Identity-based provisioning with Citrix CloudGateway

Provision and deliver apps and data based on user and user role
Application heterogeneity is growing. According to a recent Citrix survey, Windows® apps represent 61% of a typical company’s application portfolio, followed by internal web apps at 24%, SaaS apps at 10% and mobile apps at 7%. However, this picture is changing and will become even more diverse, with Windows apps expected to decrease to 50% and SaaS and mobile apps combined projected to increase to 25% of a company’s portfolio. With this wide variety of applications, companies need to provide users quick access without requiring IT to sign into multiple management systems to individually provision application access.

Citrix® CloudGateway™ leverages Microsoft® Active Directory® and other directory systems to provision, deliver and control how mobile apps—including email and intranet—as well as web, SaaS and Windows apps and data are used based on user and user role. This solution enables IT to instantly provision all of a user’s applications and data as soon as they are added to Active Directory, while preventing access by and closing accounts for users who are removed from the directory system.

The current IT environment
Today’s enterprises operate in an environment where resources are premises-based and access is based on identities, which are part of an enterprise directory system. Due to the way organizations have evolved and the dependencies of applications with certain identity formats and repositories, enterprises have had to deal with multiple directories. As an example, business partner and contractor information may be in a different directory from Microsoft application-related information, which is in a different identity repository from certain legacy applications, and so on.

On-premises identity management systems have tried to solve this challenge using virtual directories, multiple identity repositories, directory-specific configurations such as transitive trust and complex directory forests. These solutions help IT teams obtain a measure of control so that they can roll out applications based on one root identity, while allowing their identity management systems to maintain and resolve the dependencies and relationships.

However, all of these solutions break completely when the applications move out of the enterprise premises and into cloud environments. Applications delivered from the cloud cannot be tweaked, especially if they are delivered in a SaaS format, and this constraint quickly results in the following unmanageable environment:
• Multiple user identities per application or environment
• Complex management processes to maintain identities across multiple environments
• Identity federation requirements to assert identities across different environments
• Poor user experience with multiple credentials for applications
• Increased support costs resulting from locked accounts and service desk calls
• Lost employee productivity due to delayed account provisioning and locked applications
• Security cost and compliance issues, including external accounts left accessible even after the user has lost the right to access the application

How CloudGateway solves these challenges
CloudGateway provides a way to make Active Directory the single source for identifying who has access to what applications and services. CloudGateway extends Active Directory to authorize access to all enterprise and cloud-based applications. In its simplest form, a CloudGateway policy can take a user’s group membership in Active Directory and automatically create an account in a SaaS application (if that group membership dictates access to this application). As an example, let’s consider two types of applications – a human resources app that everyone in the organization must have access to and a finance app that only managers can access. A CloudGateway policy can trigger the creation of user accounts on the HR app for everyone and user accounts on the finance app only for users designated as “managers” inside Active Directory. Besides managing the user accounts on these applications, CloudGateway can facilitate seamless sign-on with support for identity federation using standards such as Security Assertion Markup Language (SAML).

1 On average, enterprise users need to deal with at least 10 IDs and passwords per day when accessing their work applications
2 A common example is a SaaS app with sensitive enterprise information is left accessible because the manual process of turning off that user’s external account fell through the cracks.
Identity-based provisioning with Citrix CloudGateway

Solution details
The CloudGateway AppController is a SAML-compliant identity provider that connects to the enterprise directory, reads the authorization policies configured and provides the appropriate secure SAML tokens for user sign-on to federation-enabled applications. To interoperate with older applications that do not support SAML, CloudGateway can act as a password manager, storing user credentials and providing them securely so users don’t have to remember their app credentials. Built into CloudGateway is a long list of “connectors” for applications that have all the required interaction logic leveraging APIs that the applications expose; for example, APIs to create user accounts within those applications based on authorization policies. Working together with StoreFront, authorized applications are exposed to users through Citrix Receiver™, forming an enterprise app store and providing users a single place to authenticate and get access to all their enterprise applications.

Further, CloudGateway has a built-in account creation and approval workflow capability that allows users to request app access or accounts from Receiver, and results in the user’s account being created only after the approvals have been provided by the configured set of approvers for such a request.
Conclusion

CloudGateway simplifies how IT manages increasing application diversity by allowing enterprises to use their existing directory system to provision and control all of their applications, including cloud-based apps. This approach requires much less effort compared with extending existing identity and access management solutions. IT benefits from this integration because there are no application changes required to support a broad set of federation-aware as well as credential-only legacy applications. For Citrix® XenDesktop® customers, CloudGateway fits seamlessly into the existing delivery infrastructure, extending the Receiver experience by adding additional applications, such as mobile, web and SaaS, into an interface that already presents users’ Windows apps and desktops. In addition, customers who utilize CloudGateway will realize immediate benefits from automated application provisioning in the form of reduced help desk calls and higher user satisfaction and productivity due to self-service and quick turnaround of app requests.