



Citrix Access Suite 4.2 Connections

5/10/2006



Table of Contents

1.	Introduction.....	3
2.	Citrix Presentation Server.....	3
2.1.	<i>Citrix Presentation Server Internal Network Communication</i>	3
2.2.	Presentation Server External Network Communication.....	8
2.3.	Presentation Server External Access: Secure Gateway Proxy.....	12
3.	Citrix Password Manager.....	15
3.1.	Citrix Password Manager in File Share Central Store Configuration.....	15
3.2.	Citrix Password Manager in Active Directory Central Store Configuration....	18
4.	Citrix Access Gateway Enterprise	20
4.1.	Citrix Access Gateway Enterprise Connections	20
4.2.	Advanced Access Control Resources' Connections.....	24
4.3.	Advanced Access Control Authentication Connections	27
5.	GoToMeeting Helper for Citrix Presentation Server.....	29
6.	Special product notes:.....	33
6.1.	Citrix License Server	33
6.2.	Citrix Presentation Server IMA Datastore Server	33
6.3.	Citrix Access Management Console.....	33
6.4.	TCP/IP ICA Browsing	33
6.5.	Interoperability with Citrix MetaFrame 1.8 Servers.....	34
6.6.	Citrix Presentation Server for UNIX	34
6.7.	Connections to Microsoft Active Directory Domain Controllers.....	34
	Appendix: Access Suite Connections Reference Table:.....	35

1. Introduction

This document provides information on connectivity and ports used in Citrix Access Suite 4.2 environments to assist network and security administrators with configuring network, access and firewall policies.

2. Citrix Presentation Server

This section covers connectivity of Citrix Presentation Server® and its components, including Web Interface server and Conferencing Manager. Also covered are Citrix® ICA® clients and their connections.

2.1. Citrix Presentation Server Internal Network Communication

Description

The diagram below illustrates connections created by users, administrators and servers in an internal corporate network with Citrix Presentation Server and its components deployed. This particular deployment is shown in integration with Microsoft® Active Directory and Microsoft® SQL Server.

Use Case 1

Some members of the Blinxalex Corporation's internal training department move around inside the corporation during the work day. Trainers often spend a day or more in another department and carry their laptops with them to securely connect to training resources. Other personnel usually work from their own offices, but sometimes have to spend time in other locations for meetings and information-sharing sessions. During these sessions public kiosk computers in conference rooms are used to enter meeting notes. Courseware development personnel working from their offices have client software integrated with their desktops, and see the server-provided applications as if the applications were installed locally.

Administrator's Note

Trainers have Program Neighborhood® Classic configured to securely access resources published on Citrix Presentation Server, either through SSL Relay or by relaying through Secure Gateway.

Conference rooms have kiosks with Internet Explorer available that allow meeting participants to connect to Citrix Web Interface Server and either access launched applications from their own desktop sessions while roaming (SmoothRoaming™) or start new ones to enter meeting notes. In this situation, the Citrix Java client is used to avoid installing any applications on the kiosk computers.

Courseware developers work from their desktop computers using Program Neighborhood Agent to provide maximum integration with Windows® computers. They see published applications in the Start Menu and on their desktop. Program Neighborhood Agent receives settings from the Program Neighborhood site of the Web Interface server.

Use Case 2

Network administrators of the Blinxalex Corporation use server-based administration tools to perform their functions. When outside of the office they connect to the management website through Internet Explorer with special accounts that use RSA SecurID tokens for logon. Then they have access to various network management and administration tools.

Administrator's Note

Administrators access a Citrix Web Interface Presentation Server site that is configured for two-factor authentication using RSA SecurID tokens with Windows Password Integration. Then they can use only the RSA SecurID token to logon to the system and get access to administrative applications published on Citrix Presentation Server, including the Citrix Access Suite Console and Citrix Management Console.

Configuration

- The environment shown in the diagram is for a two-server Citrix Presentation Server 4.0 farm with the IMA Datastore hosted on Microsoft SQL Server.
- Authentication is performed by Microsoft Active Directory. (Presentation Servers are member servers of the Active Directory domain.)
- Citrix License Server and Web Interface reside on separate, dedicated servers. (It is possible to install Web Interface and Citrix License Server on the same computer as the Presentation Server.)



- Web Interface contains several sites configured for different tasks, including a site that is configured with two-factor authentication using RSA SecurID 6.0 tokens.
- RSA ACE 6.0 server is present in the network to allow for two-factor authentication.
- Client computers are shown as a single icon that emulates all clients that use a variety of connection methods, including Internet Explorer (or another browser), Program Neighborhood or Program Neighborhood Agent clients.



Reference:

The connection table provided below can be used to search for a specific connection by source and / or destination:

Source	Destination	Ports Used
Access Suite Console	Citrix Presentation Server	135 + DCOM
Access Suite Console	Presentation Server Summary Database	1433
Access Suite Console	Web Interface Server	80
Citrix Management Console	Citrix Presentation Server	2513
Citrix Presentation Server	Active Directory Domain Controller	3268, 3269
Citrix Presentation Server	Citrix License Server	27000 + Random*
Citrix Presentation Server	Citrix Presentation Server	2512
Citrix Presentation Server	IMA Datastore	1433
Citrix Presentation Server	MF 1.8 Server	1604 Directed UDP
Citrix Presentation Server	Terminal Services Licensing Server	135
Citrix Presentation Server	Web Interface Server	80, 443
Internet Browser	Citrix License Server / License Management Console	8082
Internet Browser	Web Interface Server	80, 443
Program Neighborhood	Citrix Presentation Server	80, 443
Program Neighborhood	Citrix Presentation Server	1494, 2598
Program Neighborhood Agent	Citrix Presentation Server	80, 443, 1494, 2598
Program Neighborhood Agent	Web Interface Server	80, 443
Secure Gateway	Citrix Presentation Server - Secure Ticket Authority	80, 443
Secure Gateway	Web Interface Server	80, 443
Web Interface Server	Active Directory Domain Controller	3268, 3269
Web Interface Server	Citrix Presentation Server - XML Service	80, 443
Web Interface Server	RSA ACE Server	5500, 5580
Web Interface Server	Secure Gateway	443

Please see section 6.1 for detailed information

2.2. Presentation Server External Network Communication

Description:

This diagram illustrates connections performed when an external access to Citrix Presentation Server and its components are configured using a Secure Gateway session. The Secure Gateway is an application that runs as a service on a server that is deployed in the DMZ. The server running the Secure Gateway represents a single point of access to the secure, enterprise network. The Secure Gateway acts as an intermediary for every connection request originating from the Internet to the enterprise network.

Use Case 1:

Some Blinxalex Corporation users have an option to telecommute from home and use an Internet browser to securely connect to the list of server-based applications available to them. Users who work with sensitive data or applications use RSA SecurID tokens to provide additional authentication.

Administrator's Note

External or telecommuting users connect to a Presentation Server site on Web Interface Server through the Secure Gateway server, and then receive access to the published Citrix Presentation Server applications and resources. They would use either the Citrix Web client or Citrix Client for Java to launch the published applications and open ICA sessions.

Sensitive applications are made available from a different Presentation Server site on the same Web Interface server – this site is configured with two-factor authentication using RSA SecurID tokens. Both an RSA SecurID token and Windows (domain) password are required to logon. After the user enters both credentials they get a list of the sensitive applications. They then use the Citrix Web client or Citrix Client for Java to launch the published applications and open ICA sessions.

Use Case 2:

Members of the Blinxalex Corporation's marketing department sometimes collaborate with external consultants to create publications. These consultants are given temporary guest access and thus gain the ability to connect to a conference via the Web and participate in editing documents slated for publication.

Administrator's Note

In this situation, a "Guest User Web Interface for Conferencing Manager" site is configured on the Web Interface server, which allows guest users to connect to Conferencing Manager meetings without gaining access to other server resources. Consultants are given a guest username that is configured to have access to a specific conference in which a regular user launches an application to review and edit documents.

Conferencing Manager is installed and configured on the Citrix Presentation Server and External Conferencing Service is also configured (required for Guest User Web Interface to work).

Refer to the Administrator's Guide for Conferencing Manager for more information.

