



# COMPUTER ASSOCIATES (CA) APPLICATION PROGRAMMING INTERFACE (API) GATEWAY SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

## Version 1, Release 1

## 19 September 2016

## Developed by CA and DISA for the DoD

## Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

# TABLE OF CONTENTS

**Page**

**1. INTRODUCTION ..... 1**

1.1 Executive Summary ..... 1
1.2 Authority ..... 1
1.3 Vulnerability Severity Category Code Definitions ..... 1
1.4 STIG Distribution ..... 2
1.5 SRG Compliance Reporting ..... 2
1.6 Document Revisions ..... 2
1.7 Other Considerations ..... 2
1.8 Product Approval Disclaimer ..... 3

**2. ASSESSMENT CONSIDERATIONS ..... 4**

2.1 CA API Gateway Server Operating System Compliance ..... 4
2.2 CA API Gateway Server NDM STIG ..... 4
2.3 CA API Gateway Server ALG STIG ..... 4

**3. CONCEPTS AND TERMINOLOGY CONVENTIONS ..... 5**

3.1 Policy Manager ..... 5
3.1.1 CA API Gateway Policy ..... 5
3.1.2 Policy Assertions ..... 5

# LIST OF TABLES

**Page**

Table 1-1: Vulnerability Severity Category Code Definitions ..... 2

# 1. INTRODUCTION

## 1.1 Executive Summary

The Computer Associates (CA) Application Programming Interface (API) Gateway Security Technical Implementation Guides (STIGs) provide technical security policies, requirements, and implementation details for applying security concepts to a gateway combining policy management and central policy enforcement. The STIG has two components, one based on the Network Device Management (NDM) Security Requirements Guide (SRG) and the other based on the Application Layer Gateway (ALG) SRG.

The CA API Gateway enables an enterprise solution for backend data and applications integrating with existing Identity Access Management (IAM) solutions. The Gateway includes a built-in Public Key Infrastructure (PKI) engine, FIPS 140-2 level encryption, and Security Assertion Markup Language (SAML) support. The Gateway form factors within scope of this STIG are the network device and virtual appliance running on the Red Hat Enterprise Linux (RHEL) operating system.

## 1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

## 1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

**Table 1-1: Vulnerability Severity Category Code Definitions**

| | DISA Category Code Guidelines |
|---|---|
| CAT I | Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity. |
| CAT II | Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity. |
| CAT III | Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity. |

## 1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

## 1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

## 1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

## 1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing

Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

## 1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

# 2. ASSESSMENT CONSIDERATIONS

## 2.1 CA API Gateway Server Operating System Compliance

The CA API Gateway servers use the RHEL operating system. The implementation must use RHEL version 6.7.x or higher. The RHEL 6 STIG must be applied to each gateway server.

## 2.2 CA API Gateway Server NDM STIG

The CA API Gateway servers must apply the CA API Gateway NDM STIG. This STIG provides security guidance for the management plane on CA API Gateway servers.

## 2.3 CA API Gateway Server ALG STIG

The CA API Gateway servers must apply the CA API Gateway ALG STIG. This STIG provides security guidance for the data and control planes on CA API Gateway servers.

# 3. CONCEPTS AND TERMINOLOGY CONVENTIONS

The CA API Gateway is an XML firewall and service gateway that controls how web services are exposed to and accessed by external client applications. The Gateway provides runtime control over service-level authentication, authorization, key management, credentialing, integrity, confidentiality, schema validation, content inspection, data transformation, threat protection (including integration with external virus scanners for Simple Object Access Protocol [SOAP] attachment scanning), routing, protocol switching, Service-Level Agreement (SLA) enforcement, logging, and other functions.

## 3.1 Policy Manager

The Policy Manager is the user interface for the CA API Gateway. Located on the internal local area network, the Policy Manager communicates with the CA API Gateway. The Policy Manager is used to construct web service and XML application policies; manage policy users; configure identity bridging; and configure, audit, and monitor the CA API Gateway.

### 3.1.1 CA API Gateway Policy

For the CA API Gateway, a policy defines restrictions for the consumption of a published service that is protected by the Gateway. Policies can be global or specific to a particular service. Policies are constructed by adding assertions in a logical sequence.

### 3.1.2 Policy Assertions

Policy assertions are the building blocks for policies in the Policy Manager. Most assertions require configuration either before or after being added to the policy development window.