carahsoft.

Welcome to the

Carahsoft-ATARC Federal Cloud Marketplace Forum

Wednesday, July 24, 2019

Featuring FedRAMP Solutions & Successes

Getting to Success

Shawn Wells

Senior Principal & Chief Security Strategist, U.S. Public Sector, Red Hat

Red Hat

An open source approach to FedRAMP

Shawn Wells
Chief Security Strategist,
North America Public Sector
shawn@redhat.com || 443-534-0130

Red Hat

Taking the ATO process from 6 months to 30 days

By Aidan Feldman • July 19, 2018

Navy Aims for "Compile to Combat in 24 Hours"

By CHIPS Magazine - July-September 2018

When U.S. Navy warships prepare for deployment, Sailors work long hours testing radars and weapons systems; engineering, navigation and communications equipment; and hull, mechanical and electrical systems. It takes a huge effort by crews to ensure ships are ready to fight on arrival in

ORock Technologies Adds Red Hat OpenShift Container Platform to its FedRAMP Moderate Cloud

ORock to offer Secure Containers as a Service solution with Red Hat OpenShift

Red Hat

FedRAMP High.

FedRAMP Moderate.

FedRAMP Low.

....

....

AC-2: Account Management

AT-2: Security Awareness Training

AU-8: Time Stamps

CA-7: Plan of Action & Milestones

CM-10: Software Usage Restrictions

CP-2: Contingency Plan

IA-5: Authenticator Management

IR-8: Incident Response Plan

MA-4: Nonlocal Maintenance

FedRAMP High.

FedRAMP Moderate.

FedRAMP Low.

....

....

AC-2: Account Management

AT-2: Security Awareness Training

~~AU-8: Time Stamps~~
AU-9: Protection of Audit Information

CA-7: Plan of Action & Milestones

CM-10: Software Usage Restrictions

CP-2: Contingency Plan

~~IA-5: Authenticator Management~~
IA-2(12): Acceptance of PIV Credentials

IR-8: Incident Response Plan

MA-4: Nonlocal Maintenance

Red Hat

FedRAMP High.

FedRAMP Moderate.

FedRAMP Low.

....

....

~~AC-2: Account Management~~
AC-8: System Use Notification

AT-2: Security Awareness Training

~~AU-8: Time Stamps~~
AU-9: Protection of Audit Information

CA-7: Plan of Action & Milestones

~~CM-10: Software Usage Restrictions~~
CM-4: Security Impact Analysis

CP-2: Contingency Plan

~~IA-5: Authenticator Management~~
IA-2(12): Acceptance of PIV Credentials

IR-8: Incident Response Plan

~~MA-4: Nonlocal Maintenance~~

Red Hat

J2 | Common

	A	C	F	G
1	Control ID	NIST Security Control Class	Requirement Description	Control Response
2	AC.1.a	Technical	(U) The NRO shall develop, disseminate, and review/update at least annually a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. [Source: NIST SP 800-53 AC-1]	
3	AC.1.b	Technical	(U) The NRO shall develop, disseminate, and review/update at least annually formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. [Source: NIST SP 800-53 AC-1]	
4	AC.2.a	Technical	(U) The NRO shall identify account types (i.e., individual, group, system, application, guest/anonymous, and temporary) for each information system. [Source: NIST SP 800-53 AC-2]	
5	AC.2.b	Technical	(U) The NRO shall establish conditions for group membership. [Source: NIST SP 800-53 AC-2]	
6	AC.2.c	Technical	(U) The NRO shall identify authorized users of the information system and specify access privileges. [Source: NIST SP 800-53 AC-2]	
7	AC.2.d	Technical	(U) The NRO shall require appropriate approvals for requests to establish accounts. [Source: NIST SP 800-53 AC-2]	
8	AC.2.e	Technical	(U) The NRO shall manage the process of establishing, activating, modifying, disabling, and removing accounts. [Source: NIST SP 800-53 AC-2]	

AC-3	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AC-3 What is the solution and how is it implemented?

OpenControl

Structured language for ATO responses, created by 18F

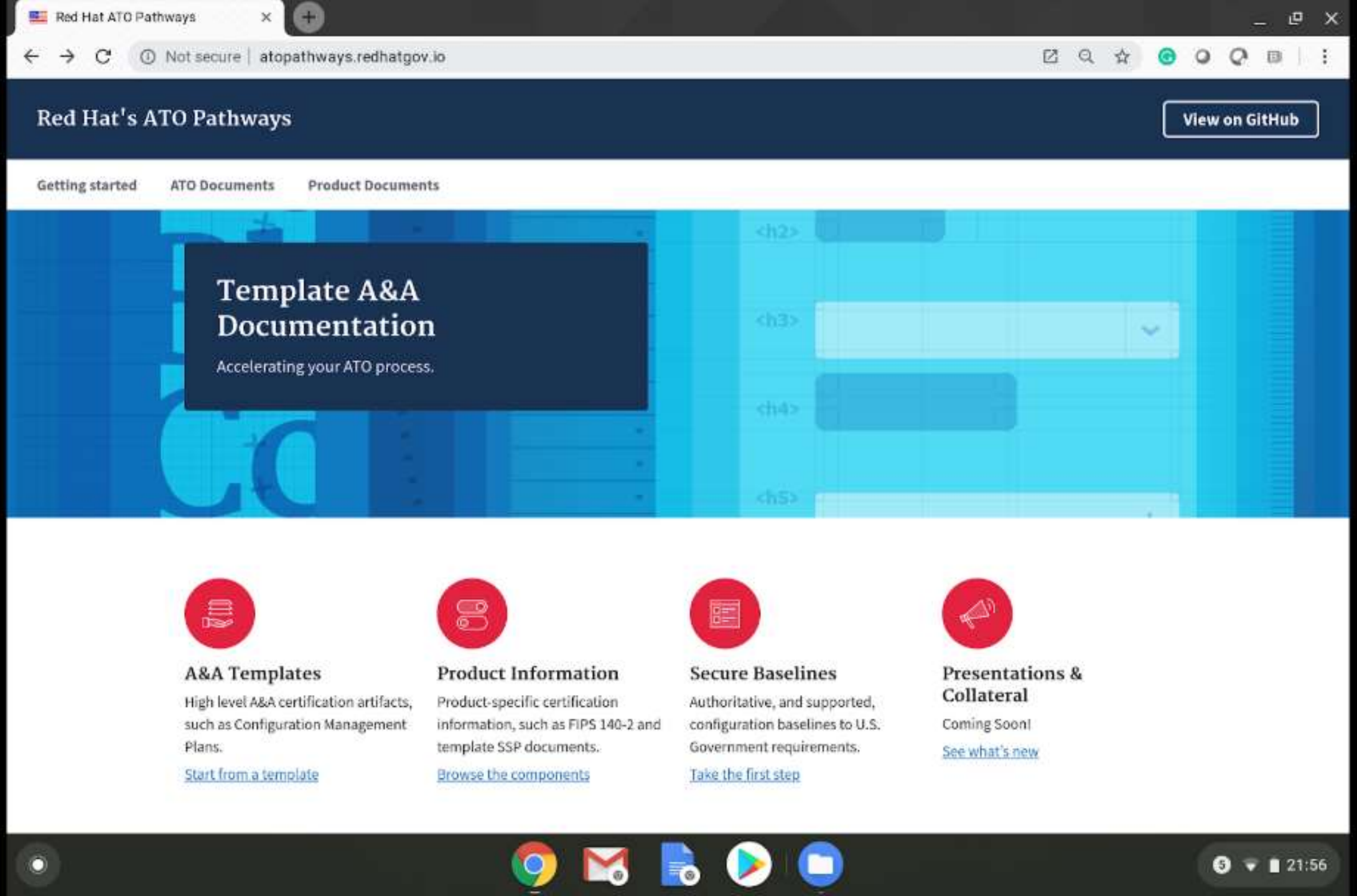
redhat

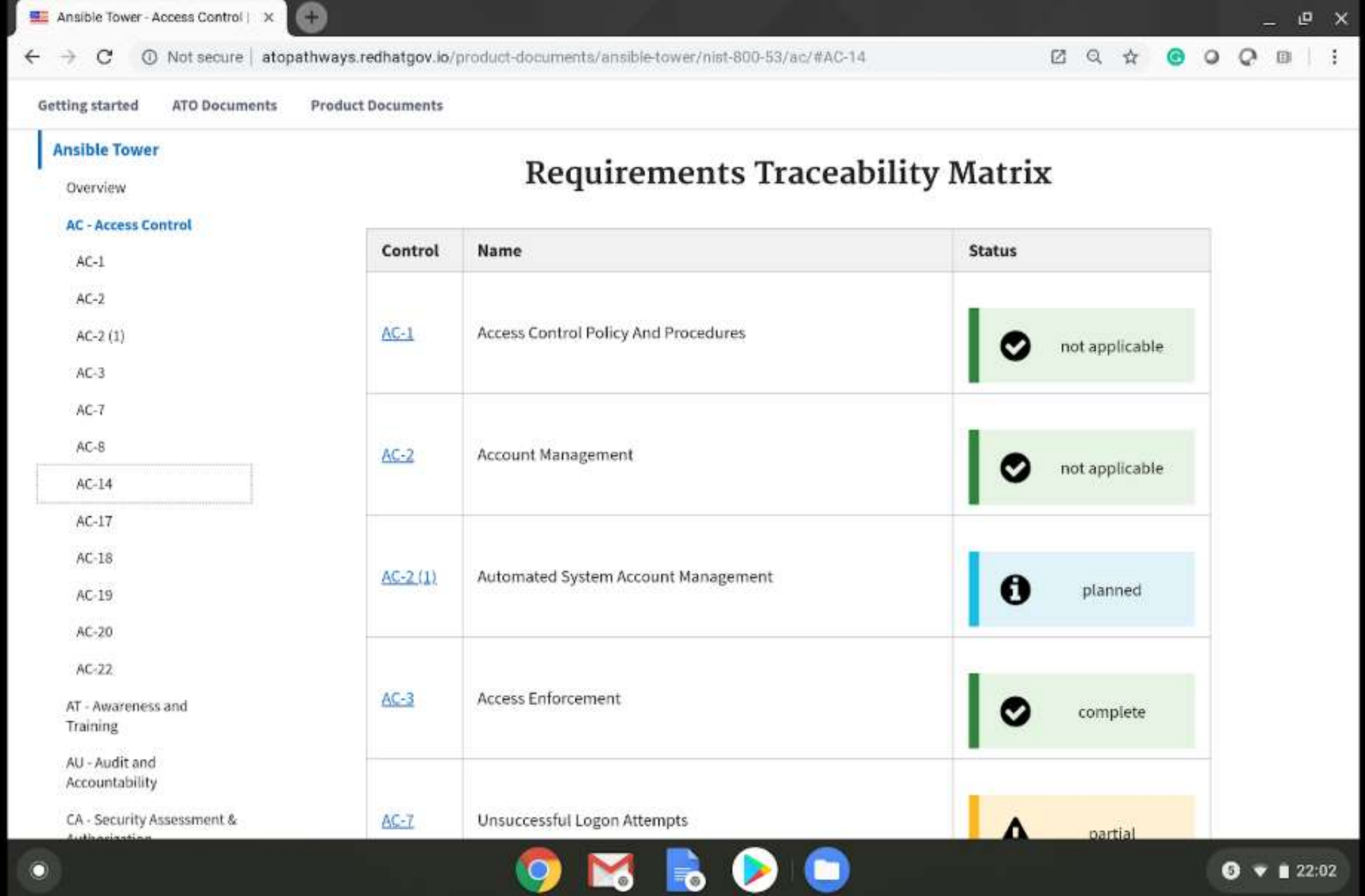
```
- control_key: AC-14
  standard_key: NIST-800-53
  covered_by: []
  implementation_status: complete
  narrative:
    - text: |
        'Regardless of access mechanism, such as the Ansible
        Tower console, unauthenticated users will only be shown
        the system use notifications (as defined in AC-8) and
        login prompt. This is non-configurable behavior.'
```

```
name: DoD-STIG
standards:
 NIST-800-53:
   AC-1: {}
   AC-14: {}
   AU-2: {}
   SC-3: {}
   SI-7: {}
```

```
name: FedRAMP-mod
standards:
 NIST-800-53:
   AC-1: {}
   AC-2: {}
   AT-7: {}
   AU-11: {}
   CA-4: {}
```

```
name: DHS-4300A
standards:
 NIST-800-53:
   AC-20 (1): {}
   AC-20 (2): {}
   AC-20 (3): {}
   AC-20 (4): {}
   AC-21: {}
```