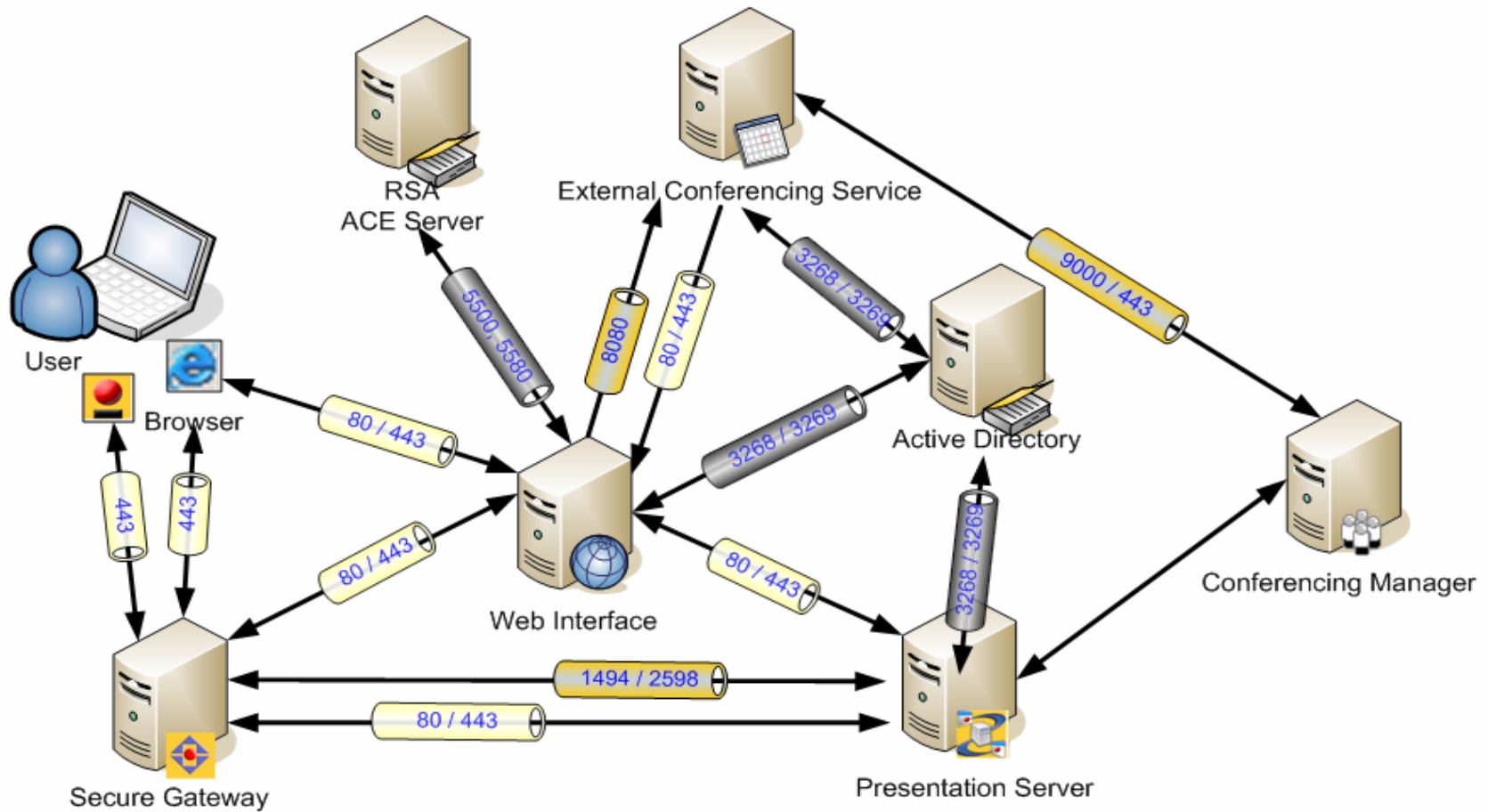
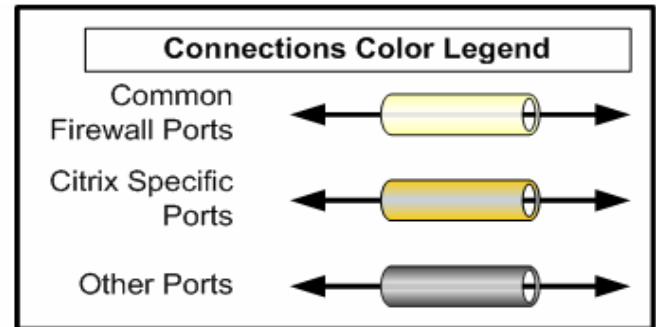
Configuration

- The environment shown in the following diagram is external access to the Citrix Presentation Server 4.0 farm.
- Authentication is performed by Microsoft Active Directory (Presentation Servers are member servers of the Active Directory Domain.)
- The Secure Gateway server is installed and configured.
- The Web Interface server contains several sites configured for different tasks, including a site that is configured with two-factor authentication using RSA SecurID 6.0 tokens.
- Conferencing Manager is installed and configured in the Presentation Server farm, and Guest User Web Interface for Conferencing Manager is configured on the Web Interface server. External Conferencing Service is installed on a separate server to provide access for the external guest user through the Web Interface Guest User site.
- RSA ACE 6.0 server is present in the network to allow for two-factor authentication.

(Note: Although both RSA authentication and Guest User Web Interface are shown in the same diagram here, it is not recommended to configure them both on the same Web Interface server at the same time.)

- Client computers are shown as a single icon that emulates all clients that use a variety of connection methods, including Internet Explorer (or another browser) and Program Neighborhood. All clients are considered to be external to the corporate network in this scenario.

Presentation Server External



**Reference:**

The connection table provided below can be used to search for a specific connection by source and / or destination:

Source	Destination	Ports Used
Citrix Presentation Server	Active Directory Domain Controller	3268, 3269
Citrix Presentation Server	ICA Client	Random Port 1023 – 5000*
Citrix Presentation Server	Web Interface Server	80, 443
Citrix Presentation Server - Conferencing Manager	External Conferencing Service	9000, 443
External Conferencing Service	Active Directory Domain Controller	3268, 3269
External Conferencing Service	Web Interface Server	80, 443
ICA Clients	Citrix Presentation Server	1604*
Program Neighborhood	Citrix Presentation Server	80, 443
Program Neighborhood	Citrix Presentation Server	1494, 2598
Secure Gateway	Citrix Presentation Server	1494, 2598
Secure Gateway	Citrix Presentation Server - Secure Ticket Authority	80, 443
Secure Gateway	Web Interface Server	80, 443
Web Interface Server	Active Directory Domain Controller	3268, 3269
Web Interface Server	Citrix Presentation Server - XML Service	80, 443
Web Interface Server	External Conferencing Service	8080
Web Interface Server	RSA ACE Server	5500, 5580
Web Interface Server	Secure Gateway	443

