CloudGateway: App Requests with Automated Provisioning

Providing users with simpler, faster access to their apps, and IT with hassle-free, automated workflows and provisioning

With a constantly growing, ever-changing workforce and business requirements, dealing with the increasingly wide range of device and application needs, while keeping pace with security and the adoption of new technology creates a challenging environment for any IT department. Additionally, as technology providers are focusing their efforts on creating consumer applications, users now introduce more and more SaaS applications into their work environment. Throw in the myriad of devices that employees bring to work and you’ve got a very complex IT environment. Clearly, IT needs a solution that can unify the management of all the enterprise Windows, Web & SaaS applications, and devices.

CloudGateway enables IT to regain control by unifying the management, control and delivery of apps, devices and data. One of CloudGateway’s key features is the ability to automate user requests, approval workflows and application account provisioning upon approval.

The Current Scenario

Manual procedures that are employed today to provision and de-provision accounts slow down the process of on-boarding users and migrating users from one role to another role within an organization. On one hand, IT is facing frustrated users who don’t have immediate or timely access to the apps and data they need to do their jobs. On the other hand, IT is struggling and is slow to support and enable new apps, new devices and new users. This predicament becomes increasingly more apparent when there is substantial user turnover in enterprises.

How CloudGateway Solves These Challenges

CloudGateway consists of three strategic components: Gateway services (security), Storefront services (aggregation and delivery of all apps and data) and AppController (content controller for web and SaaS apps). These components seamlessly integrate with Citrix Receiver, XenDesktop and XenApp to deliver a single point of app access for users and a single point of control for administrators.
Gateway services authenticate and authorize users into the application delivery environment, providing strong security and the ability for administrators to craft granular control policies that take into account the entire access scenario context (e.g. device, network, user, location) before allowing users to enter the environment.

StoreFront services enumerate and aggregate all content, including virtual desktops and apps delivered by XenDesktop and XenApp, web apps and 3rd-party SaaS apps. The apps can be organized into different ‘stores’ and/or ‘categories’ that users access through Citrix Receiver.

The Content controllers deliver various types of applications with single sign-on access, enumerating and launching those apps via StoreFront. Content controllers also help enforce the secure access policies established by the Gateway services.

**Solution Details**

CloudGateway provides users with one unified place to easily access existing applications, subscribe to new applications for which they are authorized, or request approval to access applications for which they are not yet authorized.

To accomplish this, CloudGateway utilizes a role-based user and application matrix to intelligently provide contextual delivery of applications to users. All Windows, web and SaaS applications are consolidated and delivered through StoreFront. The content controllers (e.g. XenDesktop, XenApp and AppController) provide numerous application “connectors” that provide users single-click, single sign-on access to any application for which they are authorized; not just traditional enterprise apps, but cloud based web and SaaS applications as well. If users are not yet authorized to use an application they can easily request access from the same screen.

With Citrix Receiver integration, CloudGateway delivers a consistent user experience on all device types. Most mobile devices may leverage a native Receiver client specifically designed for the best experience on that platform. Users with unique mobile devices that do not support native Receiver clients can easily leverage a fully HTML5-compliant version of Receiver (called Receiver for Web) that is accessed from a web browser. This flexibility makes it easy for IT teams to deliver zero-day access to apps when deploying CloudGateway - ensuring the ultimate in flexibility and productivity.

When users start Citrix Receiver from outside the corporate network, they must first authenticate using Gateway services – which also performs any endpoint analysis scans defined by administrators to determine the full access scenario context. Receiver then provides the results of the endpoint analysis – which could include information about the presence and version level of the user’s device, it’s operating system, antivirus, firewall, type and/or version of the client browser, and their connection bandwidth - along with the user’s network identification to StoreFront services, in order to obtain a list of available applications. StoreFront contacts each of the content controllers to aggregate a complete listing of the applications to which the user is authorized to access, based on their context and corresponding secure access rules established by administrators.
The screenshot below shows the user interface with a list of available apps; the apps to which they have already subscribed appear on their desktop. Some of the apps display a ‘Request’ button; these are apps for which approval is required before access is granted. When the user clicks a ‘Request’ button an automated workflow (which is defined by the administrator) gets activated, and if approval is granted through the workflow the user will gain access with no intervention required by IT. If the request is denied, no access is granted.

Defining Workflows

AppController’s powerful workflow engine and intuitive administrative user interface are used to create unique workflows and associate them with applications and/or provisioning tasks. The flexible nature of the workflow engine allows you to design fully automated workflows based on your existing organization structure, security guidelines and compliance rules, and update the workflows as the structure, security guidelines and compliance rules change. Provisioning tasks include creating, deleting, enabling, disabling, resetting passwords, and unlocking user application accounts.
CloudGateway first uses scans through an enterprise authoritative source of information, such as your Active Directory, to discover information about your employees, their titles, roles and their hierarchy in the organization. It then leverages this information and allows you to define approvers based on their name, title, or role. You can configure and tweak things such as the workflow approval sequence, total number of approvals required, whether approvers are mandatory or not, who a task should be delegated to when a primary approver is on leave, how often task reminders should be sent, etc.

These workflows route user requests for application access to the defined approvers via email. Approvers are provided with a single-click link to approve or deny each request. When clicked, this link navigates and automatically logs the approver into a portal where they can view and act on one or multiple pending tasks. Based on the configuration, approvers can receive an email every time a user raises a request or a single consolidated summary email at a pre-defined time every day, with all their pending requests. A single click can approve, reject or delegate the task to another approver.

AppController uses HTTPS calls to asynchronously update StoreFront on the progress of the workflow and user account creation. Users can easily keep track of their requests by monitoring the request status in Receiver.

AppController’s flexible provisioning engine utilizes APIs, Web Services, SPML and SAML to communicate with applications and create new user accounts. When the approval process is complete, AppController automatically creates the user account, enables single sign-on to the application for the user and updates the user’s Receiver with the new account information. The next time the user logs in to Receiver, they see that their request is complete, and the application is automatically added to their home screen.

The provisioning engine is fully automated and can be utilized to on-board/off-board users with no manual intervention.

Additionally control and automation can be brought through Active Directory groups. With this feature CloudGateway seamlessly synchronizes with your enterprise Active Directory and detects new users that are added to security groups. Based on an administrator defined group-to-application mapping, users added to a group in Active Directory can automatically be provisioned in an associated application. Similarly, when users are removed from the Active Directory group, they are automatically de-provisioned from the associated application.

**Conclusion**

CloudGateway goes above and beyond to simplify today’s manual IT processes for managing user accounts across Windows, Web and SaaS applications. Customers who utilize CloudGateway will realize an immediate benefit from reduced IT workloads, help desk calls and higher user satisfaction and productivity due to self-service and quick turnaround of app requests.