. Make the following edits to the `IntroscopeAgent.profile` file in the `<Agent_Home>\wily\core\config` directory:
    - Append `CTG_ECI_Tracer_For_Sysview.pbd` to the `introscope.autoprobe.directives` property.  
  
For example:  
  
`introscope.autoprobe.directivesFile=CTG_ECI_Tracer_For_Sysview.pbd,hot  
deploy.`
    - Edit `<EM hostname>` to point to the Enterprise Manager computer.  
  
For example:  
  
`introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=<EM  
hostname>.`
  - d. Add the `ctgclient.jar` file to the classpath. For example, `"C:\Program Files\IBM\CICS Transaction Gateway\classes\ctgclient.jar;"`. This path must be the same location that the monitored CTG client application uses.
  - e. Configure the CTG CA SYSVIEW Agent:  
  
Copy the contents of the configuration template file `Cross-Enterprise_APM_CTG_Config_Template.profile` in the `<Agent_Home>\wily\core\config` directory into the `IntroscopeAgent.profile` file in the `<Agent_Home>\wily\core\config` directory. The template contains directions on how to use these additional configuration options. The options allow you to specify whether your installation supports CTG channels, and the transactions to be traced by matching on the program.
  - f. Restart the CTG-based client application that the Java agent monitors. The client application can itself be an application server.

4. Enable the web services CA SYSVIEW tracer:
  - a. Install the SOA Performance Management tracer in `<Agent_Home>\wily\examples\SOAPerformanceManagement` by copying all files in the `ext` directory to the `<Agent_Home>\wily\core\ext` directory.  
**Note:** For more information, see the *CA APM for SOA Implementation Guide*.
  - b. Copy the `ext\com.wily.introscope.ext.sysview.agent_<version>.jar` and `ext\WS-SYSVIEW-Tracer.jar` files from the `<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext` directory to the existing `<Agent_Home>\wily\core\ext` directory of the Introscope agent.
  - c. Verify that the `WS-SYSVIEW-Tracer.jar` and `com.wily.introscope.ext.sysview.agent_<version>.jar` files are in the `<Agent_Home>\wily\core\ext` directory.
  - d. Verify that the `WS_Tracer_For_SYSVIEW.pbd` file is in the `<Agent_Home>\wily\core\config` directory.
  - e. Make the following edits to the `IntroscopeAgent.profile` file in the `<Agent_Home>\wily\core\config` directory:
    - Append `WS_Tracer_For_SYSVIEW.pbd` to the `introscope.autoprobe.directives` property.  
For example:  
`introscope.autoprobe.directivesFile=websphere-typical.pbl, hotdeploy, spm.pbl, WS_Tracer_For_SYSVIEW.pbd`
    - Edit `<EM hostname>` to point to the Enterprise Manager computer.  
For example:  
`introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=<EM hostname>`
  - f. Restart the web services client application that the Java agent monitors. The client application can itself be an application server.
5. Enable the HTTP CA SYSVIEW tracer:
  - a. Copy the `ext\com.wily.introscope.ext.sysview.agent_<version>.jar` and `ext\http-tracer.jar` files from the `<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext` directory to the existing `<Agent_Home>\wily\core\ext` directory of the Introscope agent.
  - b. Verify that the `http-tracer.jar` and `com.wily.introscope.ext.sysview.agent_<version>.jar` files are in the `<Agent_Home>\wily\core\ext` directory.
  - c. Verify that the `HTTP_Tracer_For_SYSVIEW.pbd` file is in the `<Agent_Home>\wily\core\config` directory.

- d. Make the following edits to the IntroscopeAgent.profile file in the <Agent\_Home>\wily\core\config directory:
  - Append HTTP\_Tracer\_For\_SYSVIEW.pbd to the introscope.autoprobe.directives property.  
For example:  
introscope.autoprobe.directivesFile=websphere-typical.pbl, hotdeploy, spm.pbl, HTTP\_Tracer\_For\_SYSVIEW.pbd
  - Edit <EM hostname> to point to the Enterprise Manager computer.  
For example:  
introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=<EM hostname>
- e. Restart the web services client application that the Java agent monitors. The client application can itself be an application server.

