PRACTICE GUIDE | Energy
NIST SP 1800-2a

Identity and Access Management for Electric Utilities

Executive Summary

- The National Cybersecurity Center of Excellence (NCCoE) developed an example solution that electric sector businesses can use to more securely and efficiently manage access to the networked devices and facilities upon which power generation, transmission, and distribution depend.
- The security characteristics in our access management platform are informed by guidance and best practices from standards organizations, including the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards.
- The NCCoE's approach uses commercially available products that can be included alongside your current products in your existing infrastructure. They provide a centralized system with a comprehensive view of all users within the enterprise and across the IT, operational, and access control silos often found in electric companies.
- The example solution is packaged as a "How To" guide that demonstrates implementation of standards-based cybersecurity technologies in the real world, based on risk analysis. The guide helps organizations gain efficiencies in access management, while saving them research and proof of concept costs.

THE CHALLENGE

The electric power industry is upgrading older, outdated infrastructure to take advantage of emerging technologies that will create "a platform [that] efficiently [integrates] new energy resources, new technologies, and new devices into the system."[*] The ever greater numbers of technologies, devices, and systems connected to utilities' grid networks need protection from physical and cybersecurity attacks.[†]

Our conversations with utility company employees confirmed that current identity and access management (IdAM) implementations are often decentralized and controlled by numerous departments within a company. Several negative outcomes can result from this: an increased risk of attack and service disruption, inability to identify potential sources of a problem or attack, and a lack of overall traceability and accountability regarding who has access to both critical and noncritical assets.

To better protect power generation, transmission, and distribution, electric companies need to be able to control access to their networked resources, including buildings, equipment, information technology, and industrial control systems—all of which have unique technical and political challenges.[‡] Identity and access management (IdAM) systems for these assets often exist in silos, and employees who manage these systems lack methods to effectively coordinate access to devices and facilities in these silos. This drives inefficiency and can result in security risks for utilities, according to our electric sector stakeholders.

[*] Thought Leaders Speak Out: The Evolving Electric Power Industry, The Edison Foundation Institute, June 2015.
[†] State of the Electric Utility 2015, Utility Dive, January 2015.
[‡] Protect Critical Infrastructure, McAfee, 2012.

Imagine that a technician has access to several substations and remote terminal units connected to the company's network in those substations. The technician moves out of the region, so she quits her job. Without a centralized IdAM system, managing her access to various facilities and systems can be cumbersome and time-consuming, even error-prone. Electric utilities need the ability to provide the right person with the right degree of access to the right resources at the right time, and quickly.

THE SOLUTION

The NIST Cybersecurity Practice Guide "Identity and Access Management" demonstrates how commercially available technologies can meet your utility's need to control access to resources across the enterprise.

In our lab at the NCCoE, part of the National Institute of Standards and Technology (NIST), we built an environment that simulates an electric company's IT architecture, including the typical technology silos found in a utility (such as IT, operational technology, and physical access control systems).

We show how an electric utility can implement a centralized IdAM platform to provide a comprehensive view of all users within the enterprise across all silos, and the access rights they have been granted, by using multiple commercially available products.

The guide:

- maps security characteristics to guidance and best practices from NIST and other standards organizations, and to NERC CIP standards
- provides
  - a detailed example solution with capabilities that address security controls
  - a demonstrated approach using multiple products that achieve the same result
  - instructions for implementers and security engineers, including examples of all the necessary components and installation, configuration, and integration
- uses products that are readily available and interoperable with your existing information technology infrastructure and investments
- is modular and suitable for organizations of all sizes, including corporate and regional business offices, power generation plants, and substations

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee regulatory compliance. Your utility's information security experts should identify the standards-based products that will best integrate with your existing tools and IT system infrastructure. Your company can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

Our example solution has the following benefits:

- products and capabilities can be adopted on a component-by-component basis, or as a whole, thereby minimizing impact to the enterprise and existing infrastructure
- can reduce the risk of malicious or untrained people gaining unauthorized access to critical infrastructure components and interfering with their operation, thereby lowering overall business risk
- allows rapid provisioning and de-provisioning of access from a centralized platform, so IT personnel can spend more time on other critical tasks

- improves situational awareness: proper access and authorization can be confirmed via the use of a single, centralized solution
- improves security posture by tracking and auditing access requests and other IdAM activity across all networks
- can enhance the productivity of employees and speed delivery of services, and support oversight of resources, including information technology, personnel, and data

SHARE YOUR FEEDBACK

You can get the guide at http://nccoe.nist.gov and help improve it by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

- email energy_nccoe@nist.gov
- participate in our forums at hhttp://nccoe.nist.gov/forums/energy

Or learn more by arranging a demonstration of this reference solution by contacting us at energy_nccoe@nist.gov.

TECHNOLOGY PARTNERS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution.