Creating and Enforcing Advanced Access Policies with Citrix XenApp

Granular policies for users, devices, locations and connection types let you secure and manage the user experience the right way to enable any mobile workspace scenario.
To empower people to be fully productive anywhere, IT needs to enable fast, simple access to services with a great user experience on any device over any network—while ensuring that corporate information remains protected. Traditional approaches to user access designed for a simpler computing environment lack the flexibility to address diverse trends and use cases such as consumerization, telecommuting, BYOD, third-party collaboration and the rise of mobile devices. IT needs a more granular way to manage and secure user access the right way for every scenario.

Many organizations already rely on Citrix® XenApp® as the foundation of their strategy to deliver applications as services to any device. Equally valuable, though often overlooked, is the ability to use XenApp to create and enforce advanced access policies to support a wide variety of use cases, from blocking access to USB devices for users outside the network to optimizing video playback based on available bandwidth. By defining policies around factors such as device, connection type and the location of a user inside or outside the enterprise network, IT can automatically configure the user experience to allow optimal business productivity while ensuring effective security for corporate information.

Secure application delivery and advanced access control with XenApp

XenApp enables any Windows® application to be virtualized, centralized and managed in the datacenter and instantly delivered as a service to users anywhere on any device. Benefits of this approach such as anywhere, any-device access, improved manageability and performance are well known; for example, XenApp can reduce transaction times for client-server applications by up to 300 percent because applications run next to their database in the datacenter, even when accessed from distant locations. What is often overlooked is the role XenApp can play, in tandem with other Citrix solutions, in protecting corporate information.

The centralization of applications and data within the hardened datacenter makes XenApp a secure-by-design solution. Only screen update, mouse click and keystroke commands cross the network to the user’s endpoint device, greatly reducing the risk of data exposure or exfiltration. No data resides on the device, and nothing is left behind when the network connection is terminated.

Beyond its inherently secure architecture, XenApp also helps IT enable secure mobile productivity by creating advanced access control policies for specific groups of users, devices or connection types. For example, you can create policies allowing a group of users to
access a wide range of applications and data while on the LAN, a subset of those resources while on a tablet at home, and a smaller subset from a smartphone connected through a public network. Another, less trusted group could be restricted to a small subset of resources under all conditions. Administrators can go even further by restricting the ability of users in insecure environments to copy, email or print data, or to save confidential files to removable media. You can also limit access based on the security posture of the specific endpoint being used, or limit users on public kiosks to viewing data and nothing else.

Access control policies can also be designed to optimize the user experience. For example, for users determined to be using a mobile device, the policy can enable a touch-screen interface for published applications. In situations with limited bandwidth, XenApp can manage video streaming and caching to ensure high-quality playback while ensuring that business-related content is given a higher priority than other content employees may view.

The following sections explore the tools used to create and enforce advanced access policies with XenApp and examples of the policies that can be defined.

**Access policy definition and enforcement**

The native access control capabilities of XenApp work in tandem with the Citrix NetScaler Gateway secure application and data access solution to support policy creation and enforcement for any use case or scenario. XenApp determines the policies to be applied based on both connection filters such as IP address, client name, user name and remote access profile; and resources filters such as desktop group, desktop kind, application and IT-assigned tags, then automatically delivers the right experience with the right level of security in each scenario.

For users connecting from outside the corporate LAN, NetScaler Gateway provides a critical additional layer of security and access control. NetScaler Gateway first ensures secure remote access by using secure Citrix ICA proxy technology to encrypt data without the need to establish a full VPN tunnel from remote devices. Once connected, NetScaler Gateway uses Citrix HDX SmartAccess technology to perform pre-authentication endpoint analysis to ensure that the user’s device is free from malicious files and protected with up-to-date firewalls, antivirus definitions and hard drive encryption tools, and that it has not been jailbroken, rooted or otherwise compromised. If these requirements are not met, the user can be restricted to a limited set of applications and data, or redirected to a remediation site where the security deficiencies can be addressed. These policies can be applied dynamically as users move among different devices, applications and locations. Upon authorization, NetScaler Gateway applies tags to the user’s session to indicate conditions such as the IP address being used and the type of computer or mobile device being used.
Once a remote user has been granted access via NetScaler Gateway, XenApp uses the SmartAccess tags assigned by NetScaler Gateway to guide the application of the appropriate XenApp policies for access to published resources.

Citrix Receiver™ ensures a high-quality experience for every user by making it easy for IT administrators to securely enable application access from any type of personal or corporate-owned device while ensuring that IT security procedures and processes are enforced. Citrix Receiver is in constant communication with the XenApp infrastructure to identify the optimal application delivery method for any user based on device features, available network connection and specific application-related tasks. Users in any location can download Citrix Receiver and securely access XenApp published applications, making it easy for IT to meet employee demands without compromising security standards.

IT also has the option of working with policies using the Group Policy Management Console in Microsoft Windows. This can be a good approach if your network environment includes Microsoft Active Directory and you have the appropriate permissions to manage Group Policy Objects (GPOs).