* See section 6.4 for detailed information

2.3. Presentation Server External Access: Secure Gateway Proxy

Description

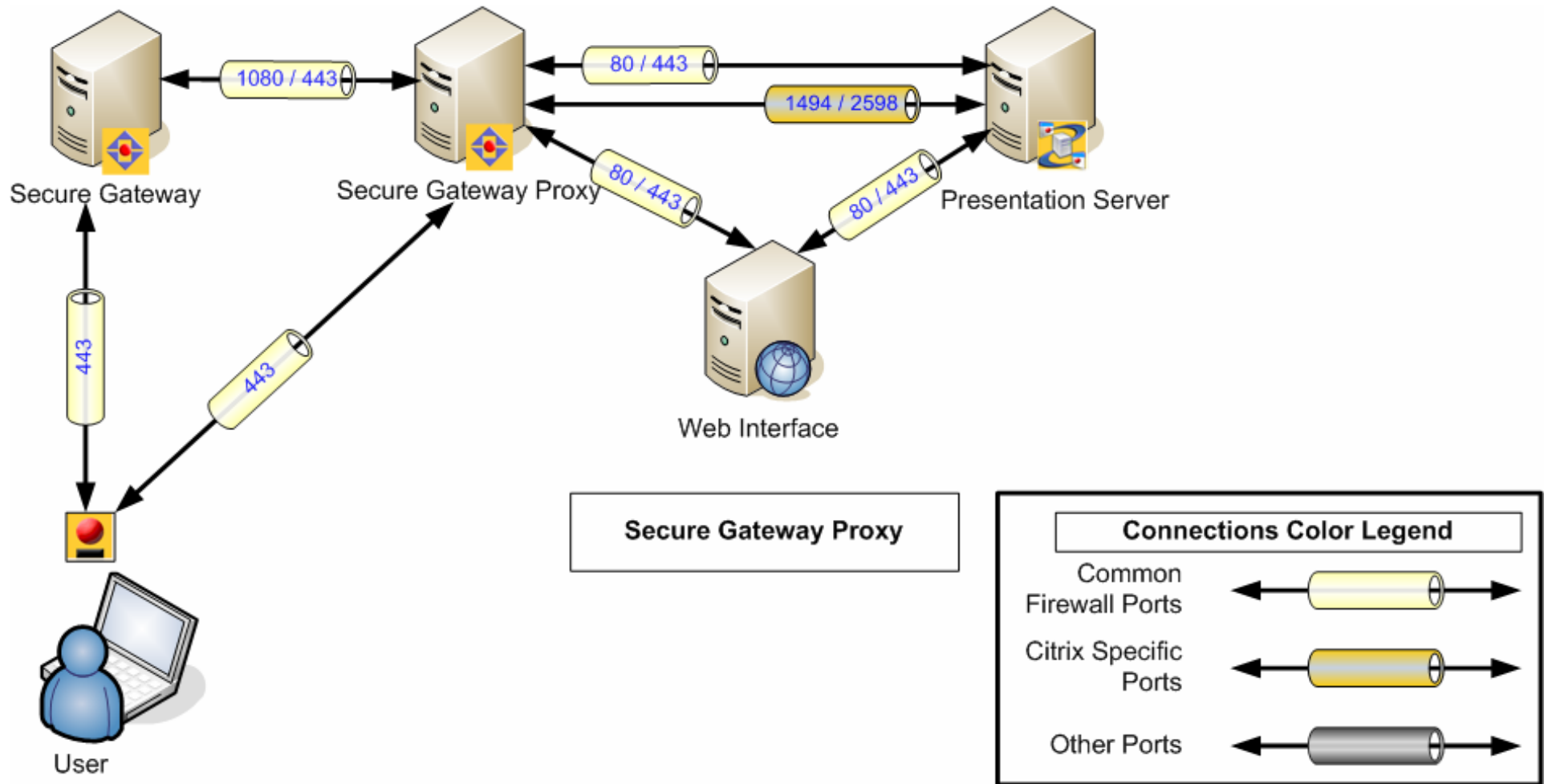
For increased security, the Secure Gateway Proxy is used with the Secure Gateway in a double-hop DMZ deployment. The Secure Gateway is installed in the first DMZ and the Secure Gateway Proxy is installed in the second DMZ. The Secure Gateway Proxy acts as a conduit for traffic originating from the Secure Gateway to servers in the secure network and from servers in the secure network to the Secure Gateway.

Use Case:

The Blinxalex Corporation's Security department provides an additional layer of external / peripheral protection to their internal network by installing two firewalls.

Administrator's Note

External or telecommuting users connect to a Presentation Server site on the Web Interface Server through the Secure Gateway server in the first DMZ and are then routed through the Secure Gateway Proxy in the second DMZ before accessing either the Web Interface server or Presentation Server resources.





Reference:

The connection table provided below can be used to search for a specific connection by source and / or destination:

Source	Destination	Ports Used
Secure Gateway	Secure Gateway Proxy	1080, 443
Secure Gateway Proxy	Citrix Presentation Server	1494, 2598
Program Neighborhood	Secure Gateway Proxy	443
Program Neighborhood	Secure Gateway	443
Secure Gateway Proxy	Web Interface Server	80, 443

3. Citrix Password Manager

The Citrix Password Manager™ diagrams below cover two modes of deployment for Password Manager: File Share mode (IFS) and integration with Microsoft Active Directory.

3.1. Citrix Password Manager in File Share Central Store Configuration

Description

The environment shown in the diagram below includes Citrix Password Manager Agent deployed both on client computers and on Citrix Presentation Server. This diagram also shows a connection from the Access Suite Console with the Password Manager Console plug-in used to administer Password Manager configuration and policies. In this environment the Password Manager Central Store resides on a network file share.

Use Case:

All Blinxalex corporate headquarters users like the ability provided by their network environment to remember credentials for various network applications, websites and resources. Whenever they go to a site that requires a password or launch another application that requires logon, Password Manager submits those credentials for them automatically. Password Manager, working to provide enterprise single sign-on functionality, even prompts users to save credentials when a new authorization dialog or screen appears.

Also, when users forget their passwords there is a mechanism already in place to simplify password resets, thus avoiding calls to the helpdesk or administrators for help.

Administrator's Note

In the Blinxalex corporate network, Password Manager Agent is deployed both on local client computers and on Citrix Presentation Server. The Password Manager Agent provides enterprise single sign-on functionality for users by prompting for, storing and using logon credentials for applications, sites and network resources. These credentials are stored in the Password Manager Central Store (which could be located either on a file share or integrated with the Microsoft Active Directory.)

The mechanism that allows users to reset their own passwords is called Self-Service Password Reset and is based on the Password Manager Service. It can be integrated into Web Interface and/or the Windows logon dialog.

For more information, review the Password Manager Administrator's Guide



Configuration:

- Password Manager is deployed using the network file share mode - the Central Store is located on a file share.
- Password Manager Agents are installed on client computers, as well as on Presentation Server, to provide ESSO functionality for both locally installed and published applications.
- The Password Manager Service is installed on a separate server to provide self-service functionality to users of the Password Manager Agent (for example, self-service password reset.)
- Administrators use the Access Suite Console with the Password Manager module to configure settings and policies for the Password Manager Agents.

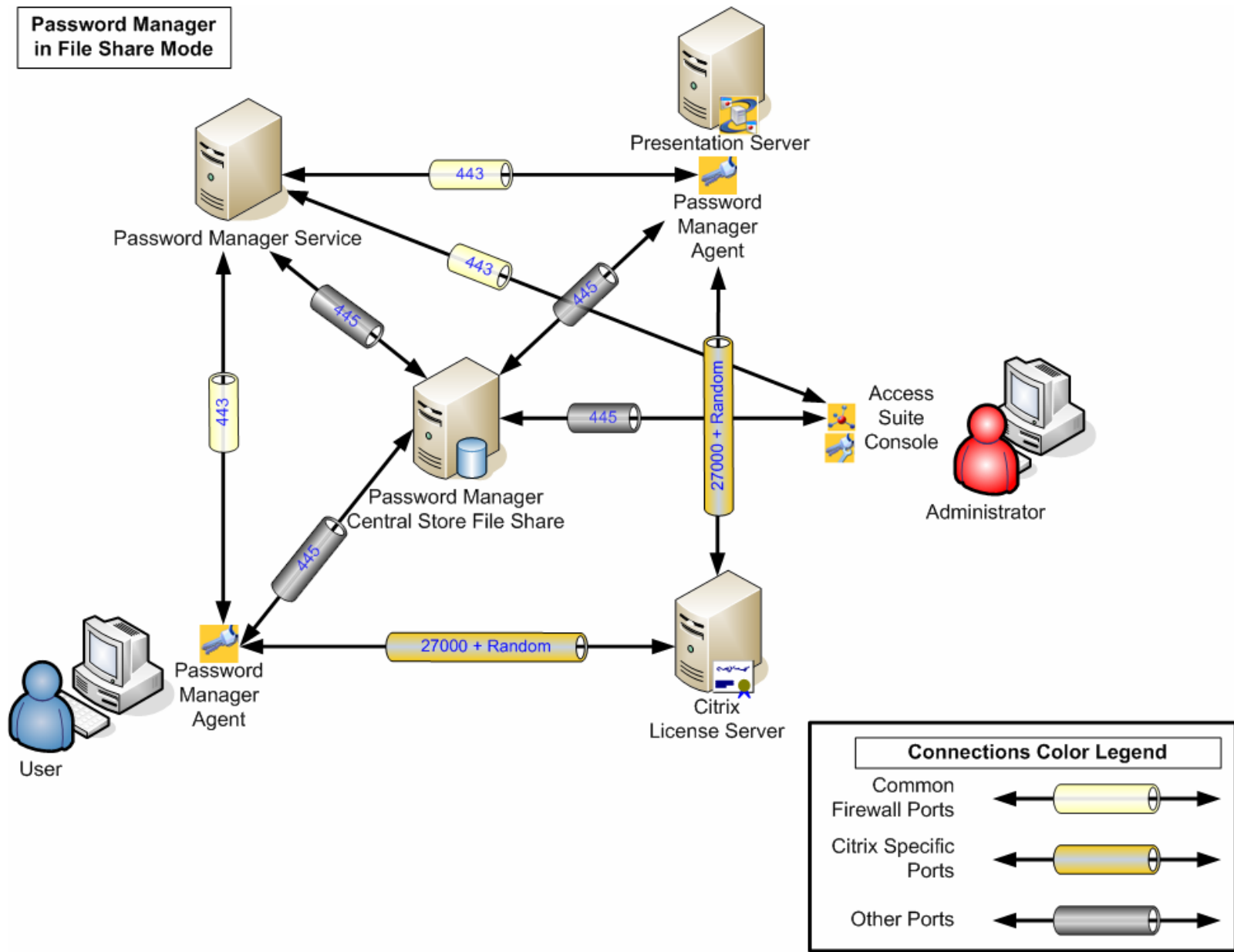
Reference:

