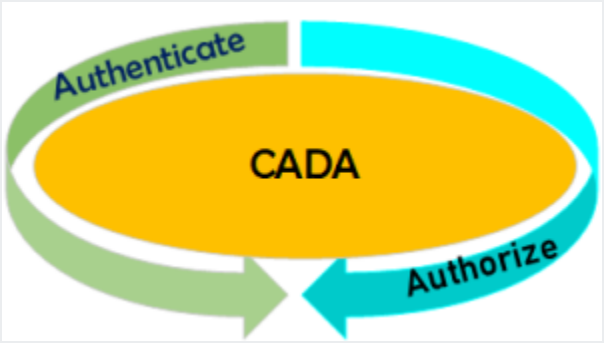
# E-CADA




**Enterprise Comcast Authentication and Delegated Administration**

## Overview

**CADA** is a centrally administered system which provides **authentication** and authorization to users who log on to servers/network devices to perform administrative work. It provides **Multi-factor authentication** and **Authorization** to Linux based servers and Network Devices using **Radius** and **MIT Kerberos Authentication**. Privileged accounts access is controlled by **SUDO** and **TACACS** roles by providing controls that helps to centrally secure, manage and monitor privileged accounts.

## CADA Salient Features

- Self-service UI for users and Admin
- Linux and Network Devices commands controlled for privilege access.
- Easy SSH key management for Service accounts
- RSA radius token PIN reset
- MIT Kerberos password reset
- RSA Token Assignment/download and management
- JIRA queue for Device on boarding
- API's automation for Device on-boarding /deprovision
- IDM integration for user Termination process.
- Easy CADA report access
- User Temp access
- PCI/SOX compliance/24/7 support
- Dynamic DNS integration for on-boarding

- CADA Architecture and Diagrams
- CADA RSA AMIS
- CADA RSA AMIS - Steps to deploy RSA AMIS Client on different platforms
- Access to CADA
- CADA User Help Guide
- RSA TOKEN SETUP

- CADA Service account Request
- CADA Operations Flow
- CADA Client installation
- Requesting CADA Account & Intake Process
- CADA 2.1 API Documentation
- RSA AM AMIS SELF API

- CADA RSA SERVICE ACCOUNT REQUEST
- How-to Videos
- Troubleshooting CADA Issues & Support
- **CADA FAQs**
- CADA Job Aid
- CADA UAR PROCESS
- CADA Tier 0

### Blog stream

Create a blog post to share news and announcements with your team and company.

Comcast Confidential - Any unauthorized disclosure or use is strictly prohibited