**Policy assignments and use cases**
A XenApp policy can be assigned to specific users and machine objects that meet IT-defined criteria for connection and resource types. You can add as many assignments to each policy as you choose; policies with no assignments will be applied globally to all connections. Policy templates and wizards simplify your management of the user experience within your environment with pre-configured settings that optimize performance for specific environments or network conditions—for example when there is low bandwidth or users require a high quality user experience.

A broad range of available assignments for XenApp policies let you address diverse access use cases throughout the enterprise.
Access Control – IT can apply a policy based on the access control conditions through which a client is connecting. If the connection is made with NetScaler Gateway, session policies appropriate for remote access or mobile devices, or both, can be applied. For example:

• If NetScaler Gateway determines, based on HTTP header information, that a user is connected from a mobile device, the appropriate mobile device optimization settings in XenApp can be applied.
• IT can also choose to block features such as printing, and access to security-sensitive apps and data, for people connected from outside the corporate LAN.

Citrix CloudBridge™ session – For sessions launched through the Citrix CloudBridge WAN optimization platform, IT can apply policies to ensure a high-quality experience by managing data transmission over the WAN. For example:

• A policy can force video redirection to transfer video data outside of the ICA data stream, enabling CloudBridge to cache the video locally. This eliminates the need to re-transmit video data over the WAN for subsequent viewings by the same or other users.
• In scenarios with very restricted bandwidth, IT can increase or remove ICA bandwidth limits when CloudBridge is used. Other locations can be designated for maximum bandwidth for printing, drive redirection and other less important virtual channels.

Client IP Address – Filtering policies based on the IP address (IPv4 or IPv6) of the user device used to connect to the session can address use cases for both user experience and security. For example:

• In corporate environments with a location-based IP addressing scheme, IT can assign the printer closest to the user for each session.
• For high-security scenarios, IT can limit access and usage of sensitive data by preventing clients outside a specific IP address range from connecting to client drives or using clipboard mapping.

Client Name – The ability to filter policies based on the name of the endpoint can be useful in environments with standard computer naming schemes. For example:

• IT can easily assign printers and other peripherals based on proximity to fixed-location computers.
• Loaner laptops available for temps or contractors can be assigned restricted functionality to maintain security, such as by preventing file uploads and downloads, or the use of USB storage.

Delivery Group – Based on the Delivery Group membership of the desktop running the session, IT can help people access the right resources for their needs while preventing access to inappropriate resources. For example:

• IT can point each Delivery Group to the virtual desktops intended for their use, whether to ensure that they use desktops tailored to the needs of teams such as HR, finance or marketing, or to prevent one group from using more than their share of standardized desktops and leave other groups short.
• Local resources such as printing and USB storage can be disabled for kiosk-style desktops and apps.
Tag – This highly flexible capability lets IT apply policies based on any tags applied to the client or desktop running the session. For example:

- A small number of devices that support an esoteric use case can be managed and secured in highly specific ways by setting tags on a VM level.

Organizational Unit (OU) – Filters based on OU location make it simple to configure the Profile Manager profile path, along with other profile parameters, for each location or branch in your organization.

User or Group – Policies can be defined to manage the user experience in the right way for specific types of users. For example:

- IT can customize ICA or HDX session parameters such as local resource access, performance optimizations and printer mapping to match the requirements of the users, such as by optimizing graphics performance for CAD users or assigning high-end scanners and printers to marketing personnel.

ICA policies
ICA policies let you manage and secure the user experience based on factors such as group membership and network location. This allows you to:

- Control whether or not drives on the user device are connected when users log on to the server.
- Control cut-and-paste data transfer between the server and the local clipboard. Users can still cut and paste data between applications running in sessions.
- Control how drives map from the user device.
- Control whether users’ local disk, floppy, or network drives are available in a session.
- Control whether users’ local CD, DVD, or Blu-ray drives are available in a session.
- Control whether users’ local removable drives are available in a session.
- Control whether USB devices are available in a session.
- Control creation of client printers on the user device.
- Control the location where printer properties are stored.
- Control whether print requests are processed by the client or the server.
- Control whether users can access printers connected to their user devices.
- Control installation of native Windows drivers when automatically creating client and network printers.
- Choose a printer based on a roaming user’s session information.

Delivery Group exclusion filters
In addition to the access policies and assignments described above, you can restrict access or otherwise manage virtual desktop sessions through exclusion filters on access policies that you set with the XenApp Software Development Kit (SDK). For example, you can restrict machine access to a subset of the users listed on the Delivery Group’s user settings page, and you can specify the allowed user devices that can connect to machines.
The Secure ICA minimum encryption level setting lets you specify the minimum level at which to encrypt session data sent between the server and a user device. You can raise encryption levels to further secure communications and message integrity for certain users. If a policy requires a higher encryption level, Citrix Receiver clients using a lower encryption level are denied connection.

**Conclusion**

As mobile workspaces transform the way people work and enterprise use cases proliferate, you need the flexibility to manage access to data and resources with a high degree of granularity. Citrix XenApp, working in tandem with Citrix NetScaler Gateway and Citrix Receiver, provides a simple way to ensure a high-quality experience anywhere inside or outside the LAN, on any device, while protecting sensitive corporate information.