The connection table provided below can be used to search for a specific connection by source and/or destination:

Source	Destination	Ports Used
Access Suite Console / Password Manager	Password Manager Central Store / File Share	445
Access Suite Console / Password Manager	Password Manager Service	443
Password Manager Agent	Citrix License Server	27000 + Random*
Password Manager Agent	Password Manager Central Store / File Share	445
Password Manager Agent	Password Manager Service	443
Password Manager Service	Password Manager Central Store / File Share	445

**Please note, detailed information regarding the Citrix License Server communication is provided in Section 6 of this document.*

**Password Manager
in File Share Mode**





3.2. Citrix Password Manager in Active Directory Central Store Configuration

Description:

The environment shown in the diagram below includes the Password Manager Agent deployed both on client computers and on Citrix Presentation Server. This diagram also shows a connection by the Access Suite Console with the Password Manager Console plug-in used to administer Password Manager configuration and policies. In this environment, Password Manager is integrated with Microsoft Active Directory.

Reference:

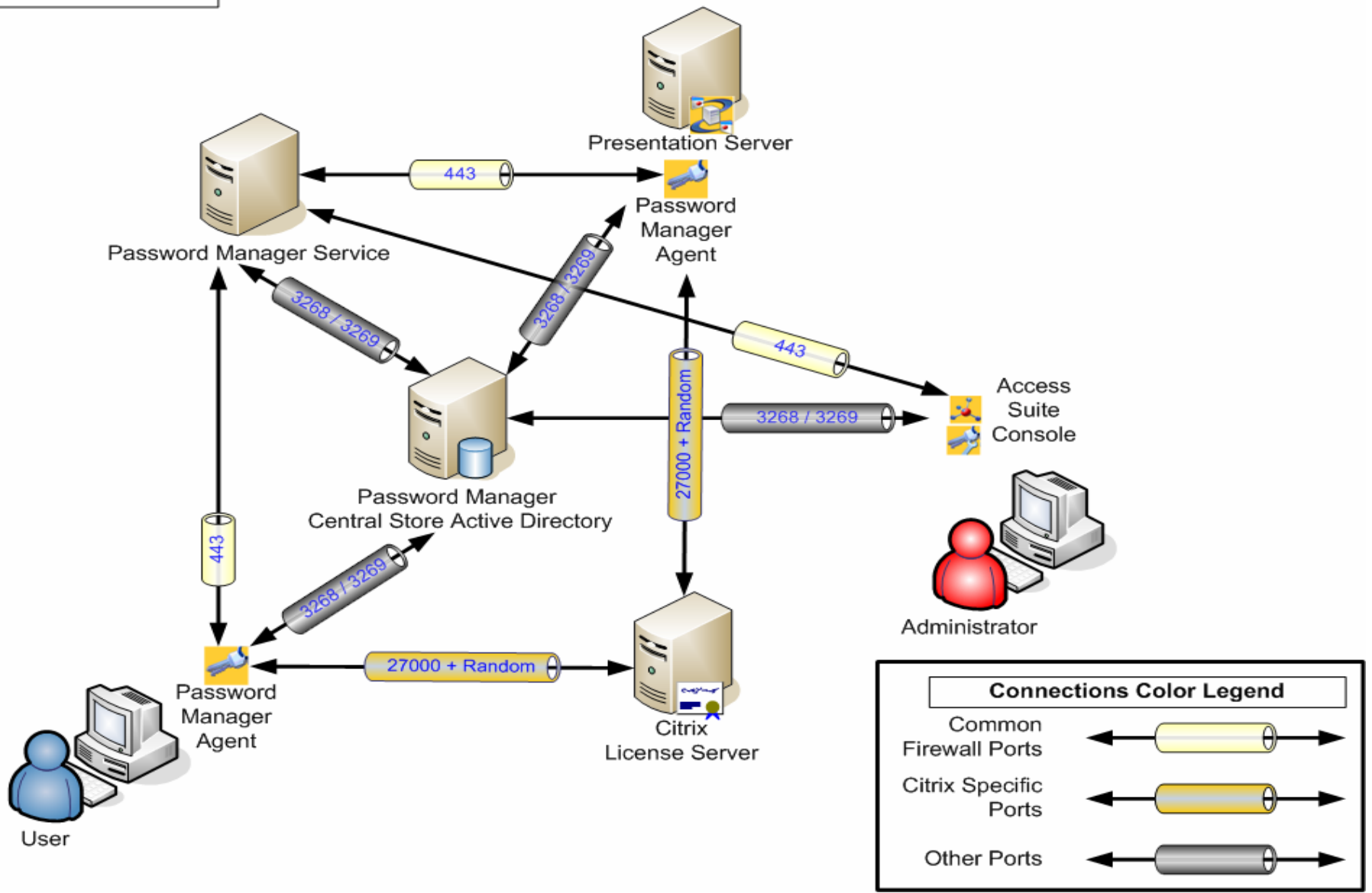
The connection table provided below can be used to search for a specific connection by source and / or destination:

Source	Destination	Ports Used
Access Suite Console / Password Manager	Password Manager Central Store / Active Directory	3268, 3269**
Access Suite Console / Password Manager	Password Manager Service	443
Password Manager Agent	Citrix License Server	27000 + Random*
Password Manager Agent	Password Manager Central Store / Active Directory	3268, 3269
Password Manager Agent	Password Manager Service	443
Password Manager Service	Password Manager Central Store / Active Directory	3268, 3269**

**Detailed information regarding Citrix License Server communication is provided in Section 6 of this document.*

*** More information about connections to Microsoft Active Directory is provided in section 6.7*

Password Manager in Active Directory



4. Citrix Access Gateway Enterprise

The Citrix Access Gateway™ Enterprise section covers connections to and from the Citrix Access Gateway appliance and Advanced Access Control option servers.

4.1. Citrix Access Gateway Enterprise Connections

Description

The main Access Gateway Enterprise diagram covers connections to and from the Access Gateway appliance and Advanced Access Control servers including user and administrator access.

Use Case 1:

Blinxalex corporate users have access to the main company website that allows them to see information customized for each department and group, and sometimes even for personal needs and functions. They see published and network resources, important information and company news, and can access their Web email.

Administrator's Note

Blinxalex corporate users connect to the Web server of the Access Gateway with Advanced Access Control, which is configured to provide customized information, pages and applications based on the user's identity. There are different pages configured for different user groups, each with specific design and information that would provide the most benefit to the logged on user.

There are configured integrations with Citrix Presentation Server, Web email (MS Outlook or IBM iNotes) and access to file shares.

For more information, review the *Citrix Access Gateway with Advanced Access Control Administrator's Guide*

Use Case 2:

When the same users want to access and work from this site from other, external locations, they connect to the website and company network using special client software that also verifies that the client computer adheres to the corporate security requirements. Once connected, authorized and verified users can have the same level of access as if they were still inside the office.

Administrator's Note

When authorized Blinalex corporate users are away from the corporate offices, they use the Citrix Secure Access client which communicates with the Access Gateway appliance. This provides external users with secure, VPN access to the corporate network. During the connection, users' computers are verified to match the security policies set by the administrator, such as verification of anti-virus software presence and version, etc.