Red Hat ATO Pathways
Not secure | atopathways.redhatgov.io
Red Hat's ATO Pathways
View on GitHub
Getting started
ATO Documents
Product Documents
Template A&A Documentation
Accelerating your ATO process.
A&A Templates
High level A&A certification artifacts, such as Configuration Management Plans.
Start from a template
Product Information
Product-specific certification information, such as FIPS 140-2 and template SSP documents.
Browse the components
Secure Baselines
Authoritative, and supported, configuration baselines to U.S. Government requirements.
Take the first step
Presentations & Collateral
Coming Soon!
See what's new
21:56


Ansible Tower - Access Control
Not secure
atopathways.redhatgov.io/product-documents/ansible-tower/nist-800-53/ac/#AC-14
Getting started
ATO Documents
Product Documents
Ansible Tower
Overview
AC - Access Control
AC-1
AC-2
AC-2 (1)
AC-3
AC-7
AC-8
AC-14
AC-17
AC-18
AC-19
AC-20
AC-22
AT - Awareness and Training
AU - Audit and Accountability
CA - Security Assessment &
Requirements Traceability Matrix
Control
Name
Status
AC-1
Access Control Policy And Procedures
not applicable
AC-2
Account Management
not applicable
AC-2 (1)
Automated System Account Management
planned
AC-3
Access Enforcement
complete
AC-7
Unsuccessful Logon Attempts
partial
22:02

Ansible Tower

Overview

AC - Access Control

AC-1

AC-2

AC-2 (1)

AC-3

AC-7

AC-8

AC-14

AC-17

AC-18

AC-19

AC-20

AC-22

AT - Awareness and Training

AU - Audit and Accountability

CA - Security Assessment & Authorization

CM - Configuration Management

CP - Contingency Planning

AC-14: Permitted Actions Without Identification Or Authentication

The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

AC-14 Control Response Information
Implementation Status:
complete

AC-14: What is the solution and how is it implemented?
'Regardless of access mechanism, such as the Ansible Tower console, unauthenticated users will only be shown the system use notifications (as defined in AC-8) and login prompt. This is non-configurable behavior. External service APIs also require authentication prior to granting resource access.'

NIST NATIONAL CHECKLIST PROGRAM

The National Checklist Program (NCP) is the U.S. Government repository of publicly available security checklists,

that provide detailed low level guidance,

on setting the security configuration of system components and applications

https://nvd.nist.gov/ncp/repository?authority=Red+Hat&startIndex=0

▼ NIST SP 800-53 = **CM-5(3)**		
Ensure gpgcheck Enabled For All yum Package Repositories	high	pass
Ensure gpgcheck Enabled for Local Packages	high	fail
Ensure Red Hat GPG Key Installed	high	pass
Ensure gpgcheck Enabled for Repository Metadata	high	fail
Ensure gpgcheck Enabled In Main yum Configuration	high	pass
▼ NIST SP 800-53 = **CM-6(3)**		
Verify and Correct File Permissions with RPM	high	fail
Verify File Hashes with RPM	high	pass
▼ NIST SP 800-53 = **CM-6(a)**		
Disable SSH Support for User Known Hosts	medium	fail
Disable SSH Support for .rhosts Files	medium	pass

ComplianceAsCode Project

https://github.com/ComplianceAsCode

INNOVATION

DOES NO GOOD IF YOU CAN'T SECURE IT

Thanks again to our speakers, sponsors and participants.

See more at:
carahsoft.com/FedRAMPForum
carah.io/fcmf