## Java Agent Component Files

The following table lists all the Java agent component files for the Cross-Enterprise APM.

File	Directory Structure	Description
<i>WS_Tracer_For_SYSVIEW.pbd</i>	<Agent_Home>\wily\core\config	Required .PBD file for web services SYSVIEW tracer.
<i>WS_Tracer_For_SYSVIEW-legacy.pbd</i>	<Agent_Home>\wily\example\legacy	Required .PBD file for web services SYSVIEW tracer. Uses legacy version agent. Copy this file to <Agent_Home>\wily\core\config and use it instead of <i>WS_Tracer_For_SYSVIEW.pbd</i> if you want to run in legacy mode.
<i>WS-SYSVIEW-Tracer.jar</i>	<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext	Required .JAR file.
<i>CTG_ECI_Tracer_For_SYSVIEW.pbd</i>	<Agent_Home>\wily\core\config	Required .PBD file for CTGtracer. Uses lean agent.
<i>CTG_ECI_Tracer_For_SYSVIEW-legacy.pbd</i>	<Agent_Home>\wily\examples\legacy	Required .PBD file for CTGtracer. Uses legacy version agent. Copy this file to <Agent_Home>\wily\core\config and use it instead of <i>CTG_ECI_Tracer_For_SYSVIEW.pbd</i> if you want to run in legacy mode.
<i>ctg-tracer.jar</i>	<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext	Required .JAR file.

File	Directory Structure	Description
HTTP_Tracer_For_SYSVIEW.pbd	<Agent_Home>\wily\core\config	Required .PBD file for http-tracer. Uses lean agent.
HTTP_Tracer_For_SYSVIEW-legacy.pbd	<Agent_Home>\wily\examples\legacy	Required .PBD file for http-tracer. Uses legacy version agent. Copy this file to <Agent_Home>\wily\core\config and use it instead of HTTP_Tracer_For_SYSVIEW.pbd if you want to run in legacy mode.
com.wily.introscope.ext.sysview.agent_<version>.jar	<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext	Required .JAR file.
http-tracer.jar	<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext	Required .JAR file.

## Running with Legacy Mode PBDS

You can run with legacy versions of the PBDS instead of the new mode versions that are already placed in the directory <Agent\_Home>\wily\core\config.

### Follow these steps:

1. Select and run the Java agent installer for your environment.

**Note:** For more information about legacy mode pbds, see the *CA APM Java Agent Implementation Guide*.

After you run the installer, verify that these files are in the following directories:

- <Agent\_Home>\wily\examples\legacy\CTG\_ECI\_Tracer\_For\_SYSVIEW-legacy.pbd
  - <Agent\_Home>\wily\examples\legacy\WS\_Tracer\_For\_SYSVIEW-legacy.pbd
2. Enable the legacy tracers:
    - a. Copy the CTG\_ECI\_Tracer\_For\_SYSVIEW-legacy.pbd and WS\_Tracer\_For\_SYSVIEW-legacy.pbd from the <Agent\_Home>\wily\examples\legacy directory to the existing <Agent\_Home>\wily\core\config directory of the Introscope agent.

- b. Make the following edits:
  - Append CTG\_ECI\_Tracer\_For\_Sysview-legacy.pbd to the introscope.autoprobe.directives property. For example:  
  
`introscope.autoprobe.directivesFile=CTG_ECI_Tracer_For_Sysview-legacy.pbd,hotdeploy.`
  - Edit `<EM hostname>` to point to the Enterprise Manager computer. For example:  
  
`introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=<EM hostname>.`
- c. Add the ctgclient.jar file to the classpath. For example, "C:\Program Files\IBM\CICS Transaction Gateway\classes\ctgclient.jar;". This path must be the same location that the monitored CTG client application uses.
- d. Configure the CTG CA SYSVIEW Agent:  
  
Copy the contents of the configuration template file Cross-Enterprise\_APM\_CTG\_Config\_Template.profile in the `<Agent_Home>\wily\core\config` directory into the IntroscopeAgent.profile file in the `<Agent_Home>\wily\core\config` directory. The template contains directions on how to use these additional configuration options. The options allow you to specify whether your installation supports CTG channels, and the transactions to be traced by matching on the program.
- e. Restart the CTG-based legacy client application that the Java agent monitors. The client application can itself be an application server.

3. Enable the web services CA SYSVIEW tracer:
  - a. Install the SOA Performance Management tracer in `<Agent_Home>\wily\examples\SOAPerformanceManagement` by copying all files in the `ext` directory to the `<Agent_Home>\wily\core\ext` directory.  
**Note:** For more information, see the *CA APM for SOA Implementation Guide*. Install the legacy version of the SOA tracer.
  - b. Copy the `ext\com.wily.introscope.ext.sysview.agent_<version>.jar` and `ext\WS-SYSVIEW-Tracer.jar` files from the `<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext` directory to the existing `<Agent_Home>\wily\core\ext` directory of the Introscope agent.
  - c. Verify that the `WS-SYSVIEW-Tracer.jar` and `com.wily.introscope.ext.sysview.agent_<version>.jar` files are in the `<Agent_Home>\wily\core\ext` directory.
  - d. Verify that the `WS_Tracer_For_SYSVIEW-legacy.pbd` file is in the `<Agent_Home>\wily\core\config` directory.
  - e. Make the following edits to the `IntroscopeAgent.profile` file in the `<Agent_Home>\wily\core\config` directory:
    - Append `WS_Tracer_For_SYSVIEW-legacy.pbd` to the `introscope.autoprobe.directives` property. For example:  
  
`introscope.autoprobe.directivesFile=websphere-typical.pbl, hotdeploy, spm.pbl, WS_Tracer_For_SYSVIEW-legacy.pbd`
    - Edit `<EM hostname>` to point to the Enterprise Manager computer. For example:  
  
`introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=<EM hostname>`
  - f. Restart the web services client application that the Java agent monitors. The client application can itself be an application server.
4. Enable the configuration templates by copying the `Cross-Enterprise_APM_CTG_Config_Template.profile` to the `IntroscopeAgent.profile`.



## Uninstall the Java Agent Component Files

If you choose to uninstall the Java agent component files, perform these steps.

**Follow these steps:**

1. Stop the agent.
2. Edit the *IntroscopeAgent.profile* file in the wily directory by removing these entries from the *introscope.autoprobe.directives* property.
  - *WS\_Tracer\_For\_SYSVIEW.pbd* (or the legacy version)
  - *CTG\_ECI\_Tracer\_For\_SYSVIEW.pbd* (or the legacy version)
  - *HTTP\_Tracer\_For\_SYSVIEW.pbd* (or the legacy version)
3. Remove any files copied from  
<Agent\_Home>\wily\examples\Cross-Enterprise\_APM that are in the  
<Agent\_Home>\wily\core\ext directory.
4. Restart the agent to apply the changes.

## Install the MQ Tracer (Optional)

This step is optional on the front-end Java application. Perform the following tasks only if your front-end application is invoking CICS transactions using MQ.