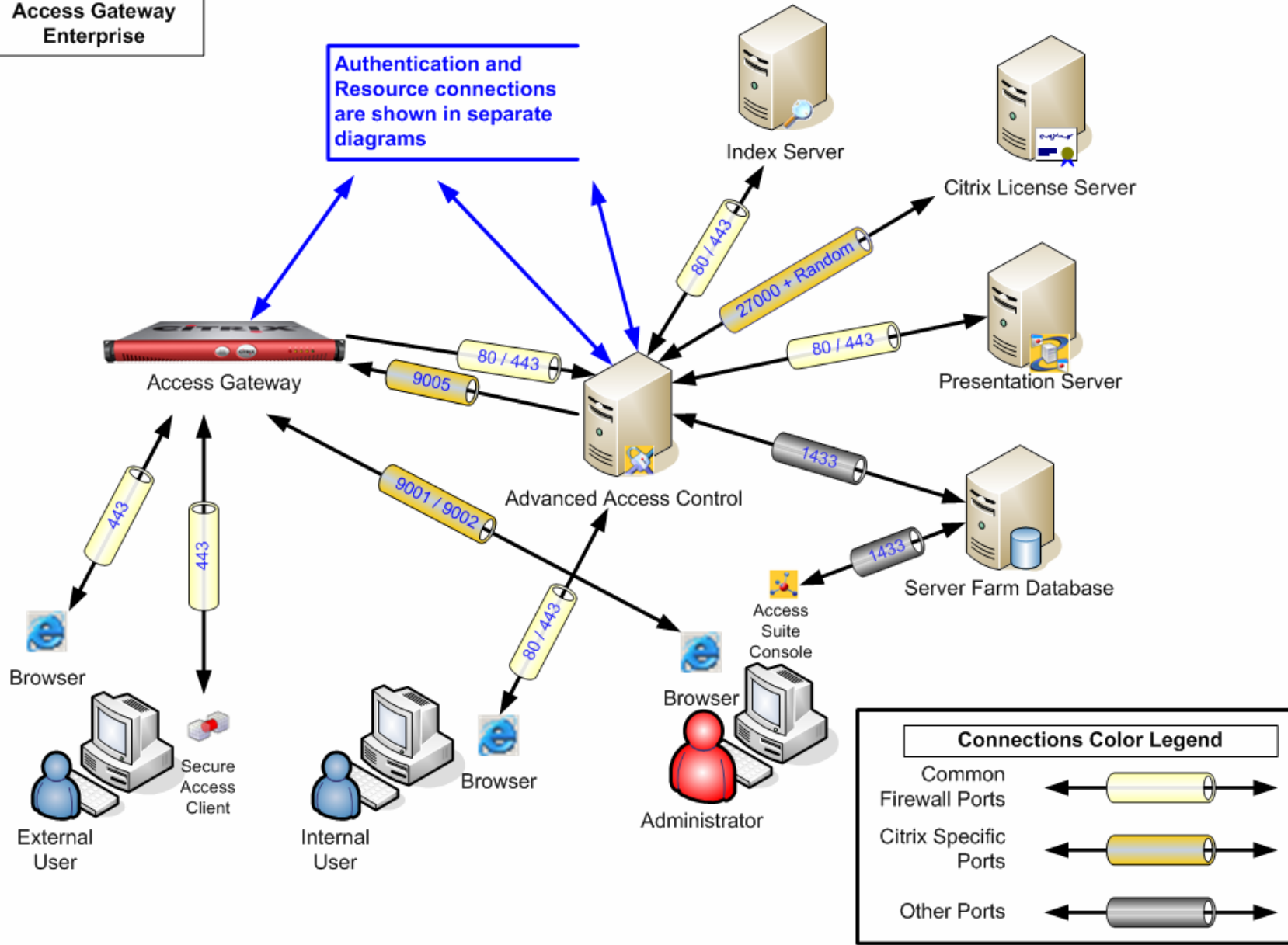
For more information, review the *Citrix Access Gateway with Advanced Access Control Administrator's Guide*

Configuration

- The Access Gateway Enterprise diagram below illustrates a deployment of the Access Gateway appliance with Advanced Access Control server.
- Authentication and resource connections from both Access Gateway and Advanced Access Control are shown on separate diagrams.
- Advanced Access Control obtains its licenses from the Citrix License Server, while Access Gateway appliance has an internal license management mechanism.
- Users connect to Access Gateway Enterprise using either an Internet browser or the Secure Access Client. They can access a variety of resources - from Presentation Server published applications, to web e-mail and file shares.
- Administrators manage the Access Gateway Enterprise environment using the Access Suite Console.
- In the environment shown in the diagram below, the Advanced Access Control farm database server is hosted on Microsoft SQL server.

Access Gateway Enterprise

Authentication and Resource connections are shown in separate diagrams





Reference:

The connection table provided below can be used to search for a specific connection by source and / or destination:

Source	Destination	Ports Used
Access Gateway	Advanced Access Control	80, 443
Access Suite Console / Advanced Access Control	Advanced Access Control Farm Database Server	1433
Advanced Access Control	Access Gateway	9005
Advanced Access Control	Advanced Access Control Farm Database Server	1433
Advanced Access Control	Citrix License Server	27000 + Random*
Advanced Access Control	Citrix Presentation Server - XML Service	80, 443
Index Server	Advanced Access Control	80, 443
Administrator / Internet Browser	Access Gateway / Administration Desktop or Portal	9001
Administrator / Internet Browser	Access Gateway / Administration Tool	9002
Internet Browser	Access Gateway	443
Internet Browser	Advanced Access Control Web Server	80, 443
Secure Access Client	Access Gateway	443

**Detailed information regarding Citrix License Server communication is provided in Section 6 of this document.*

4.2. Advanced Access Control Resources' Connections

Description

The following diagram illustrates connections from Advanced Access Control to various resource servers including file and Web resources, Web email and secure access to email.

Use Case

Blinxalex corporate users have access to an internal corporate website that is customized to provide them with the content most important to their respective departments. When users logon to this website they see the applications they need for work, departmental and corporate news, links to their email, and access to their department's central file share.

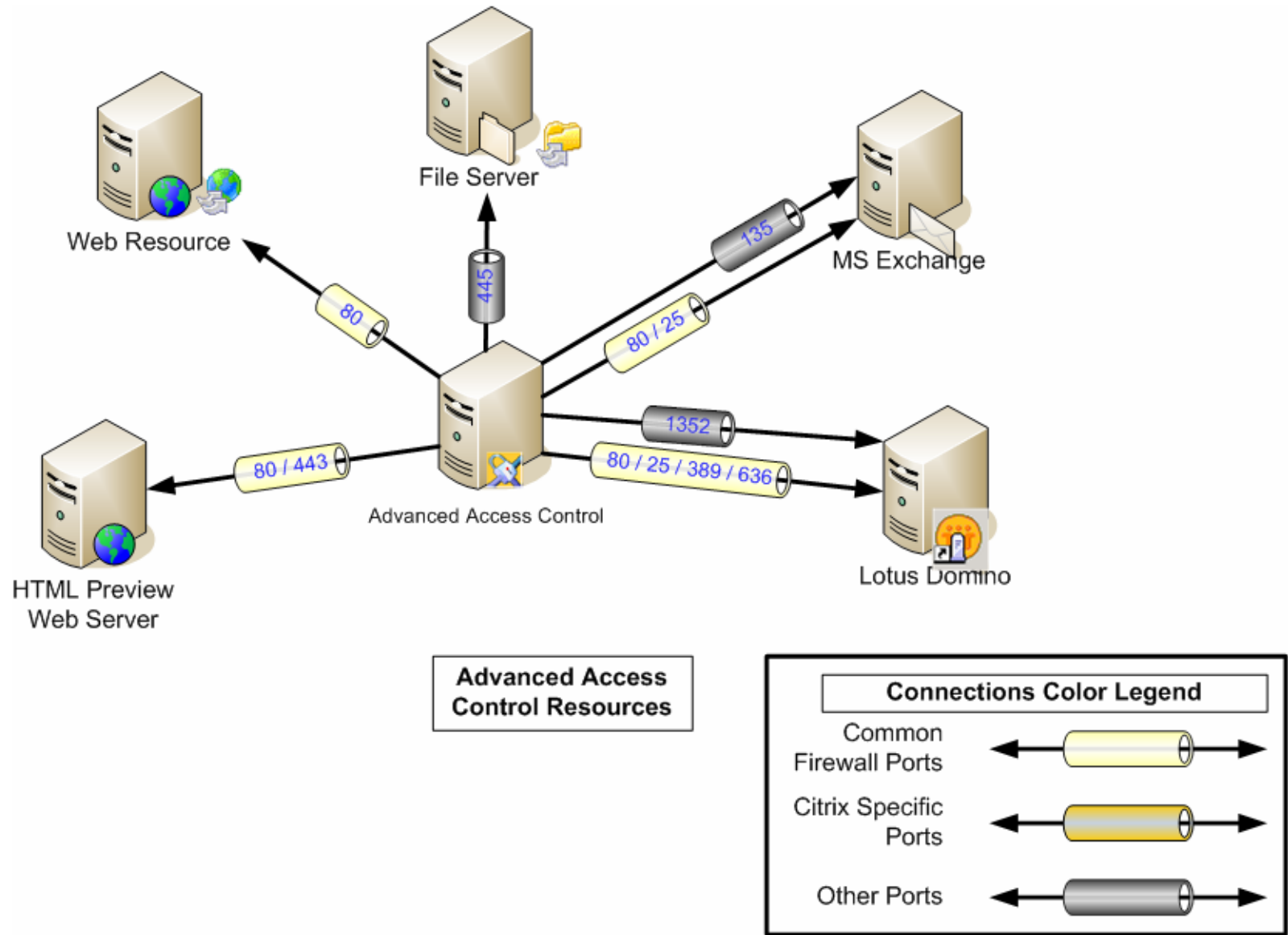
Administrator's Note

Authorized Blinxalex corporate users connect to Advanced Access Control web server with Access Center(s) configured to provide them with policy- and identity-driven resources, from Presentation Server published applications to integration with MS Exchange or iNotes web mail, as well as access to file shares through the Web Interface.

