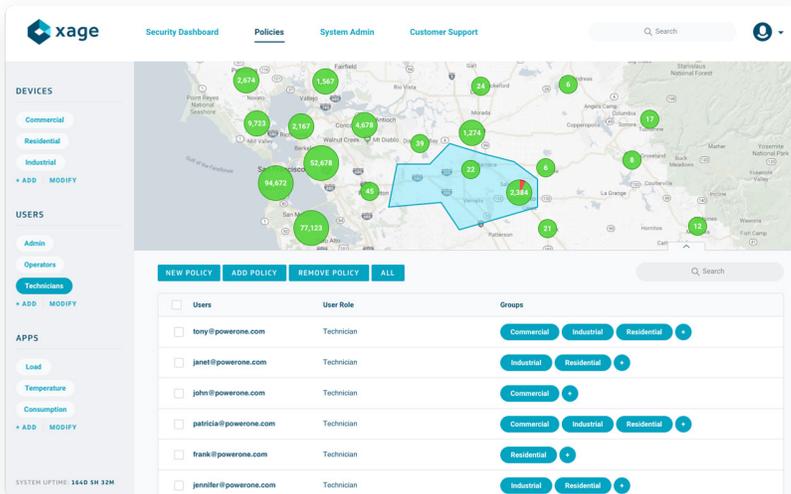


# ROLE-BASED ACCESS CONTROL

FOR INDUSTRIAL CONTROL SYSTEMS

## RBAC for Industrial Control Systems



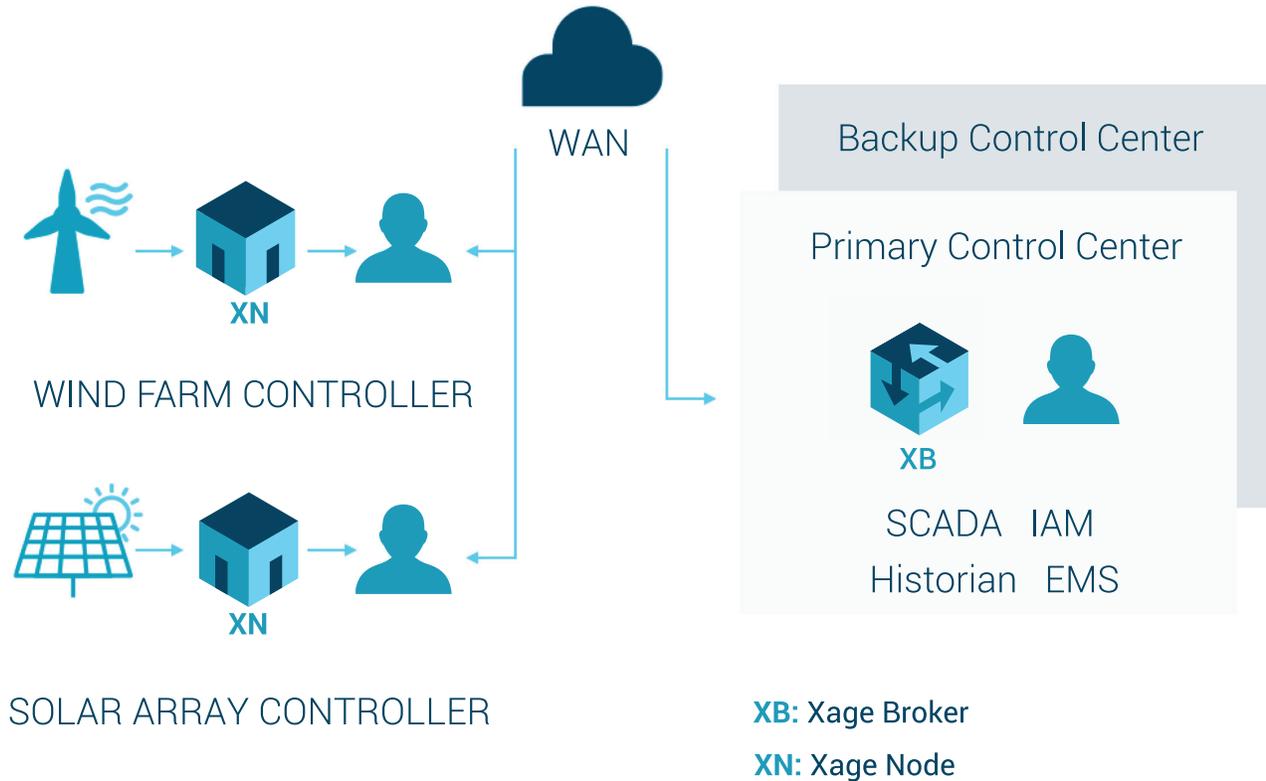
## Use Case

Industrial control systems (ICS) and industrial IoT devices require RBAC (role-based access controls) for effective maintenance operations and process control. Industrial and commercial operators face challenging roadblocks to maintaining secure credential systems: a large-scale heterogeneous IoT landscape with multiple vendors and multiple credential types; lost, stolen, hardcoded, or shared credentials; numerous management and control interfaces and protocols; or intermittent network connections.

Current security solutions provide limited visibility and security control over maintenance operations and industrial processes. As organizations and processes change, the only way to update credentials across the field may be to manually change them one-by-one. This creates an impossibly difficult and expensive task for operators, leaving systems vulnerable to cyber attacks. Plus, misused credentials could result in financial and reputational loss.



## How it Works



## Supported Protocols and Systems

Modbus, MQTT, OPC UA, DNP3, ACTIVE DIRECTORY, LDAP, RADIUS

## Xage Security Suite

Xage delivers industrial-grade security to the edges of highly decentralized industrial and commercial operations, empowering operators to manage user and device identities, credentials, and access control policies with ease. The Xage Security Fabric enables users and systems to interface with field devices across the entire operation, using centrally managed credentials with authentication and enforcement at the edge. The Xage Security Fabric is deployed across Xage Brokers in the data center and Xage Nodes at the edge. Xage delivers role-based access control services using a decentralized architecture, enabling uninterrupted service delivery over intermittent network connections without a central point of failure. The Xage Security Fabric uses consensus-based security techniques to ensure data confidentiality, enforce access restrictions and self-heal even if part of the network is compromised – so the larger the deployment, the more secure the system becomes.

The Xage Broker integrates with existing identity and services, making specific identities, credentials, and access control policies available and enforceable at the edge. Xage thus integrates industrial IoT devices and control systems (PLCs, RTUs, meters) with enterprise identity management systems such as LDAP, Active Directory, and RADIUS. With Xage, users and systems interface with IoT devices using managed identities and permissions instead of device specific credentials. The solution integrates with existing devices and protocols. Xage Nodes also integrate with HMIs, providing RBAC for users and industrial processes running in the SCADA environment. Additionally, Xage ensures regulatory compliance by rotating credentials and providing a log of every credential use and operation, making audits quicker, easier, and cheaper for the operator.

Xage Security  
445 Sherman Avenue, Suite 200  
Palo Alto, CA 94306