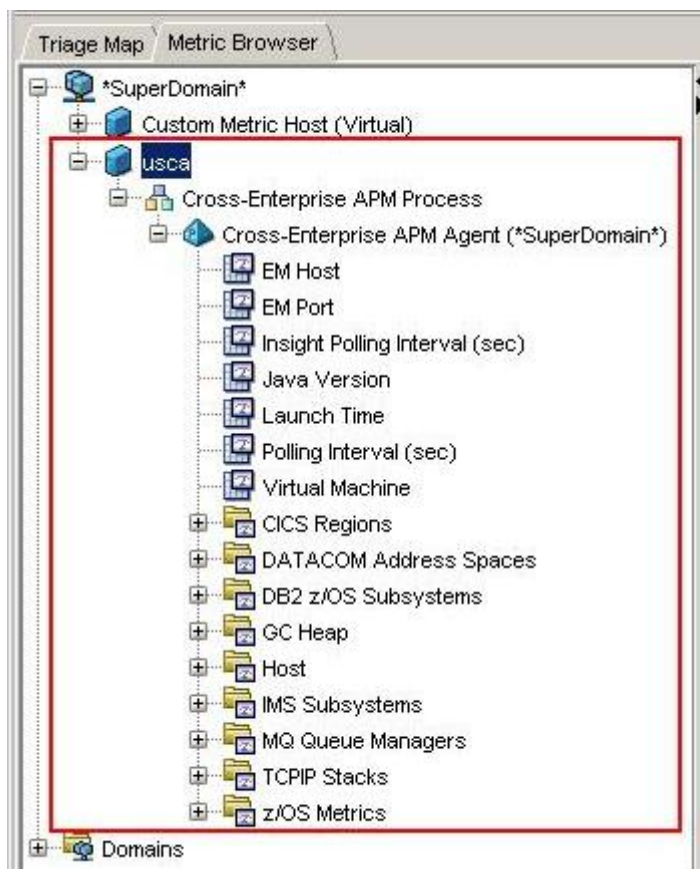
If you use MQ tracer, you have the following options:

- Install the MQPowerPack tracer only if you want to trace the MQ application on the frontend application server and CICS.
- Install all the MQPowerPack if you also want to trace message flow through MQ.

To install the MQ tracer, follow the instructions provided in the [CA APM for IBM WebSphere MQ documentation](#) (see page 109) for all MQ installation-related content.

## Verify the Installation

After CA Cross-Enterprise APM has been successfully installed, launch Introscope and go to the Investigator. You will see the host name of the z/OS machine and will see active metrics under the Cross-Enterprise APM node and backend CICS traces:



# Chapter 8: Integrate CA NetMaster NM for TCP/IP with CA Introscope

---

This section contains the following topics:

[How You Integrate CA NetMaster NM for TCP/IP with CA Introscope](#) (see page 99)

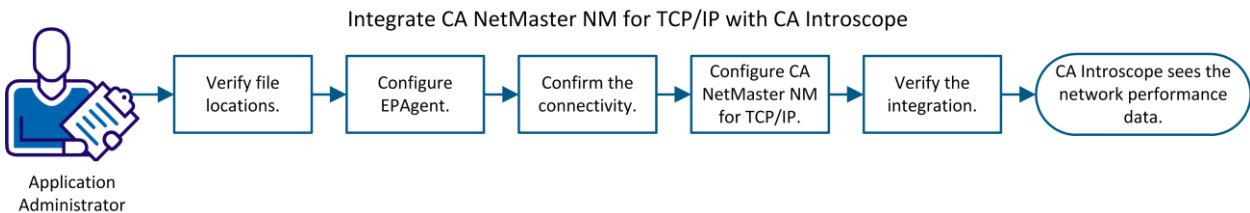
[Performance Monitoring Metrics](#) (see page 103)

[Specify the Performance Monitoring Metrics to Send](#) (see page 104)

## How You Integrate CA NetMaster NM for TCP/IP with CA Introscope

As an application administrator, you want CA Introscope to see CA NetMaster NM for TCP/IP performance data. You have both products that are already installed in your environment. To enable the visibility, you configure the integration between CA NetMaster NM for TCP/IP and CA Introscope.

The following illustration provides an overview of the process:



The process has the following tasks:

1. [Verify file locations](#) (see page 100).
2. [Configure EPAgent](#) (see page 100).
3. [Confirm the connectivity](#) (see page 101) between CA NetMaster NM for TCP/IP and EPAgent.
4. [Configure CA NetMaster NM for TCP/IP](#) (see page 102).
5. [Verify the integration](#) (see page 103).

At the end of the process, you can use the following facilities to work with the network performance data:

- Workstation Console or WebView to view dashboards of network metrics
- Workstation Investigator to examine network metrics
- Reporting on the data

## Verify File Locations

Two files contain CA NetMaster NM for TCP/IP dashboards, typeviews, and report templates. During the installation of Enterprise Manager, if you have selected the CA Cross-Enterprise Application Performance Management option, the installation process puts these files in the correct locations.

Verify that the following files are in the indicated directory:

- `<EM_Home>\config\modules\NetMasterAgent_Management_Module.jar`
- `<EM_Home>\ext\ddtv\NetMasterAgent.typeviewers.xml`

If the files are not there, copy them from the `<EM_Home>\examples\Cross-Enterprise_APM\` directory. Then, restart Enterprise Manager.

## Configure EPAgent

You customize the EPAgent properties file. If you want to connect more than two CA NetMaster NM for TCP/IP regions, you require a dummy plug-in file.

**Follow these steps:**

1. Customize the `<EPAgent_Home>/epagent/IntroscopeEPAgent.properties` file:
  - a. Verify that the following line is uncommented:  
`introscope.epagent.config.networkDataPort=8000`
  - b. Record this Network Data Port number.
  - c. Specify Mainframe for the `introscope.agent.customProcessName` property:  
`introscope.agent.customProcessName=Mainframe`
  - d. Specify NetMasterAgent for the `introscope.agent.agentName` property:  
`introscope.agent.agentName=NetMasterAgent`

- e. (Optional) If you want to connect more than two CA NetMaster NM for TCP/IP regions, add stateless plug-ins.

For example, the following lines cater for three regions:

```
introscope.epagent.plugins.stateless.names=Z0S1,Z0S2,Z0S3
introscope.epagent.stateless.Z0S1.command=<EPAgent_Home>/epagent/epaplugin/dummy_file
introscope.epagent.stateless.Z0S1.delayInSeconds=86400
introscope.epagent.stateless.Z0S2.command=<EPAgent_Home>/epagent/epaplugin/dummy_file
introscope.epagent.stateless.Z0S2.delayInSeconds=86400
introscope.epagent.stateless.Z0S3.command=<EPAgent_Home>/epagent/epaplugin/dummy_file
introscope.epagent.stateless.Z0S3.delayInSeconds=86400
```

*dummy\_file* identifies the dummy plug-in file that you create in the next step. The file has the following name:

- (Linux) *name.scr*
- (Windows) *name.bat*

- f. Save the customized file.

2. (Optional) If you want to connect more than two CA NetMaster NM for TCP/IP regions, create a dummy plug-in file.

- (Linux) In the <EPAgent\_Home>/epagent/epaplugins/ directory, create a .scr file with a single comment line:

```
# This is a dummy EPA plug-in file
```

- (Windows) In the <EPAgent\_Home>/epagent/epaplugins/ directory, create a .bat file with a single comment line:

```
:: This is a dummy EPA plug-in file
```

3. Start EPAgent.

CA Introscope is ready to accept data from CA NetMaster NM for TCP/IP.

## Confirm the Connectivity

Confirm the connectivity between the CA NetMaster NM for TCP/IP region and EPAgent. If firewalls exist, these firewalls must permit TCP/IP traffic between an ephemeral port on the z/OS IP host for the region and EPAgent Network Data Port (default 8000).

### Follow these steps:

1. Log on to the region.
2. Enter **CMD** at the Command prompt.

The Command Entry panel appears.

3. Enter the following command to ping the IP address of EPAgent:

```
PING em_ip_address
```

4. Review the response to verify that the region can reach EPAgent.

**Important!** If the test fails, reconfigure your firewalls to permit connectivity.

## Configure CA NetMaster NM for TCP/IP

You configure CA NetMaster NM for TCP/IP to enable the region to feed performance data to CA Introscope.