For more information, review the *Citrix Access Gateway with Advanced Access Control Administrator's Guide*.

Configuration

- The diagram below shows connections to various resources of the Advanced Access Control server





Reference:

The connection table provided below can be used to search for a specific connection by source and/or destination:

Source	Destination	Ports Used
Advanced Access Control	External File Server	445
Advanced Access Control	External Web Mail Server	80*
Advanced Access Control	External Web Server	80
Advanced Access Control	HTML Web Preview Server	80, 443
Advanced Access Control	Lotus Domino Server	80, 1352, 25, 389, 636
Advanced Access Control	MS Exchange Server	80, 25, 135

* External web mail servers include Web Mail access to MS Exchange and IBM iNotes.

4.3. Advanced Access Control Authentication Connections

Description

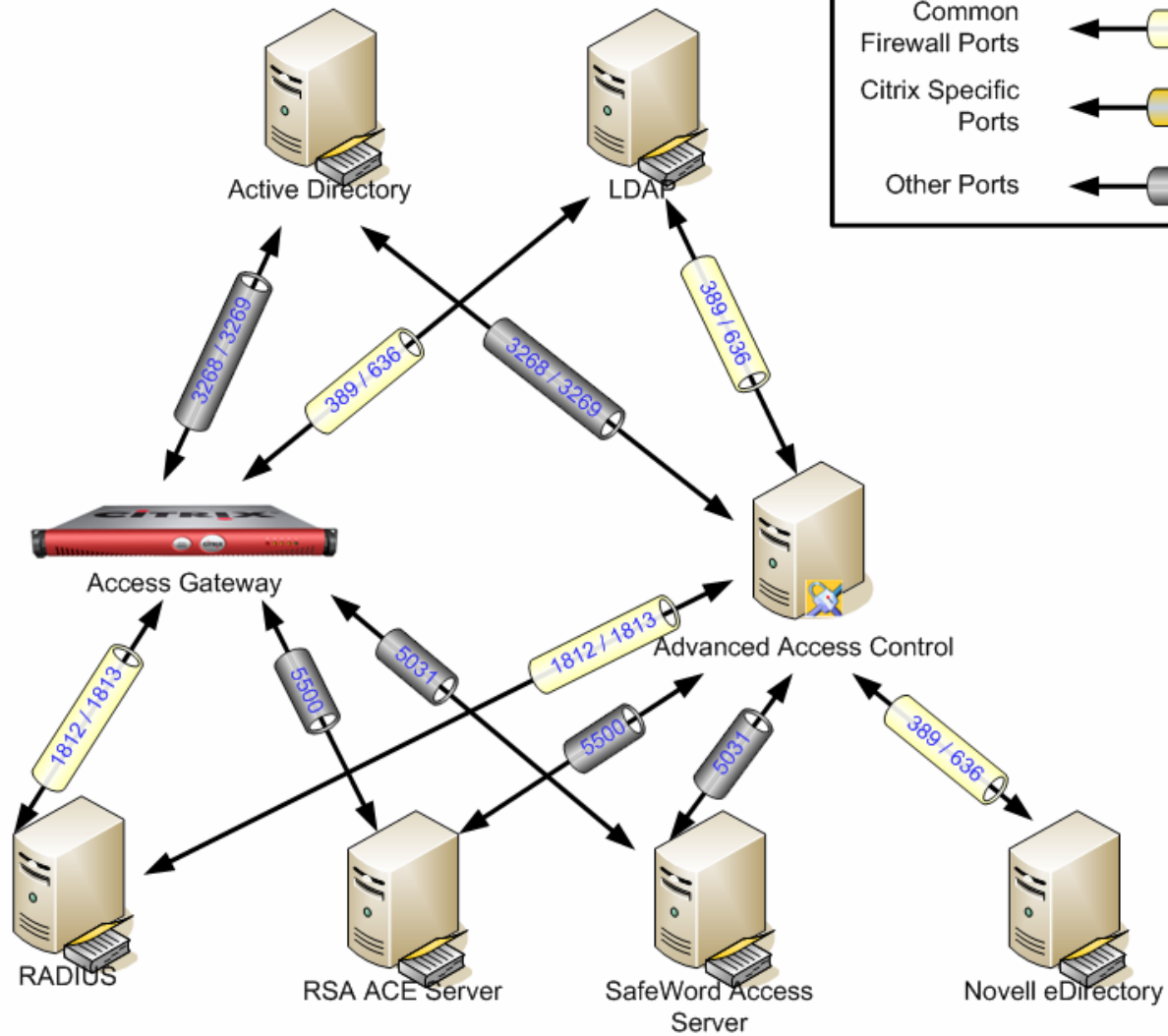
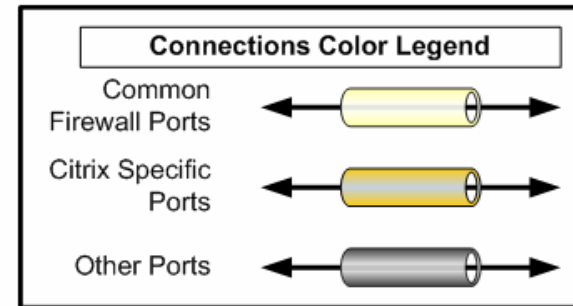
The following diagram shows connectivity from the Access Gateway appliance and Advanced Access Control server to various authentication servers.

Reference:

The connection table provided below can be used to search for a specific connection by source and/or destination:

Source	Destination	Ports Used
Access Gateway	LDAP Directory Server	389, 636
Access Gateway	RADIUS Server	1812, 1813
Access Gateway	RSA ACE Server	5500
Access Gateway	SafeWord Access Server	5031
Access Gateway	Active Directory Domain Controller	3268, 3269
Advanced Access Control	Active Directory Domain Controller	3268, 3269
Advanced Access Control	LDAP Directory Server	389, 636
Advanced Access Control	Novell eDirectory	389, 636
Advanced Access Control	RADIUS Server	1812, 1813
Advanced Access Control	RSA ACE Server	5500
Advanced Access Control	SafeWord Access Server	5031

Access Gateway Enterprise Authentications



5. GoToMeeting Helper for Citrix Presentation Server

Description:

GoToMeeting™ Helper for Citrix Presentation Server is an application provided by Citrix Online to integrate GoToMeeting functionality with published applications. GoToMeeting Helper allows Presentation Server users to perform all GoToMeeting actions normally available from locally installed GoToMeeting client software from within an ICA session. Advanced integration is possible with Microsoft Outlook and Lotus Notes email software applications.

One of the special features of the GoToMeeting Helper is the ability to configure Presentation Server to redirect a launch of a GoToMeeting online meeting to the client computer. Redirecting the launch of a meeting to the users' client computers reduces the load on the Presentation Server while keeping all other GoToMeeting functions available inside the session.

