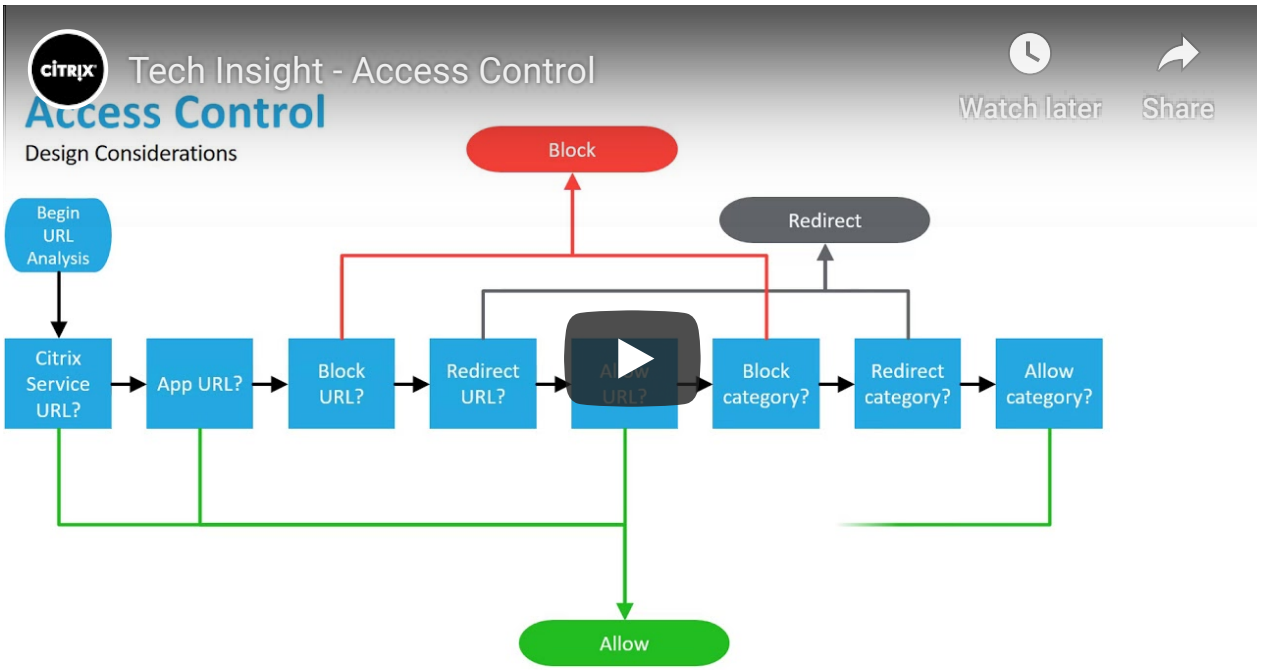
What is access control?

Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources. Through authentication and authorization, access control policies make sure users are who they say they are and that they have appropriate access to company data. Access control can also be applied to limit physical access to campuses, buildings, rooms, and data centers.



How does access control work?

Access control identifies users by verifying various login credentials, which can include user names and passwords, PINs, biometric scans, and security tokens. Many access control systems also include multifactor authentication, a method that requires multiple authentication methods to verify a user's identity.

Once a user is authenticated, access control then authorizes the appropriate level of access and allowed actions associated with that user's credentials and IP address.

There are four main types access control. Organizations typically choose the method that makes the most sense based on their unique security and compliance requirements. The four access control models are:

Discretionary access control (DAC)

In this method, the owner or administrator of the protected system, data, or resource sets the policies for who is allowed access.

Mandatory access control (MAC)

In this nondiscretionary model, people are granted access based on an information clearance. A central authority regulates access rights based on different security levels. It's common in government and military environments.

Role-based access control (RBAC)

RBAC grants access based on defined business functions rather than the individual user's identity. The goal is to provide users with access only to data that's been deemed necessary for their role within the organizations. This widely used method is based on a complex combination of role assignments, authorizations, and permissions.

Attribute-based access control (ABAC)

In this dynamic method, access is based on a set of attributes and environmental conditions, such as time of day and location, assigned to both users and resources.

Why is access control important?

Access control keeps confidential information, including customer data, personally identifiable information, and intellectual property, from falling into the wrong hands. Without a robust access control policy, organizations risk data leakage from both internal and external sources.

It's particularly important for organizations with hybrid, multi-cloud cloud environments, where resources, apps, and data reside both on premises and in the cloud. Access control can provide these environments with more robust access security beyond single sign-on (SSO).

Additional Resources

- Deliver secure access to VDI
- Learn more about Citrix Gateway and Citrix Access Control