

# EMC Smarts Service Assurance Manager Administrator

## Course Description



Course Number: SM-ES-CE-S-ADM200	
Method: ILT	Duration: 3 Days

### Course Overview

This hands-on course will empower you to administer the deployment of the InCharge Service Assurance Manager suite of solutions to fit the requirements of your organization. It provides an overview of EMC Smarts Technologies and the EMC Smarts Architecture and an in-depth explanation of the Administration Consoles. Advanced features and functions of EMC Smarts Service Assurance Manager are covered, including creating users, profiles, notification lists and tools to control the working environment for all Service Assurance Manager users and operators. You will also learn to how to use EMC Smarts Business Impact Manager to represent the managed infrastructure in the context of the business entities that it supports. Hands-on labs allow participants to install and configure EMC Smarts on a live network under the guidance of an expert instructor.

### You Will Learn How To:

- Define the flow of information between EMC Smarts components
- View and explore the results of the EMC Smarts diagnostic analysis
- Comprehend the network and service impacts caused by failures
- Customize the layout of the EMC Smarts console according to user preferences
- Maintain user logins and associated user profiles
- Automate actions to respond to failure notifications
- Incorporate customer and service info into SAM to manage infrastructure in the context of business
- Understand the use of hierarchical Service Assurance Manager servers

### Target Audience

System Administrators, System Engineers, Application Developers, and IT Managers.

### Prerequisites

None

### Course Content

#### EMC Smarts Overview

- EMC Smarts Technology
- EMC Smarts Architecture
- EMC Smarts Applications

#### Installation and Startup of EMC Smarts Products

- IP Availability Manager Installation
- Service Assurance Manager Installation
- EMC Smarts Command Line Utilities
- Registration and Use of EMC Smarts Services

#### Console Configuration

- Creating Users and User Profiles
- Specifying Notifications Associated with a User Profile

# EMC Smarts Service Assurance Manager Administrator

## Course Description



- Notification List
- Filter Criteria
- Column Headings
- Populating User Defined Fields
- Defining Tools
  - Types
  - Server-Side Tool Configuration and Program Parameters
  - Client-Side Tool Configuration and Program Parameters
- EMC Smarts Analysis Server Configuration
  - Adding and Deleting Underlying Servers
    - Domain Specification
    - Type Fields
  - Populating User Defined Fields
  - Tagging Topology Elements to Manage Overlapping IP Networks
  - Changing System Parameters
  - Specifying Information Imported into Service Assurance Manager
- Notification Adapters
  - Overview
  - Configuration
  - Activation
- Selective Groups
  - Types of Groups
  - Selective Groups
    - The Group Definition Console
    - Creating Selective Groups
  - Hierarchical Groups
    - Creating Group Import Files
    - Importing Groups
- EMC Smarts Business Impact Manager
  - Business Context
  - Impact Customizations
  - Customizing Impact Calculations
  - Business Object Model
  - Business Maps
- Escalation Policies
  - Policy Components
  - Policy Creation

# EMC Smarts Service Assurance Manager Administrator

## Course Description



### Hands-On Exercises

Throughout this course, hands-on exercises provide practical, extensive experience customizing and understanding the Service Assurance Manager Global Console. Exercises are performed under the guidance of an expert instructor, and include

Installing and Setting Up EMC Smarts Servers

Using EMC Smarts Command Line Utilities

Creating User Profiles

Modifying Notification Lists

Changing Column Headings

Populating User Defined Fields

Using Server-based Tools and Client-based Tools

Adding additional InCharge Analysis Servers

Implementing Notification Adapters

Customizing Impacts

Creating Selective Groups

Importing Customer Data, Services, and Hierarchical Groups into SAM

Defining Escalation Policies