Use Case

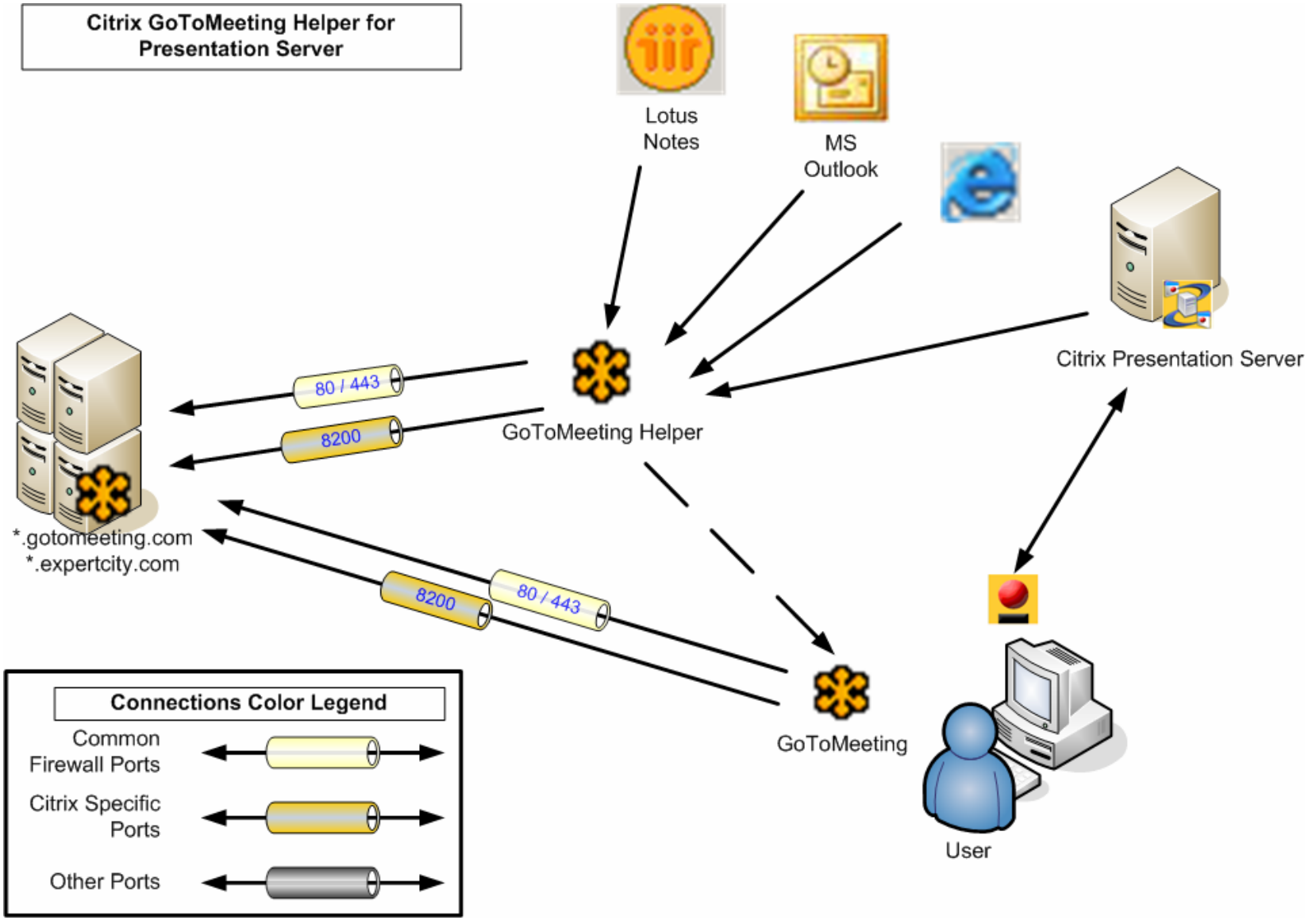
Blinxalex Corporation's marketing department users connect to Microsoft® Outlook® published on Presentation Server for email and schedule their online meetings using the Outlook GoToMeeting toolbar. They also use GoToMeeting to collaborate on presentation materials. When the marketing department users are in their own offices they can share the screen of their office desktop with other meeting attendees. When traveling outside of the department location, members of the marketing department can run Microsoft PowerPoint published on Presentation Server to share their presentations with others.

Administrator's Note

Blinxalex Corporate users connect to Microsoft Outlook or IBM Lotus Notes email clients published on the Presentation Server that also has GoToMeeting Helper for Presentation Server installed. Users have the ability to perform GoToMeeting actions using either the Outlook GoToMeeting Toolbar or menu in the Lotus Notes clients.

To collaborate on the creation of PowerPoint presentations users use published Microsoft PowerPoint and during travel run the GoToMeeting from inside the ICA session, started from published Microsoft Outlook or IBM Lotus Notes in the same session. When in the office, the meetings are redirected to the GoToMeeting software installed on their local client computer.

Administration options for the GoToMeeting Helper for Presentation Server allow the administrator to configure meetings to either run inside the ICA session on the Presentation server or to utilize the Server-to-Client Content redirection feature of the Presentation Server to redirect the meeting launch to the client desktop. For more information, review the administrator's guides for Citrix Presentation Server and GoToMeeting Helper for Presentation Server. The *Citrix Presentation Server Administrator's Guide for Installing Citrix GoToMeeting* is available in the Citrix Knowledge Base article [CTX107190](#).





Reference:

The connection table provided below can be used to search for a specific connection by source and / or destination:

Source	Destination	Ports Used
Citrix Presentation Server / GoToMeeting Helper	*.gotomeeting.com, *.expertcity.com	8200, 443, 80
Client / GoToMeeting Client	*.gotomeeting.com, *.expertcity.com	8200, 443, 80

All of these connections are outbound only.

6. Special product notes:

6.1. Citrix License Server

This document specifies “Random” for the Citrix daemon port on the Citrix License Server. If connections to the License Server are to be provided through a firewall, the Citrix daemon port should be changed to a static port number as described in the Citrix Knowledge Base article [CTX103356 – “Firewall between the License Server and the computer running MetaFrame Presentation Server.”](#)

6.2. Citrix Presentation Server IMA Datastore Server

In this document the port “1433” listed for connections from Presentation Server to the IMA Datastore is specifically for connections to Microsoft SQL Server. If your environment uses a different database server to host the IMA Datastore, please obtain information from your database server documentation regarding the network port(s) used for connection(s).

6.3. Citrix Access Management Console

To configure access through firewalls for a Citrix Access Management Console connecting to managed servers, please follow the instructions in the Citrix Knowledgebase article [CTX107050 – “Enabling Citrix Access Management Console Traffic Across Firewall Policies”](#).

6.4. TCP/IP ICA Browsing

If TCP/IP ICA Browsing is used by the ICA Client, additional connections are created between the client computer and Presentation Server. The ports used in these connections are:

ICA Client to Presentation Server: **1604 UDP**

Presentation Server to ICA Client: **Random port between 1023 – 5000 UDP**
(Outbound)

Note: It is recommended to use TCP/IP + HTTP browsing as it avoids UDP usage.

6.5. Interoperability with Citrix MetaFrame 1.8 Servers

When MetaFrame® 1.8 servers are part of a mixed Presentation Server farm, Citrix Presentation Server 4.0 establishes communication with the MetaFrame 1.8 server using **Directed UDP** over **port 1604**.

Presentation Server 4.0 to MetaFrame 1.8 Server: **1604 Directed-UDP**

6.6. Citrix Presentation Server for UNIX

Presentation Server 4.0 for UNIX® utilizes an additional port for inter-server communication different from Presentation Server 4.0 for Windows. The UNIX servers use TCP port 2897 for administration commands and management information updates and queries. Please note cross-server administration between Windows and UNIX versions of Presentation Server is not possible. Only servers running Presentation Server 4.0 for UNIX can become part of a UNIX server farm. Similarly, only servers running Presentation Server for Windows can become part of a Windows server farm.

Administrator's Note

Inter-server communication between servers running Presentation Server 4.0 for UNIX in a server farm utilizes TCP port 2897.

More information is available in the *MetaFrame Presentation Server for UNIX Administrator's Guide* available in the Citrix Knowledge Base article [CTX106447](#)

6.7. Connections to Microsoft Active Directory Domain Controllers

Connections to Microsoft Active Directory Domain Controllers are possible via several ports. The ports are:

- 389 for LDAP connection,
- 636 for LDAP SSL connection,
- 3268 for LDAP connection to Global Catalog,
- 3269 for LDAP SSL connection to Global Catalog.