### Follow these steps:

1. Verify that the TESTEXEC(RUNSYSIN) member for the region contains the following parameter:

```
PPREF= 'PROD=APM'
```

**Important!** If you update the member, restart both the region and the associated SOLVE Subsystem Interface (SSI).

2. Log on to the region.
3. Enter **/PARMS** at the Command prompt.

A list of parameter groups appears.

4. Enter **F APMEPAGENT**.

The command finds the parameter group that enables the data feed.

5. Enter **B** next to the parameter group.
6. Verify that the following fields have the indicated values:

```
.- APMEPAGENT - CA Introscope EPAgent -----  
| CA Introscope Environment Performance Agent:  |  
| Enable EPAgent Client? ..... YES  (Yes or No) |  
| IP Addr/Host Name ... epa_ip_address          |  
| EPAgent Network Data Port ..... 8000          |  
|-----|
```

***epa\_ip\_address***

Identifies the IP address or host name of EPAgent.

**Note:** If an update is required, press the F4 (Update) function key. After your changes, press F6 (Action) to apply the changes effective immediately in the region, then press F3 (File) to save the changes.

The region is already feeding or starts to feed data to CA Introscope.

## Verify the Integration

The quickest way to verify a new metric feed is to open a Workstation Console and view the NetMaster dashboards. The first data points start to appear about 15 seconds after you apply the APMEPAGENT parameter group. (Some metrics, such as Top Applications, only appear after about 5 minutes.)

**Follow these steps:**

1. Start and log in to Workstation Console.
2. Select a NetMaster dashboard from the Dashboards drop-down list at the top.
3. Confirm that the dashboard shows network performance data.

CA NetMaster NM for TCP/IP is feeding data to CA Introscope, and you can use Workstation to work with the data.

## Performance Monitoring Metrics

After you familiarize yourself with the default metrics, you can consider sending the Performance Monitoring metrics.

A CA NetMaster NM for TCP/IP region monitors performance metrics for many physical and logical mainframe network resource types. The metric sample values come from various sources including IBM operating system functions, device management applications, packet flow analysis, and physical devices.

At regular fixed intervals from 5 through 60 minutes, the region takes samples of each monitored metric. Metric sample values are compared to thresholds, for alerting. The sample values are aggregated into hourly values, for baseline calculations and further reporting, but are not retained for long periods.

**Note:** For information about how to configure monitoring for an IP resource or node, see the *CA NetMaster Network Management for TCP/IP Implementation Guide*. For information about monitoring attributes, see the *CA NetMaster Network Management for TCP/IP Administration Guide*.

You can send these metrics to CA Introscope, for example:

- To retain individual sample values in specialized metric storage, for longer than the region can keep them

For example, you want to keep months of interface throughput rates at small intervals. You use this data for verification with their link provider.

- To create dashboards combining complementary mainframe metrics from different sources

For example, you want to combine stack network interface metrics with OSA or Cisco device performance metrics.

- To create dashboards for critical business services from CA NetMaster NM for TCP/IP, CA SYSVIEW, and CA Insight DPM metrics, with multiple service components visible on one place

## Specify the Performance Monitoring Metrics to Send

The Workstation Investigator lists the Performance Monitoring metrics under the IP Resources metric category. You can configure the CA NetMaster NM for TCP/IP region to send these metrics to CA Introscope.

**Note:** To configure the region to monitor a metric (or attribute), see the *CA NetMaster Network Management for TCP/IP Implementation Guide*.

### Follow these steps:

1. Log on to the region.
2. Identify the attributes that are monitored for an IP resource or node, and if applicable, qualifier name:
  - a. Enter /IPMON to access IP Resource Monitor or /IPNODE to access IP Node Monitor.
  - b. Find the IP resource or node, and enter **H** next to it.