For more information, see the Microsoft Knowledgebase article [832017 - Service overview and network port requirements for the Windows Server system](#)



Appendix: Access Suite Connections Reference Table:

Diagram	Source	Destination	Ports Used
Access Gateway Authentication	Access Gateway	LDAP Directory Server	389, 636
Access Gateway Authentication	Access Gateway	RADIUS Server	1812, 1813
Access Gateway Authentication	Access Gateway	RSA ACE Server	5500
Access Gateway Authentication	Access Gateway	SafeWord Access Server	5031
Access Gateway Authentication	Access Gateway	Active Directory Domain Controller	3268, 3269
Access Gateway Authentication	Advanced Access Control	Active Directory Domain Controller	3268, 3269
Access Gateway Authentication	Advanced Access Control	LDAP Directory Server	389, 636
Access Gateway Authentication	Advanced Access Control	Novell eDirectory	389, 636
Access Gateway Authentication	Advanced Access Control	RADIUS Server	1812, 1813
Access Gateway Authentication	Advanced Access Control	RSA ACE Server	5500
Access Gateway Authentication	Advanced Access Control	SafeWord Access Server	5031
Access Gateway Enterprise	Access Gateway	Advanced Access Control	80, 443
Access Gateway Enterprise	Access Suite Console / Advanced Access Control	Advanced Access Control Farm Database Server	1433
Access Gateway Enterprise	Administrator / Internet Browser	Access Gateway / Administration Desktop or Portal	9001
Access Gateway Enterprise	Administrator / Internet Browser	Access Gateway / Administration Tool	9002
Access Gateway Enterprise	Advanced Access Control	Access Gateway	9005
Access Gateway Enterprise	Advanced Access Control	Advanced Access Control Farm Database Server	1433
Access Gateway Enterprise	Advanced Access Control	Citrix License Server	27000 + Random*
Access Gateway Enterprise	Advanced Access Control	Citrix Presentation Server - XML Service	80, 443
Access Gateway Enterprise	Index Server	Advanced Access Control	80, 443



Access Gateway Enterprise	Internet Browser	Access Gateway	443
Access Gateway Enterprise	Internet Browser	Advanced Access Control Web Server	80, 443
Access Gateway Enterprise	Secure Access Client	Access Gateway	443
Access Gateway Resources	Advanced Access Control	External File Server	445
Access Gateway Resources	Advanced Access Control	External Web Mail Server	80
Access Gateway Resources	Advanced Access Control	External Web Server	80
Access Gateway Resources	Advanced Access Control	HTML Web Preview Server	80, 443
Access Gateway Resources	Advanced Access Control	Lotus Domino Server	80, 1352, 25, 389, 636
Access Gateway Resources	Advanced Access Control	MS Exchange Server	80, 25, 135
Citrix Online	Citrix Presentation Server / GoToMeeting Helper	*.gotomeeting.com, *.expertcity.com	8200, 443, 80
Citrix Online	Client / GoToMeeting Client	*.gotomeeting.com, *.expertcity.com	8200, 443, 80
Password Manager Active Directory	Access Suite Console / Password Manager	Password Manager Central Store / Active Directory	3268, 3269
Password Manager Active Directory	Access Suite Console / Password Manager	Password Manager Service	443
Password Manager Active Directory	Password Manager Agent	Citrix License Server	27000 + Random*
Password Manager Active Directory	Password Manager Agent	Password Manager Central Store / Active Directory	3268, 3269
Password Manager Active Directory	Password Manager Agent	Password Manager Service	443
Password Manager Active Directory	Password Manager Service	Password Manager Central Store / Active Directory	3268, 3269
Password Manager File Share	Access Suite Console / Password Manager	Password Manager Central Store / File Share	445
Password Manager File Share	Access Suite Console / Password Manager	Password Manager Service	443



Password Manager File Share	Password Manager Agent	Citrix License Server	27000 + Random*
Password Manager File Share	Password Manager Agent	Password Manager Central Store / File Share	445
Password Manager File Share	Password Manager Agent	Password Manager Service	443
Password Manager File Share	Password Manager Service	Password Manager Central Store / File Share	445
Presentation Server External	Citrix Presentation Server	Active Directory Domain Controller	3268, 3269
Presentation Server External	Citrix Presentation Server	ICA Client	Random Port 1023 – 5000
Presentation Server External	Citrix Presentation Server	Web Interface Server	80, 443
Presentation Server External	Citrix Presentation Server – Conferencing Manager	External Conferencing Service	9000, 443
Presentation Server External	External Conferencing Service	Active Directory Domain Controller	3268, 3269
Presentation Server External	External Conferencing Service	Web Interface Server	80, 443
Presentation Server External	ICA Clients	Citrix Presentation Server	1604*
Presentation Server External	Program Neighborhood	Citrix Presentation Server	80, 443
Presentation Server External	Program Neighborhood	Citrix Presentation Server	1494, 2598
Presentation Server External	Secure Gateway	Citrix Presentation Server	1494, 2598
Presentation Server External	Secure Gateway	Citrix Presentation Server – Secure Ticket Authority	80, 443
Presentation Server External	Secure Gateway	Web Interface Server	80, 443
Presentation Server External	Web Interface Server	Active Directory Domain Controller	3268, 3269
Presentation Server External	Web Interface Server	Citrix Presentation Server – XML Service	80, 443
Presentation Server External	Web Interface Server	External Conferencing Service	8080
Presentation Server External	Web Interface Server	RSA ACE Server	5500, 5580
Presentation Server External	Web Interface Server	Secure Gateway	443
Presentation Server Internal	Access Suite Console	Citrix Presentation Server	135 + DCOM
Presentation Server Internal	Access Suite Console	Presentation Server Summary Database	1433



Presentation Server Internal	Access Suite Console	Web Interface Server	80
Presentation Server Internal	Citrix Management Console	Citrix Presentation Server	2513
Presentation Server Internal	Citrix Presentation Server	Active Directory Domain Controller	3268, 3269
Presentation Server Internal	Citrix Presentation Server	Citrix License Server	27000 + Random*
Presentation Server Internal	Citrix Presentation Server	Citrix Presentation Server	2512
Presentation Server Internal	Citrix Presentation Server	IMA Datastore	1433
Presentation Server Internal	Citrix Presentation Server	MF 1.8 Server	1604 Directed UDP
Presentation Server Internal	Citrix Presentation Server	Terminal Services Licensing Server	135
Presentation Server Internal	Citrix Presentation Server	Web Interface Server	80, 443
Presentation Server Internal	Internet Browser	Citrix License Server / License Management Console	8082
Presentation Server Internal	Internet Browser	Web Interface Server	80, 443
Presentation Server Internal	Program Neighborhood	Citrix Presentation Server	80, 443
Presentation Server Internal	Program Neighborhood	Citrix Presentation Server	1494, 2598
Presentation Server Internal	Program Neighborhood Agent	Citrix Presentation Server	80, 443, 1494, 2598
Presentation Server Internal	Program Neighborhood Agent	Web Interface Server	80, 443
Presentation Server Internal	Secure Gateway	Citrix Presentation Server - Secure Ticket Authority	80, 443
Presentation Server Internal	Secure Gateway	Web Interface Server	80, 443
Presentation Server Internal	Web Interface Server	Active Directory Domain Controller	3268, 3269
Presentation Server Internal	Web Interface Server	Citrix Presentation Server - XML Service	80, 443
Presentation Server Internal	Web Interface Server	RSA ACE Server	5500, 5580
Presentation Server Internal	Web Interface Server	Secure Gateway	443
Presentation Server Secure Gateway Proxy	Program Neighborhood	Secure Gateway	443
Presentation Server Secure Gateway Proxy	Program Neighborhood	Secure Gateway Proxy	443



Presentation Server Secure Gateway Proxy	Secure Gateway	Secure Gateway Proxy	1080, 443
Presentation Server Secure Gateway Proxy	Secure Gateway Proxy	Citrix Presentation Server	1494, 2598
Presentation Server Secure Gateway Proxy	Secure Gateway Proxy	Web Interface Server	80, 443

Notice

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

This publication contains information protected by copyright. Except for internal distribution, no part of this publication may be photocopied or reproduced in any form without prior written consent from Citrix.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

©2006 Citrix Systems, Inc. All rights reserved. Citrix®, ICA®, Program Neighborhood®, Citrix Presentation Server™, Citrix Password Manager™, Citrix Access Suite™, Citrix Access Gateway™, GoToMeeting™, and SmoothRoaming™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and other countries. Microsoft®, Windows® and Outlook® are registered trademarks of Microsoft Corporation in the United States and/or other countries. UNIX® is a registered trademark of The Open Group in the United States and other countries. All other trademarks and registered trademarks are property of their respective owners.