A list of attributes appears.
  - c. Find the required attributes, and note down the following information, including any special characters:
    - Resource class
    - Resource name
    - Attribute name
    - Qualifier name

**Note:** Do *not* include attributes of the ENUM type. The region does *not* send this type of attributes to CA Introscope.

**Note:** To avoid metric explosions and other overheads, the region can send a maximum of 64 resource-qualifier-attribute combinations.



## 3. Specify the attributes:

- a. Enter **/PARMS** at the Command prompt.

A list of parameter groups appears.

- b. Enter **F APMEPAGENT**.

The command finds the parameter group that enables the data feed.

- c. Enter **U** next to the parameter group.

- d. Specify **YES** in the Performance Monitoring field.

- e. Press F8 (Forward).

A panel appears for you to specify the attributes you want to send.

- f. Specify the resource-qualifier-attribute combinations that you noted in Step 2c in the indicated syntax, for example:

```
ASMON(IKED TCPIP11V-UDP(500)) AsBytesInByPort
APPNHPR(APPNHPR) RTPsARBRed
CSM(CSM NET) DataSpaceTotalInUse
EE(EE USILDA01.NMDCIP2) EEBytesByCP
IPNODE(NMDCIP3 FastEthernet0/0) CiscoifOutPkts
CIP(NMDCIP3 192.168.82.232) CLAWReadBlks
OSA(OSA-00 TCPIP99-P4) PriorityQueueStatus
STACK(TCPIP31 172.24.*) ConActiveByNet
VIP(A DVIPA C031-TCPIP) ConConnectsByStack
```

**Note:** For more information, press F1 (Help).

- g. Press F4 (Save).

- h. Press F6 (Action).

Your changes become effective immediately. The current metric feed connection stops; then a new metric feed connection starts, including the Performance Monitoring metrics. You can see the values of these metrics at CA Introscope after the first sampling interval.



# Appendix A: Recommended Reading

---

To learn about the products you want to use, familiarize yourself with the following guides:

- [CA APM core documentation set](#) (see page 107)
- [CA SYSVIEW core documentation set](#) (see page 108)
- [CA Insight DPM for DB2 for z/OS core documentation set](#) (see page 109)
- [CA APM for IBM WebSphere MQ documentation](#) (see page 109)
- [CICS documentation](#) (see page 109)
- [CA NetMaster NM for TCP/IP core documentation set](#) (see page 110)

Review the *Compatibility Guide*. The comprehensive guide lists Java versions, JVM vendors, application servers, hardware, and software platforms supported. You can download the Compatibility Guide from the CA Support site.

## CA APM Core Documentation

You can access CA APM documentation in two ways:

- Download the documentation from the CA APM software download area on [CA Support](#).
- Access Help from within the Workstation. For more information, see the *CA APM Workstation User Guide*.

**Note:** On UNIX, the Help system is hard-coded to use the Mozilla browser. You must have Mozilla in your classpath for the links displayed in the top-level Help window to be functional.

For a comprehensive list of documents that belong to the CA APM core documentation set, see the *CA APM Overview Guide* or Product Documentation.

## CA SYSVIEW Core Documentation

You can access the CA SYSVIEW guides from [CA Technical Support site](#).

This table describes the guides included in the main CA Introscope documentation set.

***CA SYSVIEW Administration Guide***

Provides customization and usage information for the components, options, monitoring, interfaces, and utilities.

***CA SYSVIEW CA Vantage GMI (CA GMI) Guide***

Provides the user with an introduction to components, set up procedures for GMI, and concepts and procedures necessary to access and use CA SYSVIEW from the GMI Windows Client GUI.

***CA SYSVIEW Installation Guide***

Contains complete installation and starting information and provides an overview of the product and its components.

***CA SYSVIEW Release Notes***

Describes new and enhanced features and lists any features removed.

***CA SYSVIEW Security Guide***

Provides information about limiting command and subcommand usage, defining security groups, defining what is shown on displays, limiting access and resources.

***CA SYSVIEW User Guide***

Provides basic information so all users can get started using the product immediately. The guide provides an overview of the basic tasks performed using the resource displays.

***CA SYSVIEW Using the CA Explore Report Writer***

Provides procedures for using the history reporting commands and variables to create reports.

## CA Insight DPM for DB2 for z/OS Core Documentation

You can access the CA Insight DPM for DB2 for z/OS guides from the CA Technical Support site.

This table describes the relevant guides included in the main documentation set.

### **CA Database Management Solutions for DB2 for z/OS Installation Guide**

Provides the instructions on how to install and configure CA Insight DPM for DB2 for z/OS and required infrastructure components (such as Xmanager and Xnet).

### **CA Database Management Solutions for DB2 for z/OS General Facilities Reference Guide**

Provides more information about how to prepare the Xmanager and Xnet components for use.

### **CA Database Management Solutions for DB2 for z/OS Release Notes**

Provides information concerning the latest enhancements, known issues, and installation considerations for the CA Database Management Solutions for DB2 for z/OS.

### **CA Insight Database Performance Monitor for DB2 for z/OS User Guide**

Provides information about how to manage and use CA Insight Database Performance Management for DB2 for z/OS.

### **CA Insight Database Performance Monitor for DB2 for z/OS System Reference Guide**

Provides more information about CA Insight Database Performance Management for DB2 for z/OS, including installation verification steps and advanced configuration topics.

## CA APM for IBM WebSphere MQ Documentation

You can access the *CA APM for IBM WebSphere MQ Guide* from the [CA Technical Support site](#).

## CICS Documentation

For CICS-related information, view IBM documentation.

## CA NetMaster NM for TCP/IP Core Documentation

You can access the CA NetMaster NM for TCP/IP guides from the [CA Technical Support site](#).

# Index

---

## A

- about
  - extension • 13
- access
  - login • 42

## C

- CA CSM usage scenarios • 41
- CA NetMaster NM for TCP/IP
  - integrating • 99
- configuration files, about • 75
- configuring
  - Enterprise\_APM\_Dynamic.properties • 76
  - extension • 72
  - Introscope Cross-Enterprise APM.profile • 81
  - network topology and firewall settings • 75
  - STDENV • 72
  - transaction sampling • 82
- contacting technical support • 4
- Cross-Enterprise APM Agent
  - about • 13
  - additional prerequisites • 26
  - deploying • 67
  - directory structure • 69
  - maintaining • 64
  - pre-installation • 17
  - starting • 84
  - stopping • 85
- customer support, contacting • 4

## D

- deploying
  - extension • 67
  - updates • 85

## E

- Enterprise\_APM\_Dynamic.properties, configuring • 76
- extension, configuring • 72

## I

- installation
  - pre-installation • 17

- verifying • 98
- installing
  - Java application components • 90
  - MQ tracer • 97
  - security prerequisites • 20
- integration with CA NetMaster NM for TCP/IP • 99
- Introscope\_Cross-Enterprise\_APM.profile,
  - configuring • 81

## J

- Java application components, installing • 90

## M

- maintaining, extension • 64
- management module directory, directory structure • 89
- MQ tracer, installing • 97

## N

- network performance metrics
  - description • 103
  - sending • 104
- network topology and firewall settings, configuring • 75

## S

- security prerequisites, installing • 20
- SMP/E ACCEPT RESTORE, using • 86
- SMP/E ACCEPT, using • 86
- starting, extension • 84
- stopping, extension • 85
- support, contacting • 4

## T

- technical support, contacting • 4
- transaction sampling, configuring • See transaction sampling

## U

- understanding
  - Cross-Enterprise APM Agent directory structure • 69
  - management module directory structure • 89
- using

---

SMP/E ACCEPT • 86  
SMP/E ACCEPT RESTORE • 86

## V

verifying